NCOSS

NSW Council of Social Service

WorkVentures

social inclusion through technology

Hidden Vulnerabilities:

Cyber Security and Essential Community Services in NSW

About this report

This report was commissioned by the NSW Council of Social Service (NCOSS) to improve understanding and awareness of key cyber security risks for NSW social service organisations, with funding from the NSW State Peaks Program, a program of the NSW Department of Communities and Justice.

This project was co-funded and delivered by WorkVentures, who made a significant financial contribution to the development and execution of this work. Additional funding for key resources involved in this project was provided by the Australian Government Department of Industry, Science and Resources.

We acknowledge the use of Dr Paul Watters' 100 Point Check to measure cyber maturity – details can be found at https://www.cyberstronomy.com/about.

We thank the social service organisations, cyber security specialists and consultants, who generously shared their expertise, insights, and experience to formulate this report. We appreciate the collaboration and support of our partners in bringing this important work to life.

Copyright and Citation

This publication is copyright by WorkVentures (ABN 74002721217). Non-profit social service organisations have permission to reproduce part of this report as long as the original meaning is retained, and proper credit is given to WorkVentures and NCOSS. All other persons and organisations wanting to reproduce material from this report should obtain permission from the publishers, except as used under fair dealing exceptions of Australian copyright law.

Suggested citation: Work Ventures (2025). Hidden Vulnerabilities: Cyber Security and Essential Community Services in NSW. Report prepared for NCOSS.

Acknowledgement of Country

NCOSS and WorkVentures acknowledge Aboriginal and Torres Strait Islander peoples as the Traditional Custodians of Country and their continuing connection to both their lands and seas. We also pay our respects to Elders—past and present—and generations of Aboriginal and Torres Strait Islander peoples now and into the future. We acknowledge the spirit of the Uluru Statement from the Heart and accept the invitation to walk with First Nations peoples in a movement of the Australian people for a better future.

NCOSS

NSW Council of Social Service

WorkVentures

social inclusion through technology

Contents

Abstract

In 2024, WorkVentures partnered with the New South Wales Council of Social Service (NCOSS) to assess the cyber security posture of 14 not-for-profit (NFP) organisations in the NSW social service sector, and to provide specialist advice to uplift cyber security maturity across the sector. Strikingly, none of the organisations met the benchmark for what could be considered as a mature posture across the four domains that were assessed: operational; legal and regulatory; systems; and network processes and controls.

The findings highlight the pressing need for:

1. targeted funding for NSW Government-funded community service sector organisations to improve their cyber security posture;
2. a tailored cyber security assessment and uplift program; and
3. the establishment of a sector-specific national cyber security standard.

Executive Summary

Australian not for profit (NFP) organisations face disproportionate challenges when it comes to securing their digital infrastructure. They have limited resources and expertise; specific sub-sectors (e.g. Domestic and Family Violence) hold highly sensitive data; and cyber threats are increasing in their sophistication and targeted nature.

WorkVentures has partnered with the New South Wales Council of Social Service (NCOSS) to perform an in-depth assessment of the cyber security posture for 14 NFPs that operate in the NSW community services sector. The purpose was to identify key challenges facing the sector, common deficiencies, and opportunities to bridge the gap for these organisations to effectively safeguard their data. This activity included a range of NFPs, with total revenue between $2 million and $20 million, and headcounts ranging from under 10 to over 100 full time equivalent staff. The assessment methodology examined 100 questions covering the organisation's operational, legal and regulatory, systems, and network security position. A maturity rating was calculated for each NFP across four domains out of 25 points, with a total score out of 100; a 'mature' position was deemed to be 20 points across all four domains or a total score of 80 points. Each organisation received 10 recommendations in the form of processes and controls to address the highest risk areas.

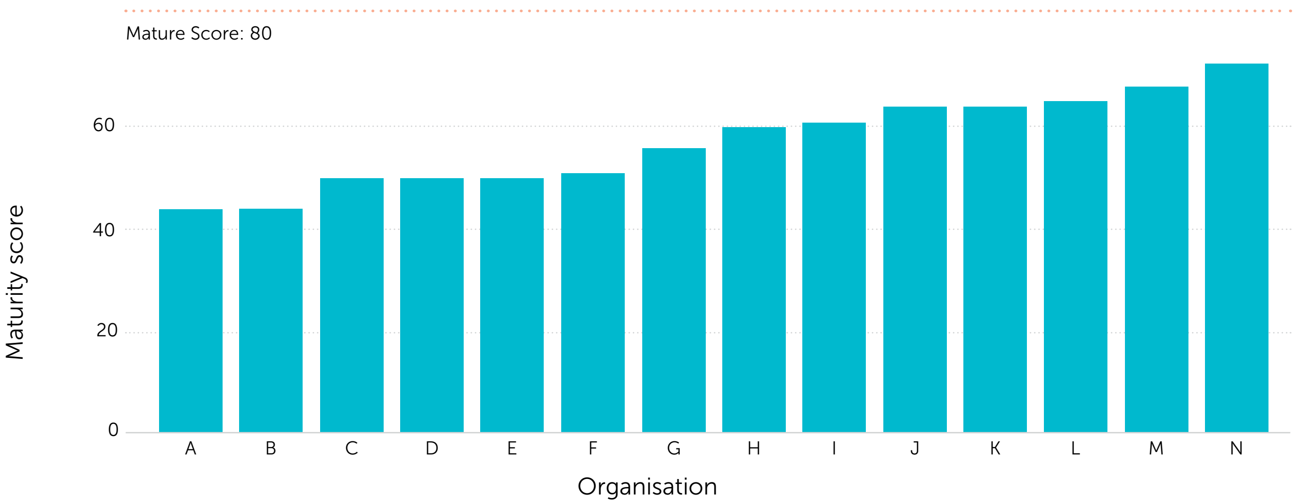
Key Findings

The assessments indicate that the NFP community services sector has substantial gaps in its cyber security posture and protection against key threats:

1 None of the assessed organisations met the benchmark of 20 points across all four domains or a total score of 80 points.

The average score was 57, with only 6 of the organisations receiving a score greater than 60.

