NORTHSEAT
Governance. And Strategy.
That Performs.

Cyber Incident Response

ESSENTIAL SNAPSHOT

May 2026

Illustrative governance reference only - not a legal instrument or formal policy document.

Purpose

Cyber incident response is the governance structure for keeping incident classification, executive authority, legal review, insurer contact, regulator pathways, communications, evidence preservation and board reporting coherent during a cyber event.

The CEO and executive team run the response. The board owns oversight of the framework, thresholds, authority settings, reporting expectations and post-incident follow-up.

A disciplined Cyber Incident Response Plan should make clear:

- which events activate the plan;
- who declares and classifies the incident;
- which incidents require board notification;
- what the CEO can authorise during the first hour;
- who controls legal, insurer, vendor, client, regulator and media communications;
- how evidence, decisions and notifications are recorded;
- how the board receives updates without entering operational command;
- how post-incident findings are reported and assigned for action.

This snapshot helps Chairs, Directors, CEOs, CIOs, CFOs, risk leaders and Company Secretaries identify where cyber incident governance may be weaker than the existence of a CIRP suggests.

Why this matters now

Cyber incident response is now a live board, insurer, regulator, customer and transaction question.

Australian trigger points include the Cyber Security Act ransomware payment reporting threshold for entities with $3M+ annual turnover, OAIC Notifiable Data Breach assessment, APRA CPS 234 obligations where applicable, SOCI Act reporting for designated critical infrastructure, ASIC's continuing focus on cyber resilience and continuous disclosure, and insurer evidence demands at claim and renewal.

A cyber incident creates two problems at once: the technical event itself, and the governance record that explains who knew what, who decided what, and why.

Before you scroll on....

⚠️ Could your current CIRP explain who declares the incident, who commands the response, who notifies the board, who approves external communications, which regulatory pathways are considered, and what record is created afterwards?

Where cyber incident governance breaks down

Cyber incident weakness usually develops through repeated habits that look harmless before an incident.

1.0 The CIRP is approved without being exercised 🚧

👉 The board receives the plan annually.
👉 Management confirms it has been reviewed.
👉 No one has walked through a ransomware, data breach, supplier compromise or degraded-communications scenario with current people and vendors.

⚠️ Consequence: the board has a plan, but limited evidence that the plan can be used.

2.0 Incident authority is unclear

👉 The CIRT Lead, CEO, legal, communications and insurer each hold part of the response.
👉 The plan does not show who decides when time is short.

⚠️ Consequence: containment, notification and communication decisions can stall while people work out who owns the call.

3.0 Board notification lacks a clear threshold

👉 “Material” or “significant” is understood differently by directors, the CEO, IT, legal and risk.
👉 The Chair may receive updates too late, too often, or in the wrong format.

⚠️ Consequence: directors may start managing the response, or receive too little information to discharge oversight properly.

4.0 Regulator, insurer and evidence pathways sit outside the plan ❌

👉 Cyber insurance conditions, panel vendors, legal privilege protocols, forensic evidence handling, and regulator notification pathways (OAIC, ASIC, APRA, ACSC, SOCI, contractual) may sit in separate documents.
👉 The incident team may find them only after the event starts.

⚠️ Consequence: the first day is spent reconstructing authority, contact points and obligations instead of executing the response.

⚠️ The incident plan, escalation thresholds, communication authority, insurer pathway, notification record and post-incident review form one connected cyber governance record. Weakness across several points makes the response harder to explain later.

Common tension points in a cyber response

Every tension point below is a governance signal. Boards with disciplined cyber incident practice use these moments to clarify authority, escalation, notification, communication and the integrity of the record.

🔍 These are the most common tension points we see, including in otherwise well-managed organisations.

Tension point	Questions to ask (but rarely are)
Existing CIRP as comfort	🔍 If a serious cyber incident hit tonight, would the board know whether the CIRP has ever worked outside the document?
First-hour authority	🔍 Who declares a cyber incident - and would the CEO, CIO and Chair all name the same person?
Board–executive line	🔍 Has management been authorised to act first and report next, or would the board slow the response by seeking comfort in real time?
Single authorised voice	🔍 If the incident reached clients or the media tomorrow, who speaks for the organisation - and would every director know it isn't them?
Decision record	🔍 If a regulator or insurer later asked how the board governed the incident, could anyone show who decided what, when and why?

⚠️ If these questions feel familiar, cyber incident governance should be reviewed before the next insurer renewal, regulator question, transaction, audit, tabletop exercise or board review cycle.

Which next step fits your board?

