FUJIFILM
Value from Innovation

IT Services

The Governance Imperative:

Cyber Resilience in Healthcare

A Board-Level Guide

Table of Contents

Healthcare in a Heightened Threat Environment

Healthcare organisations operate in one of Australia's most persistently targeted cyber environments. According to the Office of the Australian Information Commissioner (OAIC), health service providers consistently account for one of the highest proportions of reported notifiable data breaches across sectors. In the most recent reporting period, healthcare was the most affected industry.[1]

At the same time, the Australian Cyber Security Centre (ACSC) continues to identify ransomware as one of the most significant and disruptive cyber threats facing Australian organisations, particularly those delivering critical services.[2] Healthcare is considered especially vulnerable due to the operational urgency of its services and the enduring value of health information.

Health data cannot be "reset." It contains identity markers, clinical histories, Medicare details and deeply personal information. When compromised, the impact extends well beyond financial loss. It affects trust, patient relationships and institutional reputation.

For boards and executive leaders, this places healthcare cyber risk at the intersection of:

- **Sensitive Personal Data**
- **Continuous Operational Dependency**
- **Expanding Regulatory Scrutiny**
- **Public and Community Trust**

Cyber resilience must therefore be considered not merely as a technology issue, but as an enterprise risk with governance implications.

Board Consideration

If a significant cyber incident occurred tomorrow, could the organisation demonstrate structured oversight of cyber risk at board level?

Breach Frequency and Reputational Consequences

The Notifiable Data Breaches (NDB) scheme continues to demonstrate sustained breach activity within the health sector, with 20% of all breaches reported coming from health service providers. The majority of reported breaches across industries are attributed to malicious or criminal attacks, including ransomware and phishing.[3]

The ACSC Annual Cyber Threat Report highlights that ransomware incidents remain prevalent and disruptive, often resulting in system outages, data exfiltration and operational interruption.[4] For healthcare organisations, the operational impact can be particularly acute , as disruptions to clinical systems can delay patient care, restrict access to electronic medical records, interrupt diagnostic services and force hospitals to divert patients or revert to manual processes.

Unlike sectors that can temporarily suspend operations, healthcare and aged care providers rely on constant system availability. Cyber incidents may disrupt:

- **Electronic Medical Record Access**
- **Diagnostic and Imaging Systems**
- **Medication Management Platforms**
- **Patient Scheduling**
- **Billing and Claims Processing**

Operational downtime carries a multiplier effect:

Care Delivery Disruption

Financial Cost

Reputational Harm

The reputational dimension is particularly significant. Healthcare providers operate on trust. When sensitive health information is compromised, the erosion of public confidence can be difficult to restore.

Key Insight

In healthcare, cyber incidents are not solely data events. They are trust events.

Expanding Regulatory Accountability

Australia's regulatory landscape reinforces that cyber resilience is both a governance and operational responsibility , requiring oversight at the board and executive level as well as effective controls and management across day-to-day operations.

Under Australian Privacy Principle 11 (APP 11) of the Privacy Act 1988 (Cth), entities must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. This requires proactive measures, such as encryption, access controls, staff training, and secure destruction of data no longer needed.[5]

Recent legislative amendments have significantly strengthened enforcement powers and increased maximum penalties for serious or repeated privacy breaches.[6] This reflects a broader policy direction toward stronger corporate accountability in data protection.

Where applicable, APRA Prudential Standard CPS 234 – Information Security places explicit accountability on boards of regulated entities to ensure that information security capabilities are commensurate with vulnerabilities and threats.[7] Although not all healthcare providers fall under APRA supervision, CPS 234 reflects the broader regulatory expectation that cyber governance must be actively overseen at board level.

Healthcare and aged care providers may also operate within:

- **State-based Health Records Legislation**
- **Aged Care Quality Standards Governance Requirements**
- **Contractual Cybersecurity Obligations Imposed by Funders or Partners**

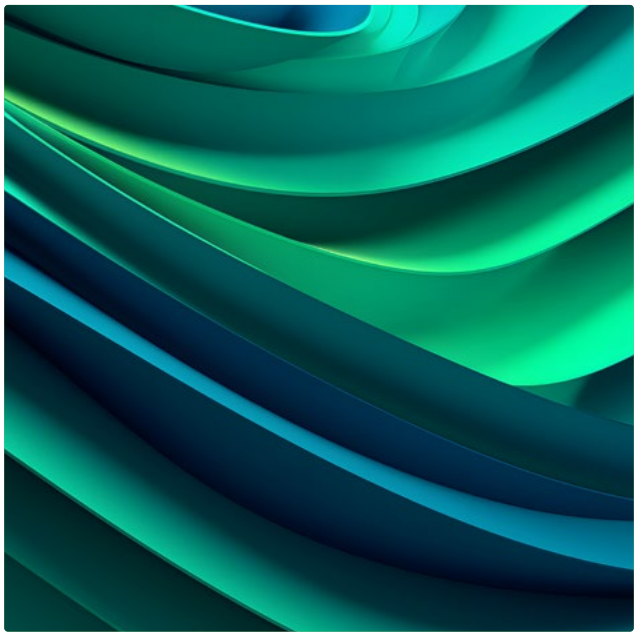
Across these frameworks, regulatory attention increasingly focuses on:

- **Evidence of Structured Oversight**
- **Regular Risk Assessment**
- **Defined Incident Response Processes**
- **Ongoing Control Testing**

Importantly, regulators assess whether "reasonable steps" were taken to protect sensitive information and minimise the risk of unauthorised access, disclosure or loss — not merely whether a breach occurred.

