COMMUNITY COUNCIL FOR AUSTRALIA

Department of Home Affairs

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Dear Consultation Team

We write expressing our serious concerns about cyber security risks to Australian charities and NFPs.

Every organisation in Australia is aware of the growing threat posed by bad actors seeking to exploit illegal access to information.

For businesses, including SMEs, your government has provided various programs and incentives to promote better data security and preparedness. Most of these incentives are in the form of tax concessions and grants (e.g. The Cyber Security Business Connect and Protect Program, the Cyber Wardens program for small business).

The 2023 - 2030 Australian Cyber Security Strategy discussion paper does not mention charities, not-for-profits, or community organisations, although it specifically mentions business 12 times and SMEs twice.

Governments across Australia do not always recognise the size and nature of the charities and not-for-profit sector. Charities alone employ over 1.3 million workers or 10.5% of the Australian workforce, and contribute over 5% to GDP in our annual turnover of $190 billion. Perhaps more importantly in the context of cybersecurity, charities hold extensive personal and financial information from millions of Australians.

Despite this massive footprint in our economy and in our lives, charities and not-for-profits have not been provided with the support they need to deal with an increasingly sophisticated level of cyber-attacks. Unlike business, charities spend every spare dollar they can find on serving their communities. Allocating more resources to strengthen cyber security would mean reducing the level of services available in our communities. Many charities and NFPs struggle to withdraw services, even though cybersecurity is clearly an important priority.

ABN: 76 141 705 599 | [redacted]
Contact: [redacted] **P:** [redacted] | **M:** [redacted] | **F:** [redacted]
E: [redacted]

There are ongoing and will be further cyber-attacks on charities and there is real potential for certain kinds of attacks to significantly damage confidence and trust in our sector. Cyber-attacks in our sector could also have devastating impacts on individuals and communities.

We ask that you consider providing increased support for charities across Australia to be able to review their current cybersecurity preparedness and to invest in better data security and protection. This is no more than what your government is already providing to business.

Leaving charities to fend for themselves in dealing with the threat posed by global cyber-security attacks is not an acceptable policy approach.

We strongly support and endorse the submission attached to this cover note from our expert CCA member Infoxchange.

Yours sincerely

Chair, Community Council for Australia

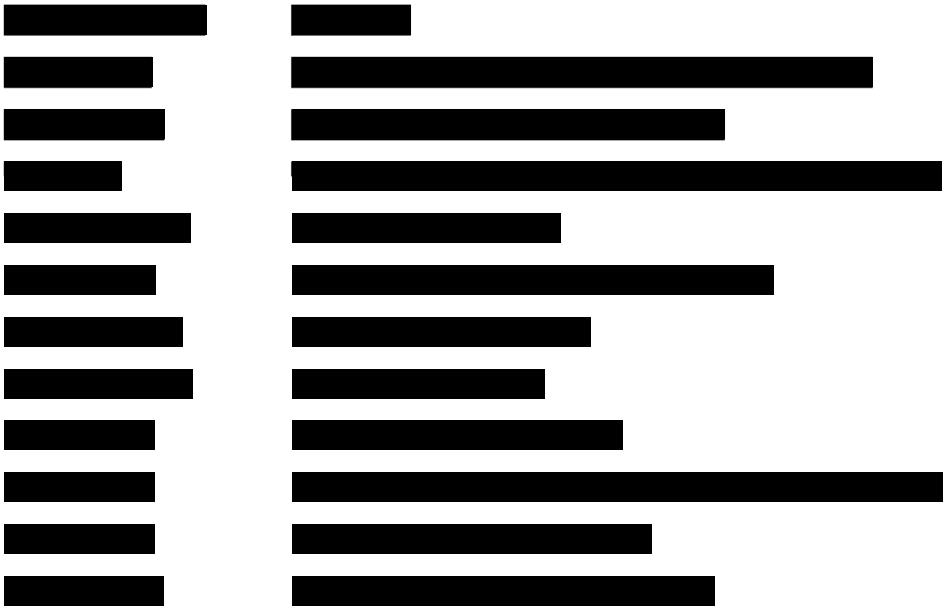
22nd of August 2025

CEO, Community Council for Australia

22nd of August 2025

ABN: 76 141 705 599 | [redacted]
Contact: [redacted] **P:** [redacted] | **M:** [redacted] | **F:** [redacted]
E: [redacted]

