



STEWARDSHIP & RISK

Cyber and Data Governance as a Board-Level Risk, Not an IT One

The standard is not perfection. It is documented board-level engagement

Cyber security is still, in most association boardrooms, treated as an IT problem that gets a brief update slot before the meeting moves on to matters the board considers its own. That framing no longer matches either the legal exposure or the practical reality. It is a governance risk in the same category as the financial and risk appetite discipline covered earlier in this quarter, and it deserves the same level of board ownership.

Which rules apply to your association?

The law depends on how your association is set up. A **company limited by guarantee** follows the Corporations Act 2001 (Cth) and its constitution. An **incorporated association** follows its state or territory associations Act and its rules. A **registered charity** also follows the ACNC Act and the ACNC Governance Standards, and some Corporations Act rules are replaced for charities that are companies. Check your own governing documents, and get advice before decisions with legal consequences.

In this resource

1. [Who Is Actually Required To Comply, And Who Should Anyway](#)
2. [The Principle The Courts Have Already Established](#)
3. [Why This Belongs At Board Level, Not Just Management's Desk](#)

Who Is Actually Required To Comply, And Who Should Anyway

The Privacy Act 1988 (Cth) generally applies to organisations, including not-for-profits, with annual turnover over \$3 million, a figure similar to, but measured differently from, the ACNC's \$3 million revenue threshold for large charities. Smaller associations are also covered if, for example, they provide a health service and hold health information, trade in personal information or deliver Commonwealth contracts; check the OAIC's guidance on [who the Privacy Act covers](#). Covered organisations must comply with the Australian Privacy Principles and the Notifiable Data Breaches scheme, which requires notifying both affected individuals and the Office of the Australian Information Commissioner following an eligible data breach. Separately, since 30 May 2025, businesses with annual turnover of \$3 million or more that make a ransomware or cyber extortion payment must report it to the Australian Signals Directorate within 72 hours. Smaller organisations that are not covered are not legally compelled to comply in the same way, but this exemption is a floor, not a safe harbour. A smaller association still handling member health records, payment details, or other sensitive personal information carries real reputational and member-trust exposure regardless of where the legal line technically sits, and the practical case for voluntary compliance is strong even where the statutory obligation is not.

The Principle The Courts Have Already Established

The Federal Court's decision in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496, while decided in the context of an Australian Financial Services Licensee's specific statutory obligations, established a principle that reaches well beyond that sector: cybersecurity risk cannot be reduced to zero, but it can and must be materially reduced to an acceptable level through adequate documentation, controls, and real follow-through when incidents occur. The case was brought

against the company, not its directors. Separately, commentators note that a serious failure by an organisation to manage a known risk can support a claim that its directors failed to act with reasonable care and diligence, sometimes called 'stepping-stones' liability. For non-charitable companies that duty is in section 180 of the Corporations Act; for registered charities it is ACNC Governance Standard 5; for incorporated associations it is the relevant state or territory Act. The relevant standard is not perfection. It is documented, board-level engagement with the risk, proportionate to the organisation's actual exposure, rather than an assumption that the IT function or an outsourced provider has it handled without anyone at board level actually confirming that.

Why This Belongs At Board Level, Not Just Management's Desk

Cyber and data risk fits precisely within the risk appetite framework discussed earlier in this quarter. It is a category a board should explicitly address in its risk appetite statement, with tolerance levels stated rather than left implicit, and it connects directly to the delegations of authority discipline covered in the previous quarter: management should own the operational implementation, while the board retains oversight and cannot delegate away its responsibility for confirming that implementation is adequate, the same delegate-authority-not-responsibility principle this series has returned to repeatedly.

- Confirm whether your organisation is covered by the Privacy Act, by turnover or by the type of information and services it handles, and treat voluntary compliance seriously even if you sit below it, particularly where sensitive member information is involved.
- Include cyber and data risk explicitly in your risk appetite statement, with specific tolerance levels rather than a general acknowledgement that it matters.
- Confirm basic, low-cost controls are in place, multi-factor authentication, regular backups, and staff training, since these basic controls are consistently recommended by the Australian Signals Directorate and were among RI Advice's documented failings.
- Maintain an incident response plan and confirm it is tested, not just written, since the RI Advice case turned as much on failure to act on known vulnerabilities as on the original gaps themselves.
- Report cyber risk to the full board on a regular, standing cycle, connecting to the delegated authority and reporting discipline discussed earlier this quarter, rather than treating it as a specialist topic outside normal board oversight.

A board does not need deep technical expertise in cyber security to discharge this responsibility properly. It needs to treat the risk with the same governance seriousness applied to every other category this series has covered, oversight, documentation, and accountability, rather than assuming a technical problem sits permanently outside the board's own remit.

This is one of the practical governance topics built into our AI for Association Leaders course, alongside the papers, tools and frameworks that turn the principle into your board's actual practice. [Explore the course](#)

Annie Gibbins

Founder and CEO, Nexus Leadership

BOARDROOM ACTION WORKSHEET

Cyber and Data Governance as a Board-Level Risk, Not an IT One

Turn the resource into evidence, a decision and an accountable next step. Keep the completed record in your association's approved board records system.

1 What is the issue or decision?

State the governance question in one clear sentence.

2 What evidence do we already have?

Record the facts, source documents and stakeholder evidence available now.

3 What evidence is still needed?

Identify the legal, regulatory, financial, member or operational information still required.

4 What is the agreed next action?

Capture the owner, timeframe and how the matter will return to the board.

Action owner	Review date	Board decision or resolution

General education, not legal, financial, tax, clinical or governance advice. Confirm specifics at the relevant primary source or with your own qualified adviser. Nexus Leadership is operated by Lipstick Consulting Pty Ltd · ABN 15 619 120 482.

CONTINUE YOUR LEARNING

Turn governance principles into practical board action.

Self-paced courses, editable resources and practical support for association boards and CEOs at nexusleadership.com.au.