

10 questions every health leader should be asking about cyber risk

If you hold patient records, donor information, or details about the people you serve, cyber risk is a governance responsibility, not just an IT one. These ten questions are a clear, practical place to start.

- 01 ☐ What are our biggest cyber risks, and how would they affect the patients, clients, donors or members who trust us with their information?
- 02 ☐ How long could we keep serving our community if our systems went down?
- 03 ☐ If we were hit by ransomware, could we recover without paying, and how long would that realistically take?
- 04 ☐ Who owns cyber risk at a leadership level, and do we get clear, regular reporting on it?
- 05 ☐ Have we actually tested our incident response plan, or are we assuming it would work when it matters? How does it address staff on leave?
- 06 ☐ Do we know which suppliers can access our data, and how confident are we in their security, not just our own?
- 07 ☐ Are we meeting our Privacy Act obligations and other relevant laws, and could we demonstrate that if a regulator, funder or client asked?
- 08 ☐ Is our cyber security spend matched to our real risk, or is it whatever happens to be left in the budget?
- 09 ☐ Do our people know how to spot and report a problem, or is security still seen as someone else's job?
- 10 ☐ If we were breached tomorrow, would we know who to call first, and what we'd say to the people affected?

Not sure how you'd answer these?

We help leaders of health, NGO and community organisations govern cyber risk with clarity and confidence. Find out more at www.ciostudio.nz/fractional-ciso

hello@ciostudio.nz
0800 120 848
ciostudio.nz