Community Council for Australia Board of Directors 2023



About CCA

The Community Council for Australia is an independent non-political member-based organisation dedicated to building flourishing communities by enhancing the extraordinary work undertaken by the charities and not-for-profit sector in Australia. CCA seeks to change the way governments, communities and not-for-profits relate to one another. It does so by providing a national voice and facilitation for sector leaders to act on common and shared issues affecting the contribution, performance and viability of NFPs in Australia. This includes:

- promoting the values of the sector and the need for reform
- influencing and shaping relevant policy agendas
- improving the way people invest in the sector
- measuring and reporting success in a way that clearly articulates value
- building collaboration and sector efficiency
- informing, educating, and assisting organisations to build sustainable futures
- providing a catalyst for the sector to work in partnership with government, business and the broader Australian community to achieve positive change.

Our success will drive a more sustainable and effective charities and not-for-profit sector in Australia making an increased contribution to the well-being and resilience of all our communities.

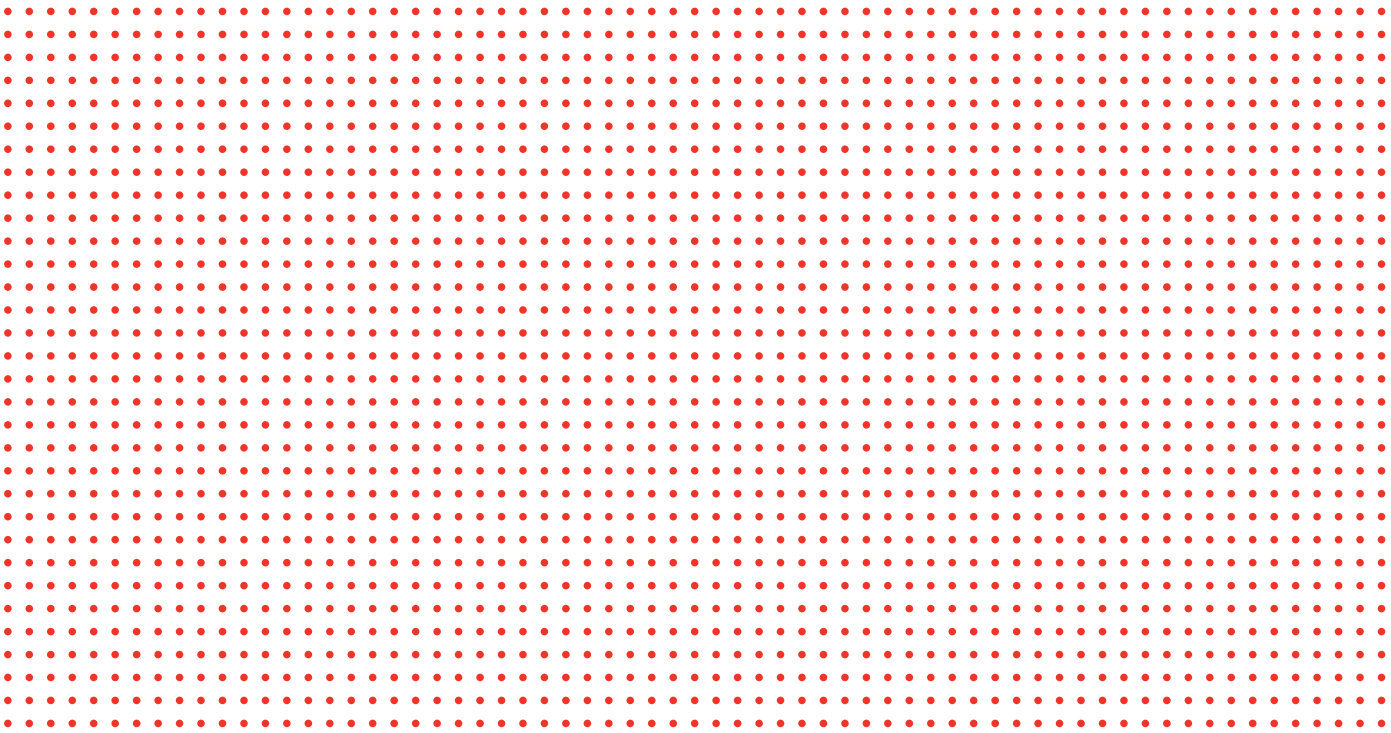
Infoxchange

Australian Government
Department of Home Affairs

Infoxchange Submission

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Department of Home Affairs | 21 August 2025