Situation	Best next step
We want to see whether our current CIRP has governance gaps	Complete the Cyber Incident Response Governance Assessment
No Board-approved CIRP exists, or the current document is informal	Start with the Foundation Edition
We have a CIRP, but it does not shape testing, escalation, board reporting, insurer contact, regulatory pathways, communications or post-incident review	Move to the Governance Edition
For organisations operating under the highest levels of accountability	Discuss Institutional design and implementation

Trigger moments

Cyber incident ambiguity becomes expensive at predictable points. Boards usually act around one of the following:

- ransomware, cyber extortion, ransomware payment decision or data breach;
- insurer, lender, auditor, funder, regulator or customer evidence request;
- new Chair, CEO, CIO, CFO, risk leader or Company Secretary;
- M&A, sale, PE investment, refinancing or due diligence;
- third-party technology failure or supplier compromise;
- failed tabletop exercise or incident debrief;
- public-trust, client-service or media exposure.

If any of these are visible on your horizon, cyber incident governance should be formalised before the next external question controls the timetable.

Our frameworks are:
👉 **Board-ready**: informed by ISO/IEC 27035, ISO 37000, Corporations Act director and officer duty principles, Privacy Act and Notifiable Data Breaches Scheme requirements, ASX Listing Rules continuous disclosure obligations and Corporate Governance Principles where relevant, APRA CPS 234 where applicable, and current Australian cyber governance expectations.
👉 **Behavioural governance**: designed for how boards and executives make decisions when facts are incomplete, systems are unavailable, advisers disagree, communications are sensitive, and informal authority can distort escalation.
👉 **Clear**: gives Directors, Chairs, CEOs, CIOs, CISOs, CFOs, Company Secretaries, legal, communications, risk, insurers and vendors shared language for incident declaration, severity, notification, authorised voice, evidence records and board reporting.
👉 **Practical**: connects the CIRP to the Risk Appetite Statement, Risk Management Framework, Business Continuity Plan, Delegation of Authority, cyber insurance conditions, vendor register, incident log, situation reports, post-incident review and board minutes.

Why this gets postponed

Boards can recognise the gap, and still delay closing it.

❌ "We already have a CIRP."
📌 The test is use. Has it shaped incident classification, CEO authority, board notification, insurer contact, regulator pathways, client communication, evidence preservation and post-incident review?

❌ "Our IT provider handles this."
📌 The provider may help contain the incident. The board still needs a governance frame for authority, escalation, reporting, communication and follow-up.

❌ "This belongs with management."
📌 Management runs the response. The board owns oversight of the framework, thresholds, reporting expectations, authority boundaries and post-incident accountability.

❌ "This will create more governance work."
📌 Clear cyber incident governance reduces repeated debate during the event. It gives management authority to act and gives directors the information they need at the right level.

❌ "We can update this during the annual review."
📌 Insurer, regulator, customer, supplier and transaction questions rarely wait for the policy calendar. A stale CIRP creates work when the organisation has the least spare capacity.

❌ "We have never had a major cyber incident."
📌 The question is whether the organisation can explain its response if one occurs tomorrow.

Application across contexts

The Foundation and Governance Editions are informed by recognised Australian governance reference points set out on page 5. Each board must adapt its CIRP to the organisation's size, structure, risk appetite, data holdings, regulatory exposure, cyber insurance conditions, supplier reliance, client obligations and operating model.

Recognised governance practice provides a reference point. Departures should be deliberate, documented and risk-assessed for their effect on role clarity, escalation, recovery priorities, board reporting and post-incident review.

The Foundation and Governance Editions are adaptable to a wide range of organisational contexts including private companies, listed companies, not-for-profits and government entities.

NorthSeat works with Boards and executive teams across private, listed, NFP and government sectors to improve governance maturity and leadership alignment.

About This Essential Snapshot

This Essential Snapshot is provided by NorthSeat as a free governance resource for board leaders.

You are welcome to:
✅ Share this document with your board, colleagues, or governance networks
✅ Reference insights in board discussions or strategy sessions
✅ Forward the download link to others who might find it valuable
✅ Print or save for personal use

We ask that you:

- Attribute content to NorthSeat when sharing or referencing
- Share the original document (don't alter, rebrand, or misrepresent content)

Not permitted:
❌ Selling or licensing this document
❌ Using this as a commercial training product without permission
❌ Removing NorthSeat branding or attribution
❌ Using this content to create competing products or services

This Essential Snapshot is a starting point. For structured frameworks or board-ready policies, contact us:

📧 liam@northseat.com.au | 🌐 www.northseat.com.au

This document does not constitute legal, governance, or professional advice. Directors should seek independent advice for governance, legal, or compliance matters.

NORTHSEAT