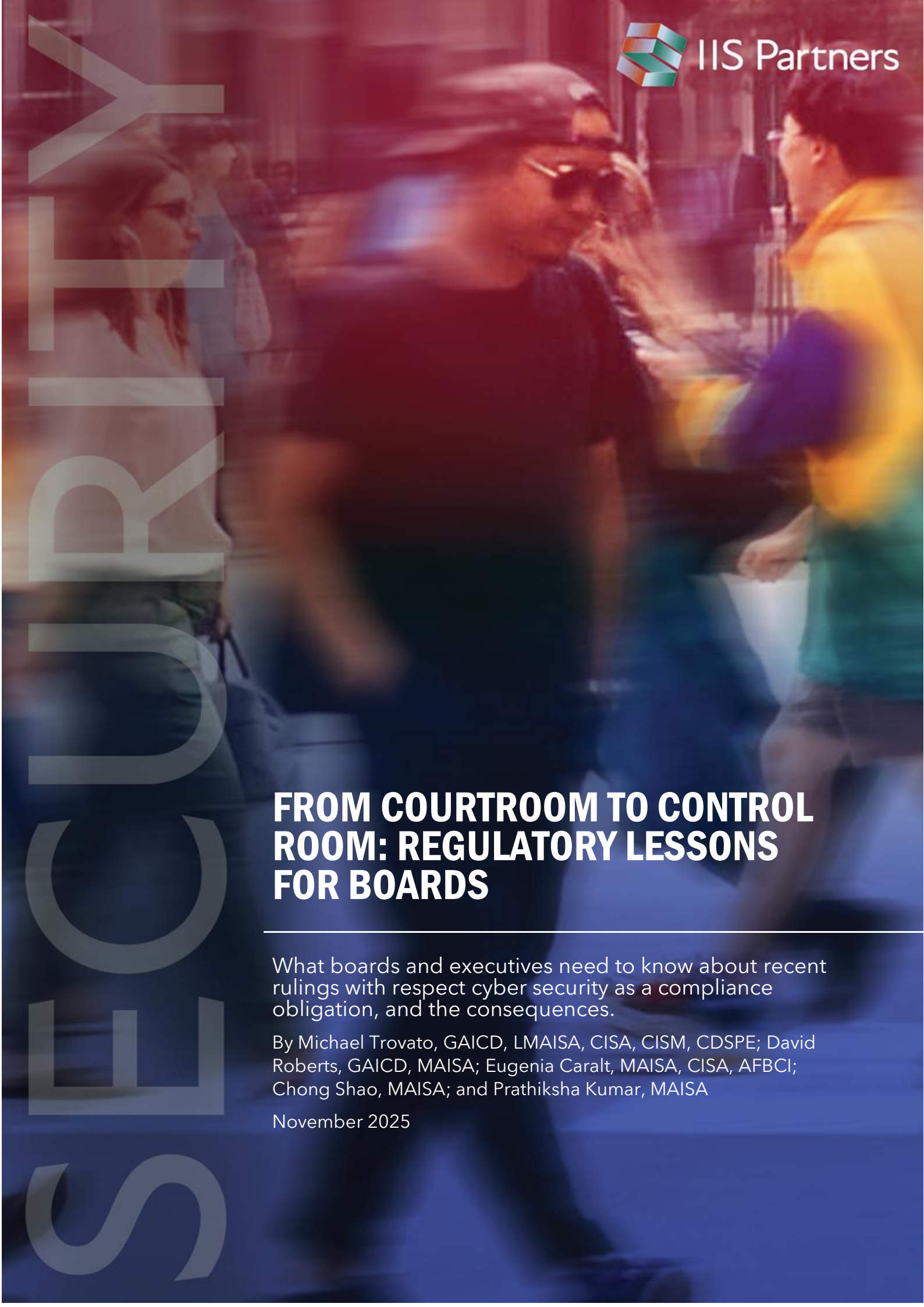


IIS Partners

FROM COURTROOM TO CONTROL ROOM: REGULATORY LESSONS FOR BOARDS

What boards and executives need to know about recent rulings with respect cyber security as a compliance obligation, and the consequences.