Contents

1. Executive Summary 1
2. Emerging Trends & Strategic Factors 2
3. Targeting & Consolidating Cyber Awareness 2
4. Successful Programs to Scale Up 3
5. Encouraging Uptake of Cyber Resources 4
6. Collaboration Between Industry and Government 5
7. Cyber Standards for NFPs and Government's Role 6
8. Unique challenges of NFP 6

1. Executive Summary

Infoxchange welcomes the opportunity to contribute to the Government's Horizon 2 Cyber Security Strategy consultation. As a not-for-profit social enterprise with over 35 years' experience supporting the community sector with technology, we deliver trusted services including the Digital Transformation Hub and Ask Izzy. These platforms already reach tens of thousands of charities and community organisations across Australia, providing digital capability building, cyber awareness and practical support. We see firsthand both the opportunities and vulnerabilities within the sector, and we are committed to working with government, industry and peak bodies to strengthen national resilience.

Not-for-profits (NFPs) are a critical part of Australia's social infrastructure. They manage highly sensitive client and donor data, support vulnerable populations and deliver essential services, yet they operate with chronic underfunding, limited IT capacity and high reliance on volunteers. This leaves them disproportionately exposed to cyber threats. Protecting the sector is not only about safeguarding organisations, but about ensuring the safety and trust of millions of Australians who depend on them.

Our submission makes the case for tailored, collaborative approaches to uplift cyber resilience across the NFP sector. Key themes include:

- Inclusion in national governance: Recognising the sector as part of Australia's critical cyber ecosystem. This includes representation on advisory bodies such as the Executive Cyber Council.
- Leveraging existing sector platforms: Scaling proven initiatives such as the Digital Transformation Hub, which has already supported over 20,000 NFPs with health checks, training, policy templates and one-on-one advice.
- Unified and relevant awareness campaigns: A single national "Cyber Safe Communities" campaign, delivered in plain language with simple, repeatable actions and tailored examples, amplified through trusted sector networks.
- Targeted funding and supports: Direct investment in baseline protections, accessible templates and subsidised tools, plus grants that help organisations implement improvements with expert guidance.
- Collaborative delivery with peak bodies and industry: Government, corporates and philanthropy working through trusted intermediaries ensures advice is relevant and adopted at scale. This includes expanding programs like Digital Transformation Hub, volunteer cyber mentors, corporate partnerships and shared services models.
- Tailored standards for smaller organisations: A plain-language Cyber Essentials Baseline, co-designed with the sector, to provide realistic, achievable steps that complement but do not duplicate the Essential Eight.

We believe Horizon 2 must explicitly include not-for-profits as partners in the nation's cyber resilience. With coordinated support, investment and sector-specific tailoring, thousands of community organisations can rapidly adopt baseline protections, protect sensitive data, and strengthen the overall security of the Australian ecosystem.

2. Emerging Trends & Strategic Factors

Q1) What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

NFPs are rapidly moving to cloud platforms, mobile apps and data analytics, but their cyber maturity lags because of chronic underfunding and limited IT capacity. More than 60 per cent report lack of budget as their biggest barrier and many still rely on outdated systems and volunteer IT support (Infoxchange, Digital Technology in the Not-for-Profit Sector Report, 2024),. This makes them a weak link in the national ecosystem. Horizon 2 should align with the NFP Digital Transformation Blueprint 2021 to 2031 and provide dedicated funding so the sector can build core cyber resilience.

Artificial intelligence is also transforming the sector, with three quarters of NFPs already using generative AI for reporting, analysis and client support (Infoxchange 2024). While this delivers efficiency, it creates new risks such as deepfakes, scams and AI-driven phishing, and almost nine in ten NFPs have no AI guidelines. Government should encourage safe adoption by issuing privacy compliance guidance, promoting affordable AI security tools and training staff to recognise AI generated threats. Horizon 2 must balance innovation with protection against misuse.

