Australian Government | Australian Charities and Not-for-profits Commission

2 September 2025

Our Ref: ACNCSUB2025/3

Stephen Palethorpe
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
CANBERRA ACT 2600

(by email: le.committee@aph.gov.au)

Further submission - Inquiry into the capability of law enforcement to respond to cybercrime

Dear Committee,

The Australian Charities and Not-for-profits Commission (**ACNC**) welcomes the opportunity to provide additional information to the inquiry into the capability of law enforcement to respond to cybercrime. The following comments are in addition to the submission lodged on 14 December 2023 and published on the inquiry website as submission number six (06), a copy of which is attached at Appendix A.

For the Committee's benefit, this supplementary submission includes:

(a) more recent information about the context in which charities operate
(b) learnings from the ACNC's cyber security reviews conducted in 2024-25
(c) a summary of our efforts to build charities' cyber resilience, including through collaboration with other government agencies.

I trust this further information will assist the Committee in its work. If you have questions about this submission, or any matter that the ACNC could assist with please contact Suhanya Mendes, Director Legal & Policy via email to Suhanya.Mendes@acnc.gov.au.

Yours sincerely,

Cate Bennett
Acting ACNC Commissioner

Context

Australia's registered charity sector includes a diverse range of almost 64,000 organisations. Charities collect and hold significant amounts of sensitive information of interest to cybercriminals. This includes personal data about the people charities help, as well as information about employees, donors and volunteers. Consistently, almost half of notifiable data breaches reported to the Office of the Australian Information Commissioner are the result of cyber security incidents.[1]

Many charities are highly vulnerable to data theft, scams and cybercriminals.[2] In our first submission, the ACNC advocated for government support and interagency collaboration to build and maintain robust cyber-secure environments for charities to address these threats. A lack of funding to help charities build cyber resilience continues to put donor data and sensitive information at risk.[3] Under-resourced charities lack funds for up-to-date technology or staff training,[4] so they will often rely on third party IT providers and as studies show, this type of outsourcing could potentially expose the charity to a large-scale data breach.[5]

The additional information in this submission calls attention to the significant risks that persist, and the ACNC's efforts since 2023 to help charities better protect themselves against cybercrime.

Reports published since 2023 have shown small to medium charities are most at risk of falling victim to cybercrime.[6] Unlike better-resourced organisations, small to medium charities have more limited resources and expertise to implement preventative measures, pay for insurance, or respond to cyber security incidents when they occur.[7]

Charities reliance on donations from the public to operate requires a high level of engagement both online and in person to build and maintain the trust required to garner ongoing support. This high engagement also makes charities obvious targets for cyber criminals and the consequences of a cyberattack can be particularly damaging to charities as it erodes the trust earned adversely impacting donor support.[8]

Cyber risk reviews conducted in 2024-25

In the past two years the ACNC has undertaken cyber security risks reviews[9] to better understand cyber security risks and identify key areas where charities could strengthen their governance to minimise these risks.

The ACNC selected 25 charities based on their size, activities, source of revenue and beneficiaries, and asked them to advise us of:

- cyber risks (or breaches) the charity had identified
- how the charity protected itself from cyber-attacks

---

[1] Office of Australian Information Commissioner, Notifiable data breaches publications, www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications

[2] 'Cyber security for charities and not-for-profit organisations ', *Australian Signals Directorate* (Web Page,18 May 2024) <https://www.cyber.gov.au/about-us/view-all-content/news-and-media/cyber-security-charities-and-not-for-profit-organisations>.

[3] Australian Council for International Development, 'Lack of funding leaves sensitive charity data exposed', (Media Release, 20 May 2024) < https://acfid.asn.au/lack-of-funding-leaves-sensitive-charity-data-exposed/ >.

[4] Infoxchange, 'Digital Technology in the Not-For-Profit Sector Report', (2024 report, November 2024) <https://www.infoxchange.org/sites/default/files/digital_technology_in_the_not-for-profit_sector_report_2024_-_infoxchange_0.pdf>.

[5] Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report: Jan-June 2024', (Web Page, 16 September 2024) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024>.

[6] Australian Institute of Criminology , 'Cybercrime in Australia 2023', 4<https://www.aic.gov.au/sites/default/files/2023-07/sr43_cybercrime_in_australia_2023_v2.pdf>.

[7] CyberCX, 'Cyber Intelligence Insights, Australian Charities', December 2023, < connect.cybercx.com.au/l/1069042/2024-06-09/2c72jjx/1069042/1717909486egiSNrJg/CyberCX_Australian_Charities_Cyber_Intelligence_Insights_Report_Publi.pdf>.>

[8] Ibid

[9] Australian Charities and Not-for-profits Commission, 'Cyber security risks', *Compliance Reviews* (Web Page) <www.acnc.gov.au/raise-concern/regulating-charities/compliance-and-enforcement/compliance-reviews#section-12754>.