FIGURE 1: Cyber maturity scores against the benchmark mature score of 80



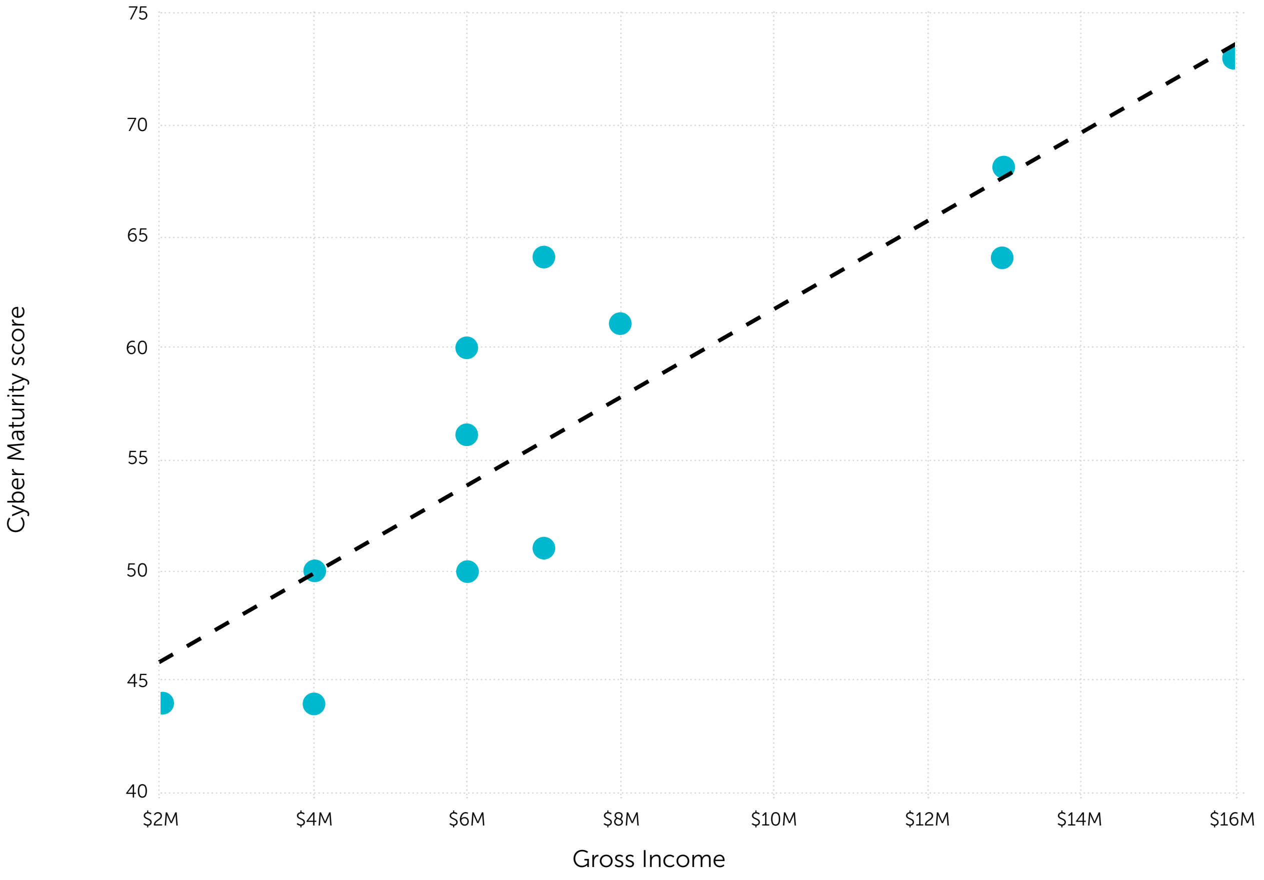
2 All organisations recognised the importance of cyber security and want to do more, but report that they are under-resourced to respond effectively.

Organisations consistently reported that they struggled to fund the necessary investments in systems and could not afford to recruit significant cyber security expertise within their organisations.

3 Smaller organisations demonstrated the lowest levels of maturity.

There was a clear relationship between revenue size and cyber security maturity. Considering that more than 65% of Australian NFPs recorded revenue under $1 million in FY22[1], immature cyber security may be pervasive across the sector.

FIGURE 2: Relationship between organisations gross income and cyber maturity score (calculated out of 100).

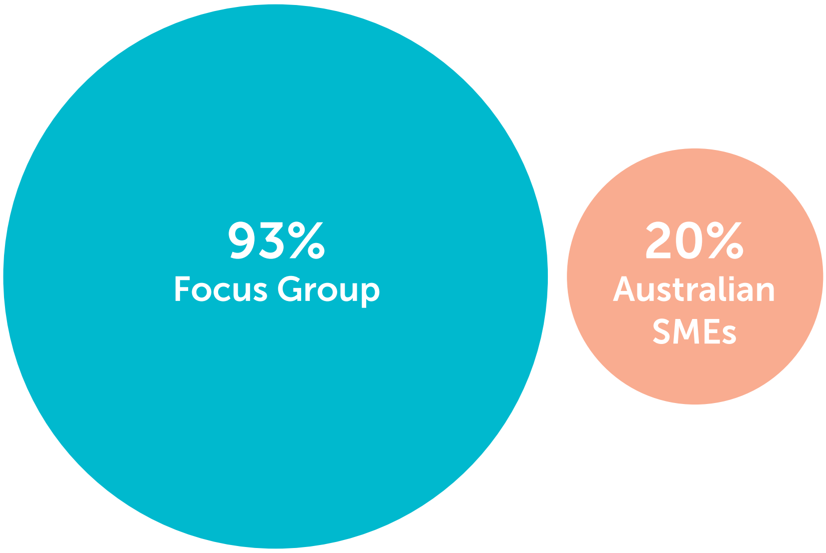


[1] Australian Charities Report – 10th Edition, https://www.acnc.gov.au/tools/reports/australian-charities-report-10th-edition, p. 17.

4 There is excessive reliance on cyber insurance.

93% of the assessed organisations had taken out cyber insurance. In contrast, only 20% of Australian Small and Medium Enterprises have cyber insurance. Feedback from respondents indicated an over reliance on transferring risk into cyber insurance and an under reliance on implementing processes and technologies to prevent cyber risks from materialising.

FIGURE 3: Percentage of focus group respondents who rely on cyber insurance, compared to that of Australian Small and Medium Enterprises



5 There is excessive and misplaced reliance on managed service providers and software vendors to manage cyber security.

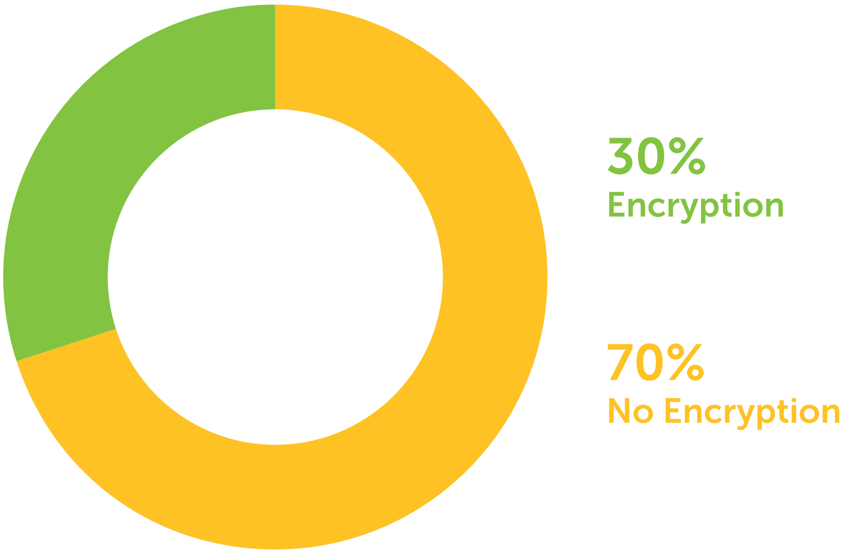
Many organisations referenced their IT managed service provider when asked about the presence and effectiveness of operational processes like third-party risk management and business continuity. 64% of the focus group had not conducted due diligence on their supply chain including vendor cloud hosted systems.

