



GOVERNANCE RISK & OPERATIONS

Cyber Insurance: Covering the Threat You're Least Likely to Actually Face

Social engineering is a common cause of breaches, and it's often the category your policy covers the least. Check the sublimits directly

Social engineering, such as phishing and impersonation, is a significant cause of Australian data breaches and a common route into cyber incidents, according to OAIC notifiable data breach reports, and this specific category of loss is where many cyber insurance policies apply their tightest, least generous coverage. An association assuming its cyber policy broadly covers whatever a cyber incident throws at it may be relying on a policy least equipped to respond to one of the threats it is most likely to face.

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. [The Specific Gap Most Boards Do Not Know Exists](#)
2. [The Application Answers That Can Quietly Undermine A Claim](#)

The Specific Gap Most Boards Do Not Know Exists

Where an employee is deceived into transferring funds or disclosing credentials, without any actual system being technically compromised, some insurers classify the resulting loss as a crime loss rather than a cyber loss, placing it outside the policy's core insuring agreement entirely. Coverage for this specific scenario, social engineering fraud, is frequently only available as an optional add-on, and even where included, it commonly carries its own sublimit set considerably lower than the policy's overall aggregate coverage. An association could hold a policy with a headline limit in the hundreds of thousands or millions of dollars, while its actual protection against one of the most common real-world attack methods sits capped at a fraction of that figure. A cyber policy's headline coverage limit tells you very little about what it will pay on the types of loss your association is most likely to experience. That answer sits in the sublimits and exclusions schedule, not the summary page.

The Application Answers That Can Quietly Undermine A Claim

Security control representations made when applying for cyber insurance, whether multi-factor authentication is enforced, whether backups are regularly tested, become material facts the insurer relies on when pricing the policy. If an incident occurs and those controls turn out to have been missing or inconsistently applied, despite being confirmed in the original application, the insurer may be able to reduce, or in some cases refuse, the claim under the Insurance Contracts Act 1984, so the controls you declare must match your actual practice. This connects directly to the cyber security governance discussed earlier in this series: the controls described in a cyber insurance application are not a one-time checkbox exercise, they are an ongoing commitment the association's actual practice needs to match for as long as the policy remains in force.

- Confirm specifically whether social engineering and business email compromise fraud are covered under your policy's core insuring agreement or only as a separate, lower-sublimit add-on, given it is one of the most common ways attackers succeed.
- Read the full policy document, including the exclusions schedule, rather than relying solely on a broker's summary, since policy wordings have changed in ways summaries do not always reflect.
- Ensure the security controls represented in your cyber insurance application are accurate and continuously maintained, since a gap between what was declared and what exists is a recognised reason insurers dispute or reduce claims.
- Confirm the retroactive date on your policy, since a breach originating before that date will generally not be covered regardless of when it is discovered.
- Ask your broker directly how many cyber claims they have helped manage, and specifically how sublimits for social engineering and business interruption apply, rather than focusing the conversation only on overall limits and premium cost.

Cyber insurance is a valuable risk transfer tool, but only where an association actually understands what it covers, and equally important, what it specifically does not. The gap between the coverage a board assumes it has purchased and the coverage the policy will pay is exactly where an incident becomes a far more costly, uninsured problem than anyone expected.

This is one of the practical governance topics built into our Board Director 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 Insurance: Covering the Threat You're Least Likely to Actually Face

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.