- the steps the charity would take, or has taken, in the event of a cyber security incident.

The reviews found that smaller charities were less likely to have an advanced approach to cyber security. This included lacking appropriate policies and procedures on data management and retention, including when working with third parties (including contracted service providers), and not having a plan to respond to cyber incidents.

Charities with robust information and data management policies and procedures in place, as well as governance that enabled and supported board members in driving strong cyber governance practices and promoted a strong culture of cyber security awareness were more cyber resilient.

This lends further support to our view expressed in our first submission, that charities would benefit from further government support to uplift cybersecurity.[10]

Building charities' cyber resilience in collaboration with other government agencies

The ACNC uses findings from compliance reviews to inform improvements to our guidance offerings to registered charities. We also seek out partnerships with other government agencies and regulators who have expertise in those areas where charities are at risk, including cyber risks.

Since our submission in December 2023 the ACNC has undertaken a number of initiatives to help charities uplift their cyber resilience. This has included:

- partnering with the Australian Signals Directorate (ASD) to improve our cyber security governance toolkit [11]
- working with ASD on their cyber security education campaign focussed on charities through our monthly newsletter [12] and social media, as well as recording a joint podcast with the Assistant Director-General Technical Threats and Visibility, ASD [13]
- publishing guidance on charities and artificial intelligence [14]
- Partnering with the Office of the Australian Privacy Commissioner (OAIC) to record a joint podcast with Privacy Commissioner, Carly Kind to discuss protecting sensitive data [15]

Collaboration allow us to leverage knowledge and expertise of subject matter experts across government and deliver targeted messaging directly to charities through ACNC communications channels, signposting the best guidance to support building cyber resilience.

Australia's not-for-profit sector averages one cyberthreat every six minutes.[16] 2024 saw a dramatic escalation in cyber threat activity, growing vulnerabilities and active exploitations.[17] The ACNC is committed to working across government to assist registered charities focus on emerging threats and build cyber resilience.

---

[10] Australian Charities and Not-for-profits Commission, 'Submission No 6 to Parliamentary Joint Committee on Law Enforcement, *Inquiry into Capability of law enforcement to respond to cybercrime* (14 December 2023) [14] and [17] <https://www.aph.gov.au/DocumentStore.ashx?id=c186c2d9-22a5-4f02-a8c4-56139765cdb0&subId=750957 >.

[11] Australian Charities and Not-for-profits Commission, 'Cybersecurity', *Governance Toolkit: Cyber security* (Web Page) <www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-toolkit/governance-toolkit-cyber-security>.

[12] Australian Charities and Not-for-profits Commission, 'Assessing your charity's risks is the first step to combating cyber threats' , *The Charitable Purpose*, 9 November 2023 and 'Building cyber resilience is everyone's responsibility', *The Charitable Purpose*, 11 April 2024

[13] 'ACNC Charity Chat podcast 32, 6 May 2024', *Charities and Cyber Security (*Australian Charities and Not-for-profits Commission 6 May 2024) <https://www.acnc.gov.au/tools/podcasts>

[14] Australian Charities and Not-for-profits Commission, 'Charities and Artificial Intelligence', *Charities and Artificial Intelligence* (Web Page) < www.acnc.gov.au/tools/guides/charities-and-artificial-intelligence>.

[15] 'ACNC Charity Chat podcast 33, 27 March 2025', *Charities and Privacy (*Australian Charities and Not-for-profits Commission 27 March 2025) <https://www.acnc.gov.au/tools/podcasts>.

[16] Australian Signals Directorate, Australian Cyber Security Centre 'Cybersecurity for charities and not-for-profits' *Protect Yourself* (Web Page, 12 March 2024) says "cyberthreats are on the rise in Australia, with charities and not-for-profits prime targets for cybercriminals" with nearly 94,000 cybercrime reports received in 2022-2023 financial year. <https://www.cyber.gov.au/protect-yourself/staying-secure-online/cybersecurity-for-charities-and-not-for-profits>

[17] Price Waterhouse Coopers, 'Cyber Threats 2024: A Year in Retrospect', *Charting a Course* (Web page, 11 April 2025) <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html>

Appendix A - ACNC submission to Joint Committee on Law Enforcement: The capability of law enforcement to respond to cybercrime (published)

Australian Government

Australian Charities and Not-for-profits Commission

14 December 2023

Inquiry into the capability of law enforcement to respond to cybercrime
Committee Secretary
Parliamentary Joint Committee on Law Enforcement

Submitted Online: The capability of law enforcement to respond to cybercrime – Parliament of Australia (aph.gov.au)

Our reference: ACNCSUB2023-013

1. The Australian Charities and Not-for-profits Commission (ACNC) welcomes the opportunity to comment on the Parliamentary Joint Committee on Law Enforcement's Inquiry into the capability of law enforcement to respond to cybercrime.