By Michael Trovato, GAICD, LMAISA, CISA, CISM, CDSPE; David Roberts, GAICD, MAISA; Eugenia Caralt, MAISA, CISA, AFBCI; Chong Shao, MAISA; and Prathiksha Kumar, MAISA

November 2025

The Federal Court made explicit what had long been implied: cyber security is integral to risk management and therefore a legal governance duty.

Introduction

Cyber security has become a top consideration in corporate governance. Australian regulators – including Australian Securities and Investment Commission (ASIC) and the Office of the Australian Information Commissioner (OAIC) – are reframing cyber security as a legal obligation, not just a technical or compliance issue, and defining what reasonable security measures look like.

Further, the courts are sending a consistent message: boards cannot outsource accountability. Governance now demands visible, demonstrable assurance that cyber security and privacy risks are actively managed and that organisations are compliant with the *Privacy Act 1988* (Cth), especially **Australian Privacy Principle (APP) 11 (Security of personal information)**.

Drawing from notable court cases and proceedings – RI Advice (2022), McClure (2025), Medibank (2024), Optus (2025), and Australian Clinical Labs (2025) – and the inputs we heard at Australian Information Security Association (AISA) CyberCon 2025 from the OAIC, IIS Partners, TrustWorks360 and our panellists, [1] this paper explores how boards and executives must evolve.

It charts the path from courtroom lessons to boardroom practice, identifying how governance expectations are tightening and what directors must do to stay ahead. **The message is clear**: regulators regard a failure to take reasonable steps as occurring where:

- Organisational and technical controls to manage cyber security risk are available;
- The entity ought reasonably have been aware of them; and
- In the circumstances it would have been reasonable to apply them, but they were not implemented.

The legal turning point for boards

The modern concept of cyber security governance in Australia begins with ASIC v RI Advice (2022) [2], the case that changed how regulators view directors' duties in the digital era. RI Advice was found to have breached its general licence obligations by failing to maintain adequate cyber security systems. The Federal Court made explicit what had long been implied: cyber security is integral to risk management and therefore a legal governance duty.

RI Advice has cemented cyber security resilience as a relevant risk that licensees needed to cover. It means that existing legislation (in this case s 912A(1) of the *Corporations Act 2001* (Cth)) could be applied because cyber security risk management was now a 'risk management system' for the purposes of the act. What flowed from that was directors now had to become aware as they hold ultimate responsibility for the act. If ASIC takes action against directors for cyber security resilience breaches it will likely be a stepping-stone case for exposing companies to risk and penalties.

Boards and directors must be able to demonstrate how they assure themselves that cyber security risks are being identified, managed, and remediated in dynamic environment based on what data they hold.

Policies, awareness sessions, and delegated responsibilities are no longer enough. Boards and directors must be able to demonstrate how they assure themselves that cyber security risks are being identified, managed, and remediated in dynamic environments based on what data they hold.

This means embedding cyber security oversight within enterprise risk frameworks, ensuring regular reporting, internal assurance, and commissioning independent reviews. It also means the Board – not the IT team – sets the appetite for risk, monitors controls, and demands evidence of their effectiveness.

More recently, McClure v Medibank (2025) [3] expanded the concept of accountability beyond prevention to include response. In the wake of Medibank's 2022 breach, a 'Big 4' consulting firm was commissioned to investigate the incident. The Federal Court later held that Medibank could not claim legal privilege over the report, as it served multiple purposes – operational review, communications management, and regulatory response – not solely legal advice.

The case extends the duty of care into how organisations respond when things go wrong. Boards must ensure that post-incident processes are disciplined, transparent, and clearly documented, balancing public accountability with legal protection – essentially to 'do the right thing' for the organisation's customers.

Moreover, during CyberCon 2025, we heard OAIC's Director of Investigations in the Regulatory Action Division, Warren Jacobs, stressing that regulatory expectations now prioritise:

- Adherence to recognised frameworks and the operationalisation of standards such as ISO 27001 Information Security Management System (ISMS), the Australian Signals Directorate (ASD) Essential Eight, or USA National Institute for Standards and Technology NIST Cybersecurity Framework (CSF), not simply their documentation;
- A risk-based approach to inform the implementation of tailored, well-designed controls that are updated with regularity, not a 'set and forget' approach or an attempt to blindly offload the risk to third parties; and
- Continuous executive oversight, assurance that the controls are working as intended and continual improvement as the risk landscape changes.