6 Most organisations have not effectively implemented basic operational and technological controls, let alone more sophisticated approaches to manage cyber security.

Only 43% of organisations had implemented effective password management practices and cyber security awareness training. Very few (29%) had implemented more sophisticated controls such as data encryption and restrictive firewall rule configurations.

It should be noted that there were often valiant efforts to secure each organisation's digital infrastructure. Despite this, the issues outlined above leave many of these organisations vulnerable to exploitation. There are tangible strategies that organisations can implement to significantly reduce their exposure to these risk findings, as detailed later in this report.

FIGURE4: 70% of organisations from the focus group responded that they do not use encryption to protect the confidentiality of sensitive data



Risks and Implications

Potential implications of these governance, control and process gaps are significant. This is especially true when considering the sensitivity of the data that the sector is storing and processing on behalf of the people they support, and the NSW Government. All the organisations in the focus group collect large volumes of sensitive personal and health information, as well as card transaction and financial data. Services range from aged care, disability support and family housing, to sexual abuse and domestic violence services.

When considering that the data of each organisation represent the most vulnerable and disadvantaged in the NSW community, the impact of a data breach at any of these organisations is substantial. A breach could have significant impacts on an individual's physical and psychological safety, as well as on an organisation's reputation, and legal and regulatory compliance. Moreover, consistent systemic breaches in the NFP sector could erode the confidence that society places in organisations as providers of quality and trusted services to people living in poverty and disadvantage. Any such erosion of trust would place pressure on the government to resume direct service delivery; this would have significant cost implications for the NSW state budget.

Recommendations

To effectively safeguard these organisations and the people they serve from further harm, WorkVentures recommends the following:

NSW Government:

1 The NSW Government should commit to a program of community service organisation cyber assessments, to identify key risks across operational, legal and regulatory, systems, and network domains. The assessments should be interview-based and involve multiple layers of the organisation, including senior executives, technical systems owners, staff responsible for risk management, and frontline workers, to provide visibility into both policy and practice across the organisation. This could be offered to all NFPs; targeted at smaller organisations; or focus on organisations working with highly sensitive data such as domestic and family violence supports.

2 Increase ongoing core funding to NFP organisations to improve their capacity to implement effective cyber security controls.

3 The NSW Government should investigate how it can utilise its own existing infrastructure and expertise to support the sector (e.g. shared cybersecurity training).

Community Service Sector Organisations:

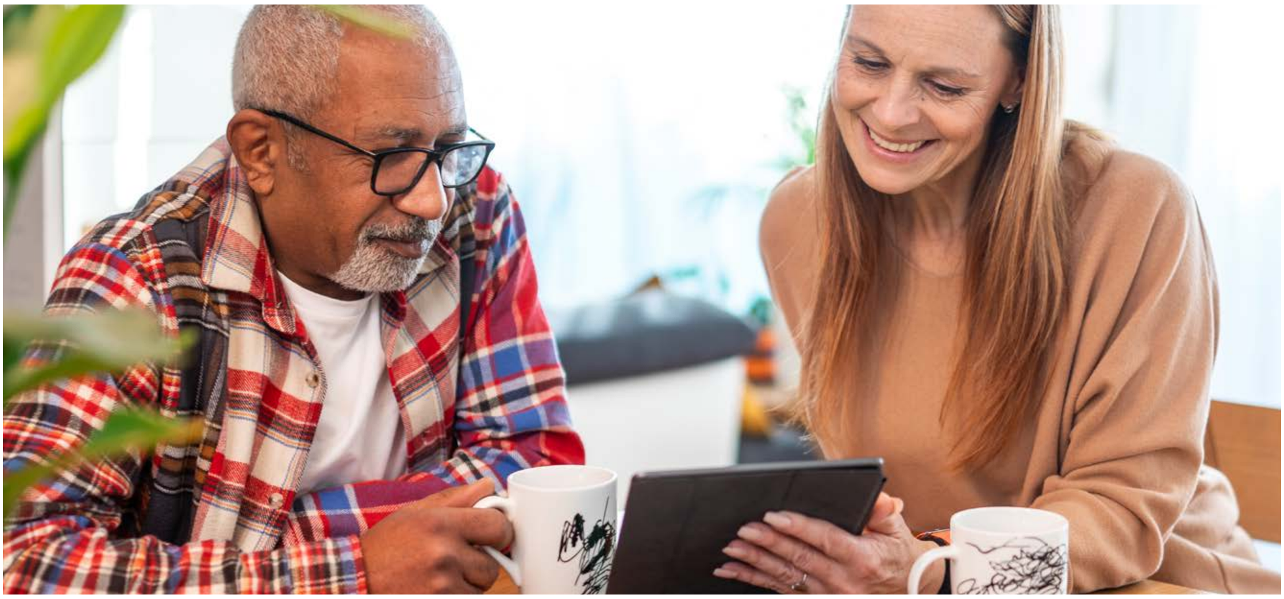
4 NFPs should ensure they implement foundational, low-cost options to bolster their cyber security. This includes the enforcement of long and unique passphrases, multifactor authentication, cyber security awareness training, regular application and operating system updates, and backups of critical data.

NFPs will need additional funding from government to address more complex ongoing challenges, such as vulnerability scanning and penetration testing, the establishment of a robust incident response plan and procedure, and third-party risk management.

Australian Government:

5 A national cyber security standard to be established for NFPs that goes beyond the scope of the proposed cyber health check, provides full coverage and is achievable for organisations that have limited resources and access to cyber security expertise.

The absence of a specific NFP cyber security strategy from the federal government or mention of the sector within the 2023-2030 Australian Cyber Security Strategy heightens the need for the above measures to be put in place.