2. We have addressed only the terms of reference that we consider are relevant to the ACNC's role as the national regulator of charities.

About the ACNC and the charity sector

3. The ACNC is the national regulator of charities established by the *Australian Charities and Not-for-profits Commission Act 2012* (Cth) (ACNC Act). The objects of the ACNC Act are to:

   a. maintain, protect and enhance public trust and confidence in the Australian not-for-profit sector; and
   b. support and sustain a robust, vibrant, independent and innovative Australian not-for-profit sector; and
   c. promote the reduction of unnecessary regulatory obligations on the Australian not-for-profit sector.

4. Currently, the ACNC has oversight of around 60,000 registered charities. The ACNC does not have oversight of the wider not-for-profit sector. These charities vary considerably in size, role, and function. Charities are a vital part of our community and economy. Registered charities employed over 1.42 million people[1] and reported revenue of $190 billion in the 2021 reporting period.[2] While some charities are large and well-known entities, most charities are very small, volunteer-run organisations.[3]

[1] Australian Charities and Not-for-profits Commission, *Australian Charities Report – 9th edition*, 2023, 19.
[2] Ibid, 24.
[3] Ibid, 12; 19-21.

GPO Box 5108 Melbourne VIC 3001
Tel 13 ACNC Fax 1300 232 569
acnc.gov.au

Context

5. Given the groups they serve, we expect that the vast majority of charities hold personal information, including financial and sensitive information. The sensitive information of charity beneficiaries, for example, may include financial information, health concerns, criminal records, or religious affiliations. Unauthorised access to this information could have significant consequences for individuals, as well as disrupt the operations of charities and potentially damage the reputation of the sector.

6. Recent examples include the 2020 attack on a vendor used by Save the Children,[4] the 2022 attack of The Smith Family,[5] and the recent attack of Pareto Phone.[6] News reporting regarding the hack of Pareto Phone indicates that the personal data of tens of thousands of donors to large charities, such as the Fred Hollows Foundation, Cancer Council and Canteen, was published.[7]

7. In Australia, 8% of respondents to the 2023 State of the Sector Report for Nonprofits reported a cybersecurity incident in the previous 12 months.[8] It is not clear if this low percentage is because:
   a. attackers are not interested in Australian charities, compared to UK charities,
   b. Australian charities do not have the capability to identify attacks, or
   c. charities are not self-reporting about data breaches, where they are not obliged to notify the Office of the Australian Information Commissioner under the *Privacy Act 1988* (Cth). Many smaller charities may not be covered under this Act.

8. Despite this, Infoxchange's 2023 survey into how not-for-profit organisations use digital technology report found that:[9]
   a. 23% of organisations "reported having effective processes to manage information security risk";
   b. 12% of respondents agreed that they were regularly conducting cybersecurity awareness training, and

---

[4] Save the Children (2020), *Save the Children Statement on Blackbaud Security Breach*, <https://www.savethechildren.org/us/about-us/media-and-news/2020-press-releases/save-the-children-statement-on-blackbaud-security-breach>.

[5] ABC News (22 November 2022), *The Smith Family says details of around 80,000 donors may have been exposed in hacking attack*, <https://www.abc.net.au/news/2022-11-22/smith-family-charity-cyber-crime-hackers-donor-details/101683860>.

[6] ABC News (23 August 2023), *Thousands of donors to Australian charities, including Cancer Council and Canteen, have data leaked to dark web*, <https://www.abc.net.au/news/2023-08-23/qld-charity-donors-dark-web-cyber-criminals-pareto-phone/102757194>.

[7] ABC News (21 October 2023), *Pareto Phone, telemarketer at centre of charity cyber hack which targeted tens of thousands of Australian donors, collapses*, <https://www.abc.net.au/news/2023-10-21/qld-pareto-phone-charity-hack-cyber-criminal/103002650>.

[8] Charity Research Centre AU, *State of the Sector 2023*, 1, <https://www.uwa.edu.au/schools/-/media/Centre-for-Public-Value/Resources/230906-State-of-the-Sector-Report.pdf>.

[9] Infoxchange, *Digital Technology in the Not-for-profit Sector Report 2023*, 10, <https://www.infoxchange.org/au/digital-technology-not-for-profit-sector>.

c. only 23% of respondents agreed that they had "effective processes to manage information security related risks" and 52% partially agreed.

