



Too critical to ignore: Cybersecurity in Australian healthcare and NFP

The spotlight is on cybersecurity for technology leaders in Healthcare Not-for-Profits (NFPs). Organisations need to protect sensitive data, keep services running, and show funders and boards that security is under control, even with lean teams, fragmented systems, and growing accountability. Caught between these pressures, Healthcare remains an industry vulnerable to cyberattacks.



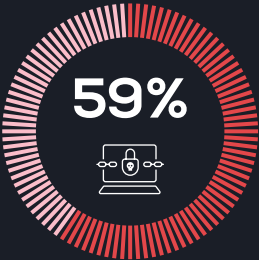
success rate for malicious attacks on Healthcare and Social Assistance in 2024-25, versus 52% across all other industries.¹



Data breach target
Health service providers accounted for 18% of all data breach notifications in Australia in the first half of 2025, making it the most breached sector.²

Care cannot stop

When systems fail, it is not just a technical inconvenience – it can make the difference between life and death for patients. In Healthcare settings, even minor disruptions can quickly affect service delivery, client trust, and operational continuity.



increase in ransomware incidents targeting Australian not-for-profit organisations in 2025.³

Visibility is fragmented

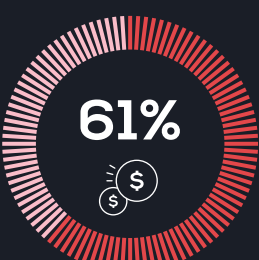
Legacy systems, cloud tools, connected devices, and third-party providers make it harder to see exposure clearly, track controls consistently, and prove that risk is being managed holistically.



of serious ransomware incidents in a 2024-25 survey by the ACSC were discovered by the ACSC itself, not by the affected organisations.¹

Capacity is constrained

Legacy systems, cloud tools, connected devices, and third-party providers make it harder to see exposure clearly, track controls consistently, and prove that risk is being managed holistically.



of NFPs say budget is the biggest barrier to improving cybersecurity.³

Compliance builds trust

Boards, funders, and partners want clear evidence of confident risk management. Better reporting and more auditable controls make it easier to defend security decisions and justify future investment.



year-on-year increase in reported data breaches to the OAIC, with Healthcare one of the most likely sectors to report a breach and be subject to a complaint.⁴

Get cybersecurity back on track

Nexon helps Healthcare providers turn fragmented security into more visible, manageable resilience with 24/7 monitoring, clearer reporting, and support for lean teams and budget constraints.

- ✓ **Proven and trusted**

Proven SOC and threat-intel maturity; deep experience integrating controls to governance requirements in Australian Healthcare organisations.
- ✓ **Unified security**

Leveraging Microsoft security, and other leading technology providers – operated by local, certified specialists.
- ✓ **Outcome-focused**

Clearer SLAs, fewer gaps, better visibility, clearer reporting, reduced chance of a successful attack.
- ✓ **One accountable partner**

Healthcare is complex. Cyber shouldn't be. Nexon brings deep healthcare expertise with advisory, managed and professional services to protect your people, processes and platforms.

Nexon Cybersecurity for Healthcare and NFPs

When security is a critical concern, you need partners who instill confidence in your organisation's resilience. Nexon supports Australian Healthcare with Microsoft-native security, local SOC support, and governance-ready reporting.

Find out more on our dedicated Healthcare and NFP site.



Sources:
¹ [Annual Cyber Threat Report 2024-2025, ASD, October 2025](#)
² [Latest Notifiable Data Breach statistics for January to June 2025, OAIC, November 2025](#)
³ [Australian NFPs gain critical cyber defence uplift as threats target charitable sector, PwC, September 2025](#)
⁴ [Annual Report 2024-25, OAIC, November 2025](#)

