NCOSS
NSW Council of Social Service

Hidden Vulnerabilities:
Cyber Security and Essential Community Services in NSW

Not-for-profit (NFP) organisations in Australia help millions of people in need every year. However, they struggle to keep their network and systems secure as they do not have enough funding or expertise to protect them from cyber threats, which are increasingly targeted and persistent.

In 2024, New South Wales Council of Social Service (NCOSS) teamed up with WorkVentures to assess the cyber security of 14 NFPs in NSW. The goal was to identify common challenges, weak spots, and ways to help these organisations better protect their data.

Key Findings

The assessments highlight the risk exposure of the NFP community services sector.

Weak Cyber security Maturity

All participating organisations had concerningly low levels of cyber security maturity. None of the organisations met the assessed minimum benchmark across operational, legal and regulatory, systems, and network controls and processes.

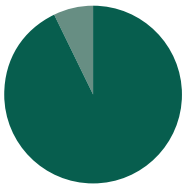
Good Intent but Limited Resources

All organisations recognised the importance of cyber security and wanted to improve, but do not have the resources to respond effectively. Organisations consistently reported that they struggled to fund the necessary investments in systems and could not afford to recruit sufficient cyber security expertise.

Smaller Organisations Are Most at Risk

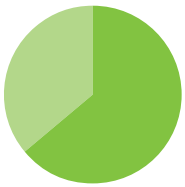
Larger organisations tended to have stronger cyber security, while smaller ones were less prepared. Since 65% of Australian NFPs had revenue under $1 million in 2022, weak cybersecurity is likely a widespread issue in the sector.

Scan for full report



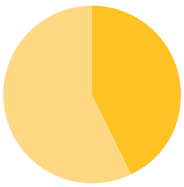
Over-Reliance on Cyber Insurance

Most organisations (93%) had cyber insurance, compared to only 20% of Australian small and medium businesses. While this is not necessarily a negative, many relied too heavily on insurance instead of sufficiently investing in strong cyber security processes and technology to mitigate the risk of an incident occurring.



Too Much Trust in External IT Providers

Alongside the transfer of risk into cyber insurance, many organisations (64%) had not conducted any form of due diligence on their critical cloud-based software vendors or IT managed service providers.



Basic Cyber Security Measures Are Lacking

Most organisations had not effectively implemented basic cyber security controls, let alone more sophisticated safeguards. Fewer than half (43%) of organisations had implemented effective password management and cyber security awareness training. Even fewer (29%) had implemented more sophisticated controls such as data encryption and restrictive firewall rule configurations.

Risks and Implications

If a cyber security incident or data breach materialised in these organisations, it could result in serious harm to vulnerable people, damage the organisations reputation, or lead to considerable operational disruption. Repeated breaches in the NFP sector could erode public trust and the sustainability of the system, forcing the government to take over services and absorb significant additional cost.

Recommendations

NSW Government should:

1. Commit to a program of community service organisation cyber assessments, to identify key risks and necessary responses.
2. Provide more funding to help NFPs improve their cybersecurity.
3. Use its own capabilities and experts to directly support the sector (e.g. shared cyber security training).

Community Service Sector Organisations should:

4. Take simple, low-cost steps to improve cyber security, such as strong passwords, multifactor authentication, cybersecurity training, regular software updates, and data backups.

Australian Government should:

5. Establish an achievable cybersecurity standard for NFPs that ensures that controls can be implemented with limited budget, whilst also providing sufficient risk mitigation against key threats.