9. Nevertheless, one in four organisations responded that they were prioritising improving their data protection and cybersecurity practices.[10]

10. Another survey of CEOs of not-for-profit organisations found that 30% of respondents were not considering or had not made progress on establishing a program to uplift their organisation's cybersecurity or privacy measures.[11]

11. Charities typically have limited resources to call on to respond to anything regarded as additional operational requirements and expenses. The *Paying what it takes: Funding indirect costs to create long-term impact* report found that Australian businesses spent on average 1.8 – 3.6 times more per employee than the not-for-profits examined in the report.[12] One reason may be that explicit funding for administrative costs, including cybersecurity, is not commonly provided. However, as our website notes, administration costs are not a useful measure of the effectiveness or impact of charities.[13]

12. The ACNC's ninth Australian Charities Report found that total expenses for charities had increased by $7.1 billion to $174.8 billion in the 2021 reporting period.[14] Other expenses, which include operational costs, constitute 37.1% of all expenses for the charities sector.[15]

13. Also, the sector is aware that the community expects charities to expend their resources on their purposes and can be critical of charities perceived to be 'wasting' resources on administrative expenses.[16] Charities may find it difficult to balance the need to spend on important administrative costs compared to their charitable programs.

Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime

14. To support charities, the ACNC has published a Governance Toolkit covering cybersecurity and associated resources. It includes a self-assessment tool and

---

[10] Ibid, 20.

[11] PwC, *Pwc Australia's 3rd Annual Not-for-profit CEO Survey*, 9, < https://www.pwc.com.au/about-us/social-impact/not-for-profit-ceo-survey.html>.

[12] Centre for Social Impact, Philanthropy Australia, and Social Ventures Australia (March 2022) *Paying what it takes: Funding indirect costs to create long-term impact*, 21-22, <https://www.socialventures.com.au/work/paying-what-it-takes-report/>.

[13] ACNC, *Charities and administration costs*, <https://www.acnc.gov.au/for-public/understanding-charities/charities-and-administration-costs>.

[14] ACNC, *Australian Charities Report* (9th ed), 2023, 26.

[15] Ibid, 36.

[16] See, for example, Social Ventures Australia and the Centre for Social Impact, 'Paying What It Takes: Funding Indirect Costs to Create Long-term Impact' (2022) 37.

checklist.[17] The ACNC, where possible, works with other agencies to ensure this guidance remains up to date. We are also considering other ways we can reach out to charities regarding cybersecurity, including with other agencies where possible.

15. Charities have a comparable need to the private sector for support and guidance to enhance data security practices, procedures, and infrastructure. In our view, the needs of charities may be more acute because of the constraints on their spending and given the factors outlined above. As a result, charities may require further support in establishing sound cybersecurity and privacy practices.

16. Overseas examples include the *Cyber security: Small charity guide* published by the UK's National Cyber Security Centre.[18]

17. We consider that specific charity-focused support may be required from law enforcement and private sector organisations, as well as other government agencies, to support charities to respond to and manage the risks of cybercrime.

Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians

18. Of the charities which responded to the UK 2023 Cyber Security Breaches Survey, 24% had identified a cyber breach or attack in the 12 months leading to the survey. This represents a decrease from the result in 2022, where 30% of charities reported identifying a breach or attack.[19] As the authors of that report note, it is not clear if this reflects a decrease in the number of attacks or if organisations had become less capable of identifying breaches or attacks. This may be related to a decrease in the percentage of charities seeing cybersecurity as a high priority perhaps due to competing priorities.[20]

19. Given the context described above and at [5] - [12], there is a risk that Australian charities will increasingly be seen as an "easy" or "soft" target, and that the percentage of charities experiencing cyberattacks will increase.

Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime

20. The ACNC acknowledges the importance of promoting information privacy and sees sound records management as part of good governance. We also acknowledge that the public is becoming increasingly concerned about the vulnerability of the large amounts

[17] ACNC, Governance Toolkit: Cyber Security, <https://www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-toolkit/governance-toolkit-cyber-security>.
[18] National Cyber Security Centre, *Cyber security: Small charity guide*, <https://www.ncsc.gov.uk/collection/charity>.
[19] Maddy Ell and Emma Johns (19 April 2023), *Official Statistics Cyber Security Breaches Survey 2023*, Chapter 4: Prevalence and impact of breaches or attacks, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#chapter-4-prevalence-and-impact-of-breaches-or-attacks>.
[20] Ibid, Chapter 2: Awareness and attitudes.

of personal and sensitive information held digitally by government, private sector, and community sector organisations, following several high-profile data breaches. If the community is confident that charities are handling personal information correctly, it will enhance trust and confidence in the Australian not-for-profit sector.

21. Further government support may be required to support charities to uplift their cybersecurity practices. We are aware that there have been government grants available to support small and medium sized enterprises to invest in their cybersecurity. Similar measures may be useful for charities.

Next steps

22. If you have queries about this submission please contact , Legal and Policy, , or , Acting Policy Manager, Legal and Policy, .

Commissioner
Australian Charities and Not-for-profits Commission