Phishing and social engineering continue to be the most common attack vectors, yet only 20 per cent of NFPs provide regular cyber training to staff and volunteers (Infoxchange 2024). Many lack basic measures such as multi factor authentication, password managers and annual awareness programs. Because NFPs connect with government and corporate systems, their vulnerabilities can increase supply chain risk. Horizon 2 should strengthen human-centric security by including NFPs in threat intelligence sharing and national cyber exercises, treating them as integral parts of the defence network.

Finally, the overall threat environment is intensifying as organised crime and state sponsored groups increasingly target softer sectors such as charities, which hold highly sensitive data including health, housing and domestic violence records. With tighter privacy regulation and rising accountability, NFPs must be explicitly included in national cyber planning. This requires grants to help them comply with new standards, tailored reporting requirements and clear recognition of their role in protecting national privacy outcomes. Horizon 2 should position NFPs as essential partners in resilience, not peripheral players.

3. Targeting & Consolidating Cyber Awareness

Q5) What could government do better to target and consolidate its cyber awareness message?

Government should unify its messaging into one cohesive national campaign tailored for charities and not-for-profits. At present, advice is fragmented across ACSC materials, sector-specific tips, and other channels. A consolidated “Cyber Safe Communities” initiative - with consistent branding and five or six core actions such as enabling MFA, using strong passphrases, and thinking before clicking - would reduce confusion. Like a public health campaign, it should use plain language, simple taglines, and frequent repetition so that staff and volunteers internalise the basics. Crucially, it must reflect the NFP context rather than defaulting to corporate examples.

This national message should be amplified through trusted local networks that NFPs already rely on, including Volunteering Australia, state Councils of Social Service, philanthropic associations,

Aboriginal Community Controlled Organisations and ethnic community councils. Experience from the Cyber Wardens pilot shows organisations are more likely to engage when invited by their own association, and the same principle applies here. Embedding the government's unified message into ACNC newsletters, sector forums and webinars would significantly increase reach and impact.

To be effective, the campaign must also tailor content to nonprofit realities. Case studies showing, for example, a small charity treasurer almost falling for a billing scam, or a homelessness service avoiding a breach by backing up data, make the advice relatable. Videos, infographics and stories of "organisations like me" resonate more strongly than abstract warnings. Content must be jargon-free and empowering, emphasising that small steps can deliver significant protection. This mirrors the approach already proven by Infoxchange's Digital Transformation Hub, which has successfully engaged tens of thousands of NFP workers with positive storytelling.

Government should also use positive reinforcement and trusted voices. A recognition program (such as a "Cyber Safe NFP" badge for organisations that complete training or meet baseline standards) would create incentives and set visible norms. Ambassadors drawn from respected charity CEOs or community leaders would build confidence, while continuing grassroots grants for local workshops would strengthen the national message by building local champions.

Finally, cyber education should be integrated into everyday processes. Simple nudges in ACNC log-ins or grant application portals, reminders in charity registration packs, and embedded resources in professional development all help keep security front of mind. Infoxchange's Hub has already reached more than 35,000 NFP staff by embedding guidance into existing training; scaling this nationally would make awareness part of routine practice, not a separate task.

4. Successful Programs to Scale Up

Q6) What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

Infoxchange's Digital Transformation Hub (DTH), launched in 2021 with support from Google.org, Microsoft, the Paul Ramsay Foundation and others, has already helped more than 20,000 NFP staff and volunteers with free training, health checks, policy templates and one-on-one advice. Its success lies in being purpose-built for the sector and delivered by a trusted provider. Many smaller organisations have adopted MFA, backup practices and basic security policies as a result. The Hub is ready to scale, with opportunities to expand regional delivery, integrate modules into government grants processes, and broaden content for groups such as First Nations organisations. Importantly, public investment would leverage significant ongoing private and philanthropic support.

State-level initiatives have also demonstrated impact. South Australia's Social Sector Transformation Fund provided small grants that enabled hundreds of charities to upgrade systems, move to secure cloud platforms and implement MFA for the first time. Similar cyber grants for small businesses in New South Wales were heavily oversubscribed, showing clear demand. A modest, federally funded grants program for NFP cyber upgrades, paired with expert guidance through trusted intermediaries, could address resource gaps nationally.

