Ransomware Response: A Director’s Governance Brief

What to ask, what to know, what to do in the first 48 hours

Purpose of This Document

This brief is designed to support directors in the critical early hours of a ransomware incident. It supplements the Australian Government's Ransomware Playbook with board-specific guidance on governance, disclosure, and oversight responsibilities.

Director's Role in Ransomware Incidents

Directors are not cyber responders — but they are accountable for overseeing an organisation's risk management, fiduciary duties, and public accountability. A ransomware incident can be material to:

- Shareholder value
- Regulatory compliance
- Public trust and licence to operate

Directors must ensure that the response is:

- Legally sound
- Strategically aligned
- Ethically justifiable

Immediate Questions for the Board to Ask

1. What systems and data have been affected?

2. Have we isolated the breach to prevent spread?

3. Has the Australian Cyber Security Centre (ACSC) been notified?

4. Are we aware of any obligations to notify regulators or customers?

5. What backups exist and have they been tested?

6. Has legal counsel been engaged regarding ransom payments and disclosure obligations?

7. Are we considering or rejecting ransom payment — and what legal risks are attached?

8. Who has decision authority on payment, and is the board involved?

9. Do any threat actors appear on DFAT's sanctions list?

10. What is our communications strategy — internal, media, regulators, and the public?

Governance Actions in the First 48 Hours

Day 1:

- Convene an urgent board or subcommittee briefing
- Confirm reporting to ASD if a ransom payment is being considered (Cyber Security Act 2024 requirement)
- Request briefing from CISO or external cyber advisors
- Ensure legal review of:
    - Payment implications under sanctions law
    - Disclosure obligations under ASX or sectoral regulations
    - Approve communication protocols for staff, stakeholders, and media

Day 2:

- - Review incident response execution and confirm containment
- - Reassess risk appetite and decision on ransom
- - Approve decision (if needed) on whether to engage third-party negotiators
- - Assess need to disclose incident to customers or investors
- - Mandate forensic investigation to inform lessons learned

Governance Decision Matrix (Simplified)

Decision Point	Responsible Role	Board Oversight?
Incident containment	CISO / CIO	No, but must be briefed
Ransom payment	CEO + Legal	Yes, especially if payment > $100k or sanctions risk
Regulator notification	GC / Compliance	Yes
Customer disclosure	CEO + Comms	Yes
Insurance notification	CFO	Yes

Board Risk Considerations

- Legal exposure: Civil or criminal penalties if ransom is paid to a sanctioned entity
- Insurance exposure: Breach of policy conditions if notification not timely
- Reputational damage: Media handling and stakeholder trust
- Repeat targeting: Organisations that pay are statistically more likely to be targeted again

Relevant Frameworks and Obligations

- Cyber Security Act 2024: Mandatory ransom payment reporting within 72 hours
- DFAT Sanctions: Unlawful to pay certain entities
- ASIC Expectations: Cyber risk governance is a core board responsibility
- ISO 27001 / NIST CSF: Internationally aligned frameworks support best practice

Final Word to Directors

Boards are not required to stop every cyber incident, but they are expected to govern cyber risk with the same seriousness as financial, legal, or operational risk. This document is a compass, not a manual. Use it to:

- Ask smarter questions
- Frame ethical decisions
- Stay out of legal jeopardy
- Guide your organisation through crisis with authority

For full incident response procedures, refer to the Australian Cyber Security Centre's Ransomware Playbook: https://www.cyber.gov.au/ransomware-playbook