Context – Cyber Security and the Australian NFP Sector

Community service sector organisations in NSW – and Australia generally – face disproportionate challenges when it comes to securing their digital infrastructure. This is largely due to limited resources and expertise, the sensitivity of data they hold, and the increasing sophistication and targeted nature of cyber threats. This is particularly concerning against a backdrop of increasing incidence and sophistication of cybercrime.

This risk has been recognised by the Australian Charities and Not-for-profits Commission (ACNC). In March 2024, the ACNC announced[2] that cyber would be a key compliance focus for the ACNC in 2024-25, including reviewing how charities manage and mitigate cyber security risks, and how charities ensure third parties manage risk on their behalf. To support the sector, the ACNC developed a Governance Toolkit on cyber security, using advice from the Australian Signals Directorate.[3] It includes some basic governance templates and outlines the legal obligations of charities in relation to notifiable data breaches.[3]

The risk exposure has also been highlighted by the Australian Cyber Security Centre (ACSC), part of the Australian Signals Directorate. In May 2024, Jacqui Barr, Assistant Director-General Technical Threats and Visibility at the Australian Cyber Security Centre, warned that charity leaders should review cyber security measures to avoid becoming an "easy target" for cyber criminals[4]. The ACSC particularly highlights phishing, business email compromise, and ransomware as key threats to NFPs[5].

[2] https://www.acnc.gov.au/media/news/acnc-2024-25-compliance-focus-misuse-complex-corporate-structures-and-cyber-security-challenges

[3] https://www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-toolkit/governance-toolkit-cyber-security

[4] https://www.acnc.gov.au/media/news/dont-be-easy-target-australias-lead-cyber-security-agency-latest-charity-chat-podcast

[5] https://www.cyber.gov.au/protect-yourself/staying-secure-online/cyber-security-for-charities-and-not-for-profits

Approach and methodology

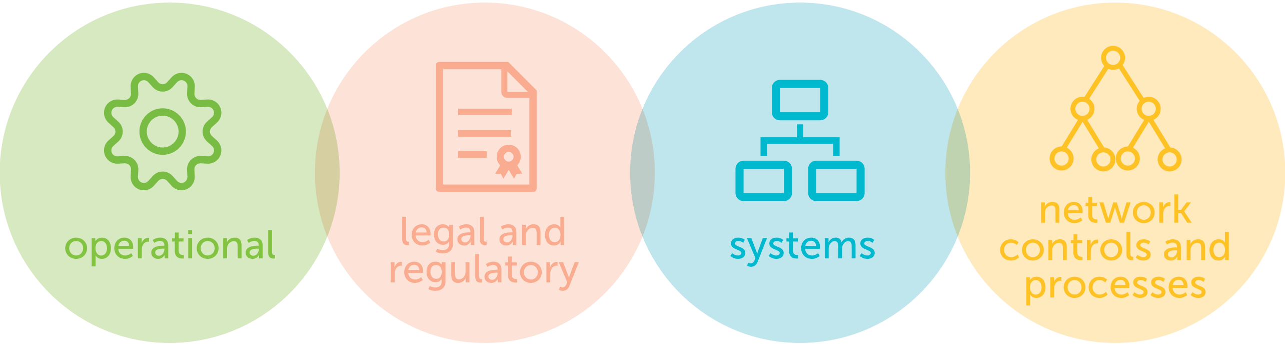
WorkVentures approach to understanding the risk profile of the sector takes a truly unique approach when examining similar cohort-based studies. It was observed that similar studies had not solely focused on cyber security for NFPs and had largely derived findings from self-reporting against a survey-style assessment.

Our approach involved up to 4 hours of workshopping and presenting ideas to stakeholders from each organisation, ranging from field staff to senior executives, to ascertain a holistic understanding of the risk profile and provide a tailored set of recommendations. Having spent approximately 50 hours of interaction with organisations within the focus group, we were able to discuss each question including the definitions and thresholds for what would be considered a 'yes' or 'no' response. This allowed us to understand the risk at a very granular level.

Each organisation was scored out of 25 across four domains, covering operational, legal and regulatory, systems, and network controls and processes, with a final score given out of 100. The baseline for a mature standard is achieved by scoring at least 20 points in each category, with a minimum total score of 80. None of the organisations from the focus group met the baseline for a mature standard, with scores ranging from 44 to 73.

A target maturity score of 80 has been established in consideration of the Law of Diminishing Returns. As an organisation increases its cyber security maturity, the effort and resources required to achieved additional improvement also increases. Reaching a point beyond 80 will result in higher costs with less proportionate benefit. The target maturity score represents a well-rounded and optimised approach, which balances the need for strong cyber security controls with the resources required to achieve additional improvement.

Four domains



Findings

Vulnerability to Common Threats

The Australian not-for-profit sector plays a pivotal role in society and supports millions of disadvantaged people every year. The sector also faces common challenges that cause complexity when navigating the ever-evolving landscape of cyber security.

Throughout the course of the NCOSS cyber assessment project, it was overwhelmingly apparent that NFPs typically operate with limited budget and personnel and that most organisations experience pressure to direct funding back into core mission delivery, rather than cyber security measures. The most recent Australian Public Service Census highlights that 44% of workers in the NFP sector describe themselves as having a linguistically diverse background. The culture of low digital literacy and cyber hygiene and the considerable representation of linguistically diverse workers in the sector, combined with the volume and complexity of human-centric threats, means that NFPs are increasingly vulnerable to social engineering techniques like phishing.

Another challenge is that most of the organisations within the focus group operate remotely - from client sites or other locations. Several organisations reported that field staff are commonly required to access sensitive data from unmanaged personal devices, without utilising a virtual private network (VPN) to encrypt traffic over public wi-fi hotspots.

The Australian Cyber Security Centre (ACSC) particularly highlights phishing, business email compromise and ransomware as key cyber threats facing the not-for-profit sector. Alarmingly, some of the most prevalent deficiencies observed across the project increase the NFPs' vulnerability to these threats.

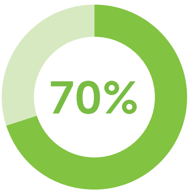
Phishing and Ransomware

Ransomware is a form of malware that locks or encrypts an organisation's files, preventing access. A ransom is then demanded by the attacker to restore access to the files.

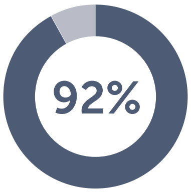
Phishing involves sending communications that trick recipients into thinking that it is from a legitimate source. This may be an email that purports to be from a bank, the organisation's CEO, or another trusted service provider. Phishing is typically how ransomware is delivered.

Common controls that can reduce the impact and likelihood of a phishing or ransomware attack include cyber security awareness training, antivirus scanning, restricting administrative privileges, application whitelisting and ensuring data backups are in place.

For the focus group organisations:



70% do not have a cyber security training program for all staff.



92% have not implemented application whitelisting.

CASE STUDY: Consequences of exposure to Ransomware

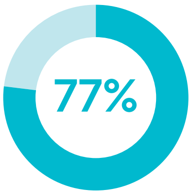
In April 2024, Australian immigration consultancy Aussizz Group fell victim to a ransomware attack that encrypted large amounts of company data, with the threat actor demanding a ransom for its decryption. Reports suggest that up to 300GB of sensitive data was exfiltrated from the organisation's network before being encrypted. This includes highly sensitive information such as pay slips, visa applications, scans of passports and other identity documents.

Business Email Compromise

Business Email Compromise (BEC) describes a technique used by attackers to deceive the target into transferring money or sensitive information. Attackers often impersonate executives, vendors, or trusted contacts to request fraudulent payments or confidential data.

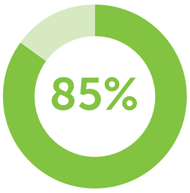
Common controls that reduce the likelihood of a business email compromise attack include employee training and awareness to identify red flags, robust access management, including strong and unique passwords and the consistent application of multi-factor authentication

(MFA), as well as internal controls to prevent fraud, such as requiring approvals for transfers over a certain threshold.

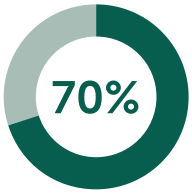


77% of the organisations have had employees' credentials compromised as part of recent data breaches.

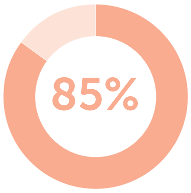
60% of the organisations whose employees' credentials had been leaked included those of senior executives.



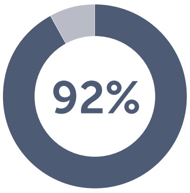
85% do not enforce frequent password rotation, increasing the likelihood that the compromised credentials are still being used.



70% do not use password managers, increasing the likelihood that the same compromised credentials are being used across multiple accounts.



More than half do not have federated accounts for domain management and so, although 85% of organisations in the focus group have provisions for password complexity, these standards are not being consistently enforced across all systems and applications.



Although 92% of respondents indicated that they have enabled multifactor authentication (MFA) across systems, this typically applied to the organisations Microsoft Office 365 environment and was not consistently applied across all critical systems.

Network Compromise

Network compromise occurs when an attacker gains access to an organisation's network, potentially allowing unauthorised access to and exfiltration of sensitive data outside the network, or the deployment of malicious software.

Common tools and controls to prevent network compromise include restrictive firewall configurations, disabling unnecessary ports and protocols, keeping all operating systems, applications and firmware updated and ensuring encryption of data on systems and services interfacing with the public internet.

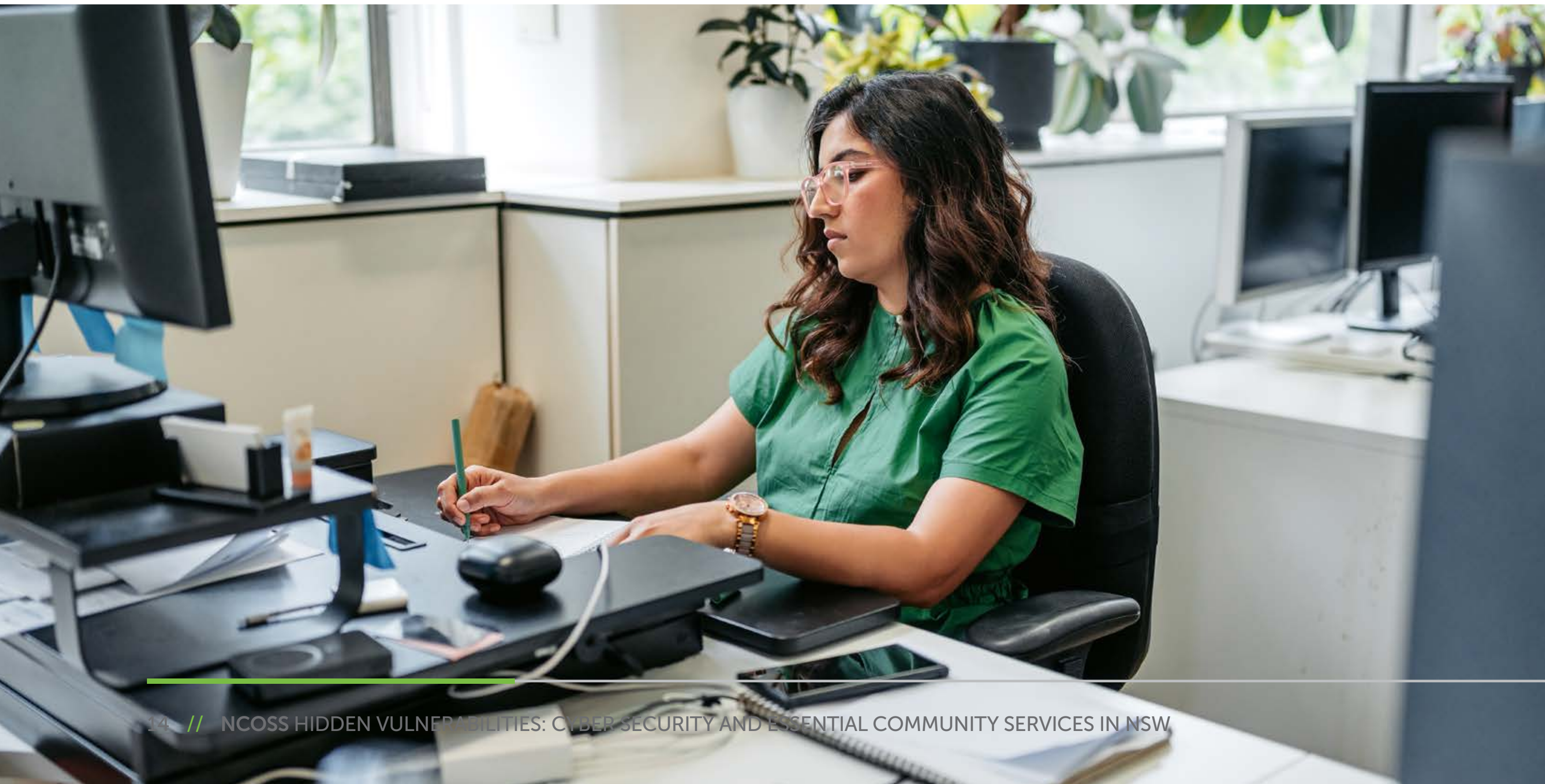
Most focus group organisations have not configured restrictive firewall rules, have not disabled all unnecessary network ports and protocols and an alarming number of organisations were using outdated encryption standards for securing data processed and stored on public facing systems.