Peer-led training models such as COSBOA's Cyber Wardens have shown value in small business settings, where employees can take on a "cyber champion" role alongside their regular work. However, this approach does not translate neatly to the NFP context. Charities and community organisations often deal with highly sensitive client and donor data, rely heavily on

volunteers with varied digital skills, and operate with very limited funding for training or IT roles. Unlike SMEs, they may not have stable staff capacity or the resources to maintain designated "cyber champions." While the principles of simple, non-jargon awareness are useful, a direct adaptation of Cyber Wardens is not fit for purpose without significant redesign to reflect the realities of the sector.

Dedicated sector uplift pilots have further validated the approach. In 2023, Infoxchange and peak body partners coached a small group of charities to adopt baseline protections; by program end, every participant had implemented multi-factor authentication and regular backups. Scaling this model across thousands of organisations could rapidly raise the sector's overall maturity and align with Horizon 2 goals.

Grassroots initiatives have also proven effective. The Commonwealth's 2022 Cyber Awareness Grants funded more than 200 community groups to deliver local workshops, often in community languages and trusted settings such as libraries. These should be renewed and expanded, with a focus on easy-read and accessible resources.

Education partnerships are another underutilised pathway. TAFE and university pilots, such as IT students assisting charities to configure secure systems, both build workforce skills and deliver practical benefits to NFPs. Incentives for tertiary institutions to embed cyber awareness into community service curricula, and structured student volunteering programs, would ensure that future staff enter the sector with baseline digital security capability.

International experience also offers models worth considering. In the UK, the "Cyber Essentials" scheme provides charities with a simple certification pathway to baseline security. A similar Australian equivalent, adapted for NFP realities, could set standards while offering recognition that builds public trust.

5. Encouraging Uptake of Cyber Resources

Q7) How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?

Many free resources already exist, such as the ACSC's Small Business Cyber Resilience tools, Cyber Wardens training modules and ACNC guidance, but NFPs are often unaware of them or lack the capacity to apply them. Government can make these resources relevant and accessible by embedding them into existing processes. For example, prompts could be added to the ACNC Charity Portal dashboard or links to free health checks offered during grant applications. Reframing resources for the NFP context, such as adapting the Small Business Cyber Guide into a "Community Organisations Cyber Safety Guide," would also improve uptake. Partnerships with Infoxchange and peak bodies can help tailor and distribute this content widely.

Sector leaders are trusted messengers, so empowering peak bodies such as Philanthropy Australia and state Councils of Social Service is key. Government can work with these groups to host webinars, circulate guidance and encourage adoption. Philanthropists could also promote uptake by asking grantees to use self-assessment tools as part of reporting. Negotiated vendor deals, like extending enterprise security licences to charities, could be championed through these peak networks.

The main barrier is often implementation, as many NFPs lack technical staff. Government support should therefore fund capacity to apply advice, building on existing programs like the Digital Transformation Hub's consultations or expanding volunteer initiatives such as "Cyber Buddy" schemes. A hotline or chat service run by ACSC or trained volunteers would further help NFPs put advice into practice with confidence.

Gentle compliance nudges and incentives can also shift behaviour. For example, the ACNC Annual Information Statement could include a voluntary question on cyber improvements, linking to resources. Insurers might reduce premiums for charities that complete training or checklists, and donors or grant programs could favour applicants who demonstrate good cyber practices. By positioning cyber steps as markers of good governance, uptake will grow.

Finally, highlighting success stories is essential. Sharing examples of NFPs that improved security using government resources through newsletters or conferences provides social proof and practical lessons. As adoption increases, feedback from the sector can refine the tools and make them even more relevant.

6. Collaboration Between Industry and Government

Q8) How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience? What type of support would be useful and who should provide it?

The Digital Transformation Hub (DTH) already provides the foundation for uplifting NFP cyber resilience. Supported by Google, Microsoft, the Paul Ramsay Foundation and others, it has helped more than 20,000 organisations with cyber health checks, policy templates, training modules, one-on-one advice and sector outreach. Rather than creating new programs, government and industry should collaborate with the Hub and peak bodies to expand reach and embed these supports nationally. Working alongside Home Affairs ensures alignment with the National Cyber Security Strategy, particularly *Shield 1: Strong businesses and citizens*.

It is important that the NFP sector has a voice in national cyber governance structures. At present, there is no NFP representation on the Executive Cyber Council, despite the sector's critical role in delivering essential services, managing sensitive data and supporting vulnerable Australians. We believe it would strengthen the Council's work to include this perspective. To that end, David Spriggs, CEO of Infoxchange, would be prepared to represent the sector if invited. Including NFP leadership would help ensure that Horizon 2 initiatives and broader strategy decisions reflect the needs and realities of community organisations, supporting resilience across the whole ecosystem.