Board Reflection

Can we evidence that cyber risk is integrated into enterprise risk management and regularly reviewed at board level?



Operational Downtime as a Patient Safety Risk

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has consistently identified ransomware as a top-tier threat to Australia, noting its ability to cause significant, often crippling, disruption to critical infrastructure and essential services.[8] In healthcare settings, the consequences of downtime extend beyond administrative inconvenience.

Disruption may impact:

- **Clinical Documentation Access**
- **Medication Management Systems**
- **Communication with Patients and Families**
- **Staff Rostering and Payroll**
- **Referral and Diagnostic Workflows**

In aged care environments, system outages may directly affect resident safety and continuity of care , as providers rely on digital systems to manage medication

administration, clinical records, care planning and staff coordination for residents who often require continuous support. This reframes cyber resilience as a component of patient safety and service continuity.

For boards and executive leaders, governance considerations may include:

- Has executive-level incident response been exercised within the past 12 months?
- Are business continuity and disaster recovery plans aligned with cyber scenarios?
- Is third-party risk formally assessed and documented?
- Are patients and clinicians adequately protected?
- Is sensitive data adequately protected?
- Does the board receive meaningful reporting on cyber posture and risk exposure?

Healthcare organisations operate at a convergence point: high-value sensitive personal data, operational dependency and regulatory oversight.

In this environment, cyber resilience is not an isolated IT matter. It is a governance imperative.

Conclusion

From Technical Control to Enterprise Accountability

Healthcare organisations are operating in an environment defined by rising breach frequency, expanding regulatory accountability and increasing operational consequences.

In this context, cyber resilience cannot remain a peripheral IT matter. It must be treated as an enterprise risk — embedded within governance frameworks, regularly reviewed at board level and aligned to operational continuity planning.

Regulators increasingly assess whether "reasonable steps" were taken to identify, manage and mitigate cyber risk. Demonstrable oversight is no longer optional; it is expected.

For boards and executive teams, this raises a practical question:

Do We Have a Clear, Evidence-based Understanding of Our Current Risk Posture?

Without structured assessment, cyber maturity is often assumed rather than measured.

Establishing a formal risk baseline enables organisations to:

- **Benchmark Against Recognised Frameworks such as the Essential Eight**
- **Identify Material Control Gaps and Prioritise Remediation**
- **Strengthen Board Reporting and Documentation**
- **Demonstrate Proactive Governance in the Event of Regulatory Scrutiny**

In a sector where operational resilience and patient trust are paramount, moving from assumption to assessment is a critical step.

Healthcare leaders seeking greater clarity over their cyber exposure can undertake a structured cybersecurity assessment to evaluate current controls, governance maturity and resilience alignment.

Further information on our Cybersecurity Assessment framework is available here:

[1] Office of the Australian Information Commissioner. Notifiable data breaches report (July to December 2024). Retrieved from: https://www.oaic.gov.au/__data/assets/pdf_file/0021/251184/Notifiable-data-breaches-report-July-to-December-2024.pdf

[2] Australian Cyber Security Centre (2025). Annual Cyber threat Report 2024–2025. Retrieved from: https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

[3] Office of the Australian Information Commissioner. Notifiable data breaches report (July to December 2024). Retrieved from: https://www.oaic.gov.au/__data/assets/pdf_file/0021/251184/Notifiable-data-breaches-report-July-to-December-2024.pdf

[4] Australian Cyber Security Centre (2025). Annual Cyber threat Report 2024–2025. Retrieved from: https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

[5] Office of the Australian Information Commissioner (2025). Chapter 11: Australian Privacy Principle 11 — Security of personal information. Retrieved from: https://www.oaic.gov.au/__data/assets/pdf_file/0035/256958/APP-Guidelines-Chapter-11-Security-of-personal-information-October-2025-v1.3.PDF

[6] Parliament of Australia, Department of Parliamentary Services (2022). Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. Retrieved from: https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/8863742/upload_binary/8863742.pdf

[7] APRA (2018). Prudential Standard CPS 234 Information Security. Retrieved from: https://www.apra.gov.au/sites/default/files/Draft-CPS-234.pdf

[8] Australian Cyber Security Centre (2025). Annual Cyber threat Report 2024–2025. Retrieved from: https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

fujifilm.com/fbau

FUJIFILM

FUJIFILM Business Innovation Australia Pty Ltd
Level 2, 54 Waterloo Road, Macquarie Park, NSW 2113 Australia
Contact us at fujifilm.com/fbau or 13 14 12