Only 23% of organisations from the focus group have a system for encrypting data and even less utilise public key cryptography for email communications.

The above examples are typically low- or no-cost solutions that can often be implemented by an IT manager or external IT provider, given the right instruction.

CASE STUDY:
Consequences of exposure to Network Compromise

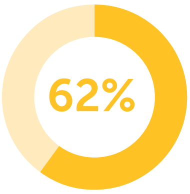
In May 2024, Western Sydney University was involved in a cyber-attack that resulted from a threat actor gaining unauthorised access to the university's IT network. The attacker was able to access the Microsoft Office 365 tenant and gain access to SharePoint files that contained student names, identification numbers, date of birth, email address, phone numbers and citizenship status.



Supply Chain Attacks:

A supply chain attack occurs when an attacker exploits a vulnerability in a third-party software, or service to gain unauthorised access to an organisation's systems or data.

Common strategies and controls to reduce the impact and likelihood of supply chain attacks include conducting third-party risk management activities, including minimum security requirements in vendor service agreements to ensure oversight and accountability and to enforce strong access management practices, including the implementation of federated identity to enable single sign-on and multifactor authentication.



62% of organisations had not conducted any form of due diligence on their supply chain, despite all the focus group being either entirely migrated, or in the process of migrating to cloud-based infrastructure and utilising a host of software-as-a-service (SaaS) applications.

50% of organisations have not enabled domain management and/or single sign-on to their Microsoft environment, with almost none federating identity services with other vendor SaaS applications.

CASE STUDY:
Consequences of exposure to Supply Chain Attacks

The 2024 ZircoDATA data breach, initiated from a ransomware attack, compromised the sensitive data of approximately 200 Australian organisations, including Monash Health, a government department, and a legal translation service. Data compromised included personally identifiable information, visa and passport information, financial records, and confidential documents. Monash Health saw records from its family violence and sexual assault support units compromised, affecting around 4,000 clients. The breach exposed the personal information of thousands, including vulnerable individuals, students, and Australian visa holders.

Insider Threat

An insider threat is a security risk posed by individuals within an organisation, such as employees, contractors, or business partners who either intentionally or unintentionally misuse their authorised access to systems or data for malicious purposes.

Common strategies and controls to reduce the impact and likelihood of insider threats include implementing data loss prevention (DLP) controls such as disabling removeable storage media permissions on laptops and blacklisting unapproved email and file share platforms, stringent access controls utilising the principle of least privilege and enabling audit logging and monitoring across systems.

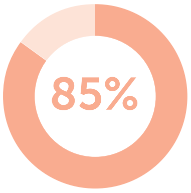
Most organisations do not have strategies or software in place to prevent data exfiltration and no defined processes or controls to monitor external parties, such as contractors or cleaners in their premises (64%).

CASE STUDY: CONSEQUENCES OF EXPOSURE TO INSIDER THREATS

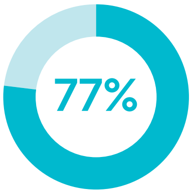
Westpac Bank faced a significant breach of customer privacy when a former relationship manager handed over banking credentials for 80 customer accounts to a mortgage broker. This insider threat incident involved resetting passwords and sharing temporary access credentials inappropriately.

Existing Strengths

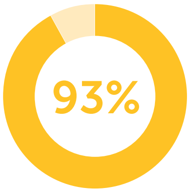
Despite the considerable number of deficiencies across the focus group there were notable positives to highlight, including:



All organisations have data backups, 85% have tested backup and restore procedures



77% have a formalised disaster recovery plan



93% have conducted criminal history checks on all employees.

Additionally, all organisations have:

- ✓ Processes in place to remove unused or inactive users
- ✓ Anti-virus scanning that includes ransomware detection
- ✓ Configured WPA2 as a minimum for all wi-fi routers
- ✓ Confirmed that any payments utilise a PCI-DSS compliant payment gateway

Compliance and Regulatory Considerations

The organisations within the scope of this project offer an array of services that involve the collection of sensitive personal information from a range of communities, including those with a disability, children, domestic and sexual violence survivors and the elderly.

Although the most strongly regulated organisation in the focus group achieved the highest cyber maturity score, there does not appear to be a correlation between regulation and cyber security maturity. This is highlighted by other heavily regulated organisations who provide a breadth of services achieving a cyber maturity score in the lower quartile of the focus group. A conclusion that could be drawn from this is that regulation alone is not sufficient to enforce cyber maturity, and further supports are required to enable change.

Another vector examined was the relationship between annual revenue and cyber maturity. The data suggests that as annual revenue increases, so does cyber maturity. A plausible hypothesis is that larger, better-funded organisations tend to have more mature systems and processes, along with budgets for essential functions like cyber security. However, there were two outliers in the sample that did not follow this trend.

Noting that no organisation in the sample achieved the benchmark for a mature standard, this underscores the need for clearer regulation and standards, and targeted funding to help align with regulatory requirements. Given the clustering of maturity scores, the level of targeted funding should be scaled according to annual revenue.

Bridging the Gap

So, what can be done to uplift Australian not-for-profit organisations to achieve cyber security maturity?

Firstly, we need to establish what cyber security maturity should look like for the sector.

As a not-for-profit, WorkVentures is aware of the challenges and barriers to entry facing organisations in the focus group and specifically as they relate to cyber security. Resourcing barriers is one of the most cited reasons for NFPs to not take reasonable steps in mitigating cyber risk and so, more needs to be done to provide equal access to services and funding that addresses this issue. Cyber security needs to be directly aligned with each organisation's mission, and governance needs to be put in place to define key roles and responsibilities as they relate to cyber. An organisation's leadership must incorporate cyber security into broader organisational discussions around strategy, risk management and funding to ensure that enough money is invested into mitigating risks that could materialise in significant disruptions to their mission.

A risk-based approach needs to be adopted to prioritise safeguards against threats that could result in a considerable impact to the organisation and that are likely to materialise. This project has highlighted the desperate need to prioritise cyber security awareness and training, strong authentication and credential management, network defence-in-depth, data loss prevention, encryption and cyber governance controls and processes. This will effectively reduce the NFP sector's risk exposure to prevalent threats and ensure that organisations can remain steadfast in their mission to serve disadvantaged Australians.

To adopt a risk-based approach, NFPs require a cyber security standard that provides holistic coverage against common threats, is highly prescriptive, and not resource intensive, so that non-technical stakeholders can interpret and implement it. The Australian Cyber Security Centre's Essential Eight provides a highly prescriptive framework for organisations to easily interpret and implement technological controls, however, it does not provide holistic coverage against the ACSC's identified common threats.