Collaboration should focus on co-delivery of training and guidance, with government providing expert content, industry contributing tools and case studies, and peak bodies ensuring the advice is relevant and trusted. Large firms can also strengthen the model through corporate volunteering and mentorship, coordinated through the Hub, giving smaller NFPs access to skilled cyber professionals.

Timely threat intelligence sharing remains critical: alerts need to be simplified and pushed through trusted sector networks and technology partners. Alignment on standards and incentives is equally important. A government-endorsed baseline checklist, backed by insurers and funders, would make adoption easier and more rewarding.

By leveraging the DTH and working in partnership across government, industry and peak bodies, thousands more NFPs can quickly implement core protections such as MFA, backups and cyber training, significantly strengthening national resilience.

7. Cyber Standards for NFPs and Government's Role

Q9) What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs? What role should government play in supporting/endorsing SMB tailored standards?

Government should establish a plain-language Cyber Essentials Baseline for small organisations, tailored to NFPs. This would be a concise checklist of core actions - enable MFA, use antivirus, apply updates, back up key data, and provide annual phishing training. Similar to the UK's Cyber Essentials, it must use clear, non-technical language and reflect NFP realities: protecting donor and client data, working with volunteers on personal devices, and operating on minimal budgets. Essential Eight remains valuable, but is often unachievable for smaller NFPs; a lighter benchmark would set a realistic starting point.

The standard should be co-designed with the sector to ensure relevance. NFPs are not just small businesses; they handle highly sensitive information and rely heavily on volunteers. Sector input ensures examples speak to real scenarios (e.g. securing case management systems or donor databases) rather than generic business processes. While SMB Cyber 1001 provides a base, NFP-specific tailoring is needed to make adoption practical.

To support compliance, government should pair the baseline with free or subsidised tools: templates for incident response and policies, donated or discounted cloud storage and security software, and ready-made training modules. These resources can be distributed through trusted channels such as the Digital Transformation Hub, making adoption simple and achievable.

Finally, the standard should be a living framework, reviewed annually with NFP feedback to adapt to new threats. Starting with a small set of achievable controls, then gradually raising expectations with strong support, will build trust, improve uptake, and steadily lift sector resilience.

Measurable outcome: by 2027, at least 70% of NFPs should meet the Cyber Essentials Baseline, doubling today's levels of baseline protection and aligning with Horizon 2 goals for stronger businesses and citizens.

8. Unique challenges of NFP

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?

Not-for-profits face distinct cyber challenges. Unlike businesses, they operate with severe resource constraints, short funding cycles and little or no IT staff. Over half of small NFPs have no dedicated IT support (Infoxchange 2024), relying instead on general staff or volunteers. At the same time, they hold highly sensitive data on vulnerable people and donors, where a breach can cause serious harm well beyond financial loss. Reliance on volunteers and high staff turnover makes maintaining consistent cyber practices difficult, while reputational damage from an incident can erode donor trust and threaten service delivery.

Because of this, NFPs need targeted government support. The most effective interventions are:

- Direct funding for baseline protections - MFA, backups, secure cloud, and managed IT services delivered through trusted intermediaries.

- Simple, repeatable training and tools for non-technical staff and volunteers, using plain language and sector-specific examples.
- Crisis response support - rapid assistance to contain incidents, protect clients, and communicate transparently with donors.
- Shared services - such as a sector-wide SOC, central identity management for volunteers, or bulk licensing deals for security software. These “one-to-many” solutions provide protections no single NFP could afford.

A coordinated three-year program, led through the Digital Transformation Hub in partnership with peak bodies, would make the greatest impact. Treating cyber security as essential social infrastructure (much like shared finance or HR platforms) is the only way to lift resilience across a fragmented, under-resourced sector.

Measurable outcome: by 2027, double the number of NFPs with documented cyber plans, MFA enabled, and staff training in place, reducing both the likelihood and impact of incidents on vulnerable Australians.

TECHNOLOGY FOR
SOCIAL JUSTICE

[redacted]
[redacted]
www.infoxchange.org

Follow us on: