

28 August 2026
ACNCSUB2026-5

Committee Secretary
Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations
Parliament House
Canberra ACT 2600
cssmbo.reps@aph.gov.au

Inquiry into cyber security for small to medium sized businesses and organisations

Dear Committee Secretary,

The Australian Charities and Not-for-profits Commission (ACNC) welcomes the opportunity to provide a submission to the inquiry into cyber security for small to medium sized businesses and organisations. We know from our engagement with charities their concern with increasing risks associated with cyber security and with international charity regulators these concerns (and the risks they present) cross borders. Recognising these increasing cyber risks, the ACNC is working closely with the Department of Home Affairs to improve cyber resilience across the sector and support organisations to better protect their systems, data and communities.

This submission focuses on the following points of inquiry:

- the cyber maturity of Australian small to medium sized businesses and organisations, including not-for-profit organisations
- the adequacy, appropriateness and accessibility of guidance provided to small to medium sized businesses and organisations by Government in relation to cyber security.

If you have any questions about this submission, please feel welcome to contact [REDACTED]
Acting director, Education and Public Affairs, via email to [REDACTED]

Sincerely,

[REDACTED]

Nadine Clode
Acting Commissioner
Australian Charities and Not-for-profits Commission



About the ACNC and the charities sector

1. 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
 - b) support and sustain a robust, vibrant, independent and innovative not-for-profit sector
 - c) promote the reduction of unnecessary regulatory obligations on the sector.
2. The ACNC regulates around 66,000 registered charities.
3. Thirty percent of charities are extra small (meaning they have an annual revenue of less than \$50,000), and another 30% are small (annual revenue between \$50,000 and \$500,000).¹
4. Roughly 53% of all charities operate with no paid staff.² For extra small charities, this increases to 89% of charities operating with no employees.³

Cyber security and the charities sector

Cyber Risks

5. Charities can hold significant amounts of sensitive information. This includes both personal information from staff, volunteers and beneficiaries, and financial information from donors. As a result, cyber threats are an ongoing and persistent reality.⁴
6. Cyber-attacks can also impact public trust and confidence in the sector, as reputational risks and loss of support from donors can stretch beyond individual charities.
7. Cyber security is increasingly a governance and organisational resilience issue for charities. Cyber incidents can disrupt service delivery, compromise sensitive information, affect donor confidence, and impact a charity's ability to fulfil its charitable purpose.
8. Unlike many commercial organisations, charities often operate with limited discretionary funding which reduces their ability to improve systems⁵. Many charities must balance investment in cyber security against competing service delivery priorities, which can affect their ability to implement and maintain contemporary cyber security controls. In addition, they rely heavily on volunteers and part-time personnel, which may impact on their ability train and develop their workers on emerging cyber security risks and mitigations.

¹ ACNC, *Australian Charities Report – 12th edition* (2026) 24 <[Australian Charities Report - 12th Edition | ACNC](#)>

² Ibid, 17.

³ Ibid, 28.

⁴ Australian Institute of Company Directors and Beyond Bank Australia, *Not-for-profit Governance and Performance Study 2025/26*, <[NFP Performance and Governance Study 2025/26](#)>

⁵ Infoxchange, *Digital technology in the Not-for-profit sector report November 2025*, < [Digital Technology in the Not-For-Profit Sector | Infoxchange \(AU\)](#)>

9. In 2025, the ACNC published findings of a compliance review looking at cyber security as an emerging area of risk for charities.⁶

10. The review identified that risks are higher with small charities. Issues with cyber security governance were found when charities:

- paid little attention to cyber security risks
- did not have a plan to respond to cyber incidents
- lacked appropriate policies and procedures on data management and retention, including when working with third parties like contractors.

Cyber maturity

11. ACNC's compliance review found that differences in cyber maturity are frequently linked to organisational capacity, available resources and access to specialist expertise, rather than a lack of awareness of cyber security risks.

12. Charities with strong cyber security achieved this by:

- having strong information and data management policies
- promoting a culture of cyber security awareness
- d) drawing on available tools, resources and guidance
- understanding the specific cyber risks relevant to the organisation.

13. While most charities that took part in the review had satisfactory cyber security governance, smaller organisations were often not as mature in their approach to cyber security.

14. Larger charities tended to be better resourced and were able to invest more significantly in cyber security compared to smaller charities. For example, some larger charities had dedicated staff focused on managing cyber security.

15. Smaller organisations were likely to draw on staff expertise and were accessing resources that were free and already available.

16. The review identified common governance gaps among charities needing to strengthen their cyber security included:

- paying minimal attention to cyber security
- not having a plan to respond to cyber incidents
- lacking appropriate policies and procedures.

Guidance and support

17. Australia's charity sector is highly diverse, with many organisations operating with limited resources and volunteer workforces (as outlined above). ACNC and Australian Signals Directorate

⁶ ACNC, *Compliance reviews*, <[Compliance reviews | ACNC](#)>

guidance⁷ recognises that charities often benefit from cyber security information that is tailored to their size, governance arrangements, risk profile and operating environment.

18. The ACNC's [Governance Toolkit: Cyber security](#)⁸ provides practical guidance to charities about cyber security risks and how to manage them. This guidance has a 'helpful' rating of 95%.⁹
19. The Australian Signals Directorate reviewed the guidance in 2024, and the page was updated in line with their advice.
20. Additionally, the ACNC provides the following resources:
 - a cyber security checklist and assessment, to improve understanding of cyber security risks and obligations
 - a template information asset register, to help charities identify the information assets they hold, as well as document where and how they are stored, and who has access to them
 - a template plan for responding to data breaches, to support charities if things go wrong.
21. The ACNC also regularly publishes news items promoting free resources (from the ACNC and other government agencies) to support charities to build their cyber capability.¹⁰
22. The ACNC supports 2023-2030 Australian Cyber Security Strategy, with specific reference to one of the six key actions (under the Horizon 2 action plan) being to *"make it easier for small and medium businesses, and the not-for-profit sector, to strengthen their cyber security."*¹¹
23. The ACNC is partnering with the Department of Home Affairs to address this key action by driving cyber uplift and maturity for the not-for-profit sector. This includes:
 - facilitating greater sharing of cyber knowledge and resources across the not-for-profit sector through establishing a collaborative not-for-profit community of practice
 - delivering a program of services to support not-for-profit cyber uplift.¹²
24. Charities and not-for-profits can join the Not-for-Profit Cyber Uplift Community of Practice (COP) to access guidance and support.¹³ Engagement with the charity sector through COP, informed by

⁷ Australian Signals Directorate, *Cyber security for charities and not-for-profits*, <[Cyber security for charities and not-for-profits | Cyber.gov.au](#)>

⁸ ACNC, *Governance Toolkit: Cyber security*, <[Governance Toolkit: Cyber security | ACNC](#)>

⁹ Based on 69 'helpful' responses of a total of 73 responses to the question 'Was this page helpful?'.

¹⁰ For example, ACNC, *Take action to protect your charity from cyber crime in 2026*, 12 January 2026 <[Take action to protect your charity from cyber crime in 2026 | ACNC](#)> and ACNC, *Take action on your charity's cyber security in October*, 7 October 2025 <[Take action on your charity's cyber security in October | ACNC](#)>

¹¹ Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy: Horizon 2 action plan* (2026) 7 <[Action Plan for Horizon 2 of the 2023-2030 Australian Cyber Security Strategy](#)>

¹² Ibid, 10.

¹³ Department of Home Affairs, *Not-for-Profit Cyber Uplift Community of Practice*, <[Not-for-Profit Cyber Uplift Community of Practice](#)>

an Expert Advisory Group, will facilitate practical, tailored cyber capability support, particularly among smaller charities with limited access to specialist cyber expertise.

25. The ACNC will amplify this work through a recently announced, Charity Resilience and Productivity Project. The project will focus on support to strengthen capability, including cyber capability, where the need is greatest: among small and volunteer-run groups, newly registered charities, organisations working across language barriers, and charities in rural and regional Australia. The project will include a specific focus on cyber hygiene, fraud awareness, data protection and the safe use of artificial intelligence and other productivity tools.