Conversely, other established cyber security standards such as ISO/IEC 27001 and NIST SP 800-53 can both provide holistic coverage against common threats, although are less prescriptive and often very abstract, and require expertise and considerable resources to implement.

> *"Cyber security needs to be directly aligned with each organisation's mission, and governance needs to be put in place to define key roles and responsibilities as they relate to cyber."*

WorkVentures recommend the establishment of a sector-specific national cyber security standard to bridge the gap for NFPs to effectively manage cyber risk. The scope of this standard would cover systems and network controls but would also extend beyond the bounds of technology and recommend relevant operational and legal and regulatory processes. It would also place a strong focus on mitigating key threats to the NFP sector by prioritising areas that were commonly identified as gaps from this project, including:

- CYBER GOVERNANCE
- ENCRYPTION
- Third-party risk management
- DATA LOSS PREVENTION
- Incident response
- IDENTITY AND ACCESS MANAGEMENT
- *Legal & regulatory considerations*
- *TRAINING AND AWARENESS*
- Bring Your Own Device (BYOD) best practices
- Network defence-in-depth

The Small Business Cyber Resilience Service program is projected to provide significant aid to small and medium businesses through assistance in developing a tailored plan to improve their cyber security, as well as risk-based recommendations and guidance on incident response. The resilience component of this service is set to rely on existing whole of government guidance, such as the Essential Eight and a cyber security health check delivered by the Department of Home Affairs.

The program requirements have been built around tailoring a service and understanding the needs of small to medium enterprises (SME's); however, not-for-profits experience a unique set of cyber security challenges that set them apart from other SME's. These unique challenges include a high dependency on volunteers and temporary staff, high levels of cultural and language diversity, as well as the fact that NFPs handle highly sensitive data and are often targeted due to the transparent nature of their operations.

To shape these services to best benefit NFPs, a reliance on holistic standards, such as the Centre for Internet Security (CIS) Controls framework and other emerging standards including the Dynamic Standards International's SMB1001:2025 should be prioritised over narrow and prescriptive frameworks like the Essential Eight.

Based on the above, WorkVentures recommends targeted funding to be directed into providing NFPs with a tailored cyber security assessment and uplift program that considers the controls and processes that were noted as common deficiencies throughout the project. This should be achieved by establishing a dedicated program that integrates expertise in working across all levels of NFPs, from the board to the front lines, to drive sustained technical, operational and cultural change.

Conclusion

This project has identified critical exposure to prevalent threats within the sector, emphasising the urgent need for targeted funding to support not-for-profits to uplift their cyber security posture.

From the results of the focus group, it was evident that the sector requires significant uplift, specifically around staff training and awareness, authentication and credential management, network defence-in-depth, data loss prevention, encryption and broader cyber governance. Despite the noted deficiencies across the participating organisations, there were many positive points to have also come out of this project, including high responsiveness to the need for uplift, as well as relative maturity around disaster recovery, anti-virus scanning, wi-fi encryption and security around donor payments.

The establishment of a sector-specific national cyber security standard and targeted funding directed into providing NFPs with a holistic cyber assessment program would provide a strong foundation for organisations to achieve and maintain resilience against critical threats. By advocating for these initiatives, stakeholders can not only safeguard the business operations and mission of Australian not-for-profit organisations, but also the communities that they serve.

Appendix

Below is the tabular data from all 14 organisations across the NCOSS cyber assessment project, broken down into operational, legal and regulatory, systems and network questions.

Operational

Question	Yes	No	N/A
Have you ever undertaken a security risk assessment?	5	9	0
Do you have a written security plan?	4	10	0
Do you have written security policies, procedure, guidelines, and standards, or use those specified by standards bodies (like NIST or ISO-27001), by vendors (like Cisco), or industry (like PCI-DSS)?	9	5	
Is there compliance with the plan, policies, procedure, guidelines and standards?	7	4	3
Have you adopted any approach to gain assurance for cyber security?	9	5	0
Do you have a designated cyber security officer who can provide expert guidance, and who is empowered to make enforceable security decision?	8	6	0
Have you ever undertaken a security and/or a data audit?	5	9	0
Do you implement all the recommendations arising from security audits?	5	1	8
Do you have a disaster recovery plan?	10	4	0
Have you ever tested your disaster recovery plan?	6	6	2
Do you have agreements and/or infrastructure in place to support a cold site or hot site?	11	3	0
Do you conduct criminal history checks on all employees?	13	1	0
Are cleaners, contractors and visitors always supervised in your building?	5	9	0
Do you have strategies and/or software in place to prevent data exfiltration?	5	9	0
Do you have processes in place to detect malicious or unauthorized activity?	14	0	0

Do you have an incident response process in place, including communications?	7	7	0
Do you have the capacity to undertake a cyber investigation, including forensics, if your systems and networks are compromised?	7	7	0
Do you have a cyber security awareness programme for all staff?	5	9	0
Do you have a cyber security training programme for all staff?	5	9	0
Have staff been evaluated for their likelihood to disclose sensitive information?	7	7	0
Have you taken out cyber insurance?	13	1	0
Have you ever undertaken a Red Team activity or had a penetration test?	4	9	0
Do you have processes to identify and remove unused or inactive users?	14	0	0
Have you enabled logging of event data across devices, systems and networks, and is this data monitored?	12	2	0
Have you created a risk-rated inventory of all systems, networks and data owned by your organization?	3	11	0

Legal & Regulatory

Question	Yes	No	N/A
Have you conducted due diligence on all entities in your supply chain?	5	9	0
Have you registered all your intellectual property in an appropriate way?	3	10	1
Do you actively search online for intellectual property breaches?	2	12	0
Do you issue takedown notices under the Digital Millennium Copyright Act (1998) or similar legislation where appropriate?	0	12	2
Do you monitor your employees' activity to detect illegal activity which could leave you liable, including the Criminal Code Act 1995?	4	10	0
Do you know if your business is subject to the Privacy Act 1988?	14	0	0