The OAIC's argument positions cyber security as a measurable standard of practice under privacy law. It reinforces that 'reasonable steps' under APP 11.1 are not static – they evolve with the threat environment and the organisation's scale.

The privacy reckoning

If the RI Advice decision established cyber security as a boardroom issue, the recent wave of OAIC actions against major organisations has transformed it into a privacy and data governance mandate. A common thread runs through these cases: failures of oversight and proportionality.

The Medibank case: security by design, accountability by default

In 2024, the Australian Information Commissioner launched civil penalty proceedings against Medibank [4], alleging that the company failed to take reasonable steps to protect personal information (APP 11.1). The case focused on systemic weaknesses – remote access without multi-factor authentication, insufficient alert triage, and a lack of timely breach detection – that exposed sensitive health information of 9.7 million Australians.

What makes the Medibank proceedings significant is not the scale of the breach (resulting in a potential, although unlikely $21 trillion fine) but the nature of the allegations – namely, that Medibank failed to take reasonable steps, especially for the size of the organisation, the sensitivity of the personal information, and based on its knowledge of compliance gaps and risks.

The OAIC's argument positions cyber security as a measurable standard of practice under privacy law. It reinforces that 'reasonable steps' under APP 11.1 are not static – they evolve with the threat environment and the organisation's scale. Boards can no longer rely on broad assurances; they must insist on specific, evidence-based reporting about system resilience and incident readiness.

The Optus and ACL cases: Proportionality and due diligence

The OAIC's subsequent actions against Optus and Australian Clinical Labs (ACL) demonstrate the regulator's proactive enforcement approach and intent to send a clear message to industry.

In AIC v Optus (2025) [5], the Commissioner alleges that Optus failed to take reasonable steps to protect personal information for over three years. The alleged failings – exposed interfaces, inadequate segregation, and under-tested controls – reflect a pattern of insufficient governance over large-scale data holdings. For boards, the case underscores the principle of proportionality: the greater volume and sensitivity of the data, the higher the standard of care.

Boards must ask harder questions – not only about whether cyber security frameworks exist, but whether they work in practice, at scale, and in today's dynamic risk environment.

By contrast, AIC v ALC (2025) [6] demonstrates that liability can extend beyond operational errors to strategic oversight. ACL acquired a business with known cyber security vulnerabilities and delayed assessing and notifying a subsequent breach. **The Federal Court's $5.8 million penalty – the first of its kind under the Privacy Act** – signals that due diligence must extend to cyber security maturity in mergers and acquisitions. Inherited weaknesses are not a defence; they are a foreseeable risk.

Further, there may be peril for ACL directors, as the Federal Court hinted that as this pertains to the ASIC Act and the Corporations Act, a 'serious contravention' occurred. ACL could face further multi-million-dollar penalties under the Corporations Act; court-mandated reforms to its risk management and data governance; or potential director disqualifications for poor oversight. This effectively could be a 'Cyber Centro', such as the landmark 2011 Federal Court decision that found directors of the Centro Properties Group breached their duty of care and diligence by failing to detect major errors in the company's financial statements.

Across these cases, the lesson is that regulatory expectation has moved from procedural compliance to provable resilience. Boards must ask harder questions – not only about whether cyber security frameworks exist, but whether they work in practice, at scale and in today's dynamic risk environment.

'***Cyber security failures are, at their core, board and governance failures***,' according to Malcolm Crompton AM, former Australian Privacy Commissioner, who for a long time now has promoted the message that boards must recognise data as both an organisation's greatest asset and its greatest liability and therefore embed its protection within corporate risk registers and assurance programs.

Governance in practice

Australian regulators now converge on a single expectation: cyber security and privacy governance must be demonstrable. Boards cannot rely on high-level assurances; they need structured, repeatable evidence that controls are fit for purpose.

OAIC's Director of Investigations in the Regulatory Action Division, was clear at CyberCon 2025 that regulatory expectations have matured beyond static compliance. He emphasised that regulators now look for authentic operationalisation of recognised frameworks. Policies and procedures alone are insufficient; organisations must demonstrate that these controls function in practice, are continuously tested, and are supported by evidence such as audit trails and independent reviews.

Boards that treat [cyber security and privacy] as governance disciplines, not technical issues, are best positioned to build lasting trust with regulators, customers, and investors.

True governance maturity involves three dimensions: accountability, assurance, and adaptability.

- **Accountability** ensures that ownership of cyber security risk is explicit and distributed. The board sets the tone by defining risk appetite, allocating budgets, and integrating cyber security resilience into strategic decisions. This includes verifying that executives understand their accountability and that board committees – such as Audit and Risk – have clear oversight roles.
- **Assurance** means that frameworks are operationalised and tested. Boards should require independent validation of control effectiveness, not just internal attestations. Regular penetration tests, audits, and scenario exercises should feed into risk reporting that directors review and question.
- **Adaptability** recognises that cyber security risk is dynamic. Governance must evolve with it. Lessons from incidents (including external ones) should drive continuous improvement, and boards should monitor how quickly recommendations are actioned. Regular reflection on emerging threats, technology dependencies, and human factors helps foster a positive governance culture.

From compliance to performance

The courtroom has redrawn the boundaries of accountability. Cyber security and privacy resilience are now legal, financial, and reputational imperatives – core elements of directors' fiduciary duty.

Boards that treat these as governance disciplines, not technical issues, are best positioned to build lasting trust with regulators, customers, and investors.

From RI Advice (2022) to Optus (2025), Australian jurisprudence and regulatory practice have confirmed that 'reasonable steps' now means evidence-based assurance: continuous validation, documented oversight, and alignment between policy and practice. Confidence will no longer come from frameworks on paper, but from proof that governance performs under pressure.

Organisational resilience is the entity's ability to adapt and evolve in the face of short-term shocks as well as long-term changes. From a data and privacy perspective, the data deluge greatly increases the prevalence and impact of both types of challenges. In the shorter term, entities must watch out for privacy missteps and cyber security breaches. In the longer term, the viability of entities may be threatened by changes to regulation and by data-driven competitors. The board should therefore be mindful of how both compliance and performance contribute to an entity's resilience and sustainability.

For Australian organisations, the message is clear: resilience is an outcome that results from good corporate governance and is a key leadership and culture issue. Those that embed privacy, security, and ethical technology into board strategy and culture will move decisively from compliance to confidence and performance.

Practical actions

For Boards
1. **Treat cyber security as a standing board risk item** – Require quarterly reporting on threat landscape, incidents, and control maturity. 2. **Ensure that the culture values customers and data** - Prioritise data privacy and data protection through training, leadership, accountability, ongoing risk assessments and documented policies, procedures and ICT. 3. **Given the technological, business and regulatory environment** – Understand in what ways is the data the entity holding an asset or a liability. 4. **Conduct independent privacy and cyber security reviews** – Validate the adequacy of frameworks and testing programs, including third party vendors. 5. **Embed privacy and security into governance frameworks** – Define roles, accountabilities, and escalation processes. 6. **With AI emerging as a new risk vector** – Directors must also ensure responsible AI use aligns with privacy, security, and ethical standards. 7. **Link executive incentives to resilience** – Align leadership performance metrics with cyber security outcomes. 8. **Ensure readiness for breach response** – Conduct simulations that include executive and board participation. 9. **Demand post-incident reviews** – Require reports that capture root causes, learnings, and systemic improvements. 10. **Invest appropriately in ICT** - Manage legacy IT systems and proactively identify the 'hidden costs' of keeping outdated technology, including costs masked by cost-cutting strategies.

For Executives

1. **Governance, accountability, and culture**
   a. Define an executive owner of protection of PI with delegated budget and KPIs.
   b. Provide regular board oversight through minuted reviews and risk appetite statements for privacy, data protection, and cyber security.
2. **Data inventory and classification**
   a. Establish and maintain a comprehensive inventory of all