Have you implemented sufficient controls to comply with the Australian Privacy Principles?	10	4	0
Do your policies, procedures, guidelines and standards ensure compliance with the Cybercrime Act 2001?	2	8	4
Is your digital marketing compliant with the Spam Act 2003?	7	2	5
Are your telecommunications practices consistent with the Telecommunications (Interception and Access) Act?	7	0	7
If you process credit card payments, are you compliant with PCI-DSS?	11	0	3
Do you know if you are required to report notifiable data breaches to the Office of the Information Commissioner (OAIC)?	9	5	0
Are you compliant with the surveillance, telecommunications, cyberbullying, information and privacy protection Acts in your state(s) of registration and/or operation?	8	6	0
If you offer financial services, are you compliant with CPG-235, PPG-234, RG-104.93 and RG-104.96?	0	0	14
If you are a director, are you aware of your obligations under the Corporations Act as they relate to cyber security?	9	5	0
If you are you an ISP, are you retaining customer data as per the Data Retention amendments to the Telecommunications (Interception & Access) Act?	0	0	14
Do you have any controls or systems in place to detect fraud?	14	0	0
Do you report any suspected cybercrime activity using ReportCyber?	4	10	0
If you sell to or deal with international suppliers or customers, are you aware of the cybercrime laws in their countries that might impact you, such as China's Cybercrime Law?	2	7	5
Are you aware whether you are required to comply with cross-border data flow rules, such as Safe Harbor provisions or EU Binding Corporate Rules?	1	4	9
Do you know if you have obligations to remove material that contravenes the provisions of the Online Safety for Children Bill 2014?	10	1	3
Are you aware if you have obligations to report under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006?	2	1	11

If you sell or provide services to customers within the European Union, are you compliant with the General Data Protection Regulation (GDPR)?	0	3	11
Are you aware of the physical location of your cloud data and applications?	13	1	0
Are you aware of, and compliant with, the data protection and/or state security laws of the countries where your cloud data and applications are hosted?	6	6	2

Technology - Systems

Question	Yes	No	N/A
Does every system or device have up-to-date anti-virus protection, including ransomware detection?	14	0	0
Are all your systems password protected?	14	0	0
Do you enforce password expiry of 3 months or less?	2	12	0
Do you enforce standards for password complexity?	11	3	0
Do you use password managers?	4	10	0
Have you enabled two-factor authentication to access critical systems and data?	13	1	0
Have you setup appropriate groups to support access control, based on the principles of “least privilege” and “separation of duties”?	13	1	0
Are your users forced to use access control?	13	1	0
Do you have a Standard Operating Environment (SOE)? With the most secure baseline?	12	2	0
Do you protect the Master Boot Record (MBR) of each system?	7	7	0
Do you force BYOD devices to have the same technical controls as company-owned systems?	4	4	6
Do you have a system for encrypting data (files, databases etc) and removeable devices, such as USB memory sticks?	4	10	0
Do you use public key cryptography for emails?	3	11	0

Are all of your operating systems and applications patched and up to date?	12	2	0
Do you backup your data and applications?	14	0	0
Have you ever tried to restore data and applications and verify that everything operates as expected?	12	2	0
Have you disabled all unnecessary network ports, protocols and services on all systems?	6	8	0
Have you changed all default passwords on all systems and hardware devices?	12	2	0
Have you allocated administrative (or "root") privileges appropriately and proportionately?	14	0	0
Have you disabled local administrator accounts on PCs?	11	3	0
Have you implemented application whitelisting?	1	13	0
Do you use cryptography to protect the confidentiality of sensitive data?	4	10	0
Do you block access to untrusted macros in Microsoft Office products?	12	2	0
Have you enabled domain management and/or single sign-on?	7	7	0
Have you enabled Data Execution Prevention (DEP) and Address Space Layout Randomisation (ASLR)?	5	9	0

Technology – Network

Question	Yes	No	N/A
Do you have a network firewall?	13	1	0
Is your firewall configured with the most restrictive set of rules possible?	4	10	0
Do you use non-routable IP addresses behind the firewall?	10	4	0
Do all your systems have their own firewall with appropriate rules?	13	1	0
Have you enabled IPv6 and/or IPSec?	6	8	0
Do you have an Intrusion Detection System (IDS)?	9	5	0

Do you have an Intrusion Prevention System (IPS)?	8	6	0
Have you designed and deployed a honeypot?	1	13	0
Are your hosted applications vulnerable to SQL-injection or cross-site scripting attacks?	5	7	2
Do you have a bandwidth manager to limit the impact of DDoS attacks?	6	7	1
Have you implemented blackholing and sinkholing to deflect malicious traffic?	2	11	1
Do you use an upstream or web content filtering service?	6	8	0
Have you disabled all non-TLS services on public-facing interfaces?	8	5	1
Do all Wi-Fi routers have a minimum of WPA2 authentication?	14	0	0
Have all applications been developed using secure coding practices?	4	7	3
Have all applications been tested for vulnerabilities, including checks for buffer overflows?	2	8	4
Have you enabled the most restrictive configurations for systems, networks, and devices where available?	8	6	0
Have you changed all default passwords on all databases and applications?	11	3	0
Do you log all network events and actively check for intrusions?	7	7	0
Have you customised error pages on all web pages to prevent stack trace displays and disclosure of sensitive information, such as physical filesystem paths and source code vulnerabilities?	5	7	2
Have you checked all configuration files to make them as restrictive as possible?	4	10	0
Do you understand what security controls your cloud provider has in place, and what you are responsible for?	11	1	2
Does your cloud provider restrict outbound traffic?	6	6	2
Have you restricted SSH and/or Remote Desktop access in your cloud environment?	9	2	3
Does your cloud provider have physical access to your encryption keys?	7	4	3

Glossary

Term	Definition
Application whitelisting	A defined list of applications that are approved to run on a system.
Business email compromise	A malicious email appearing to come from a known source such as a vendor or colleague, making a legitimate request, usually requesting the transfer of funds into the adversary's account.
Data encryption	The process of transforming readable data into an unreadable form to mask sensitive information from unauthorised access.
Multifactor authentication	A method of confirming a user's identity with a username, password and an additional factor, such as a one-time password generated by the user's device, or a biometric scan of the users face or fingerprint.
Passphrases	A sentence like string of words used to identify a user that is longer than a traditional password and easier to remember.
Penetration testing	An exercise involving a cyber security professional attempting to find and exploit vulnerabilities in a computer system or network.
Phishing	A type of cyber attack that seeks to deceive the target into revealing sensitive information by appearing as legitimate communications, typically sent through email or SMS.
Ransomware	A type of malicious software that is typically delivered via phishing and aims to deceive the user into executing a file that encrypts the files on their device, rendering them inaccessible. The attacker threatens to either keep the data encrypted or publish it publicly unless a ransom is paid.
Social engineering	A cyber threat that leverages deceptive tactics to manipulate individuals into gaining access to sensitive information, systems and sending fraudulent transactions.
Virtual private network	A technology that creates a secure and encrypted connection over an otherwise less secure network, such as a public wireless access point.
Vulnerability scanning	The process of deploying a software to scan a network or system for security vulnerabilities that could be exploited by an attacker.

Hidden Vulnerabilities:

Cyber Security and Essential Community Services in NSW

NCOSS
NSW Council of Social Service

WorkVentures
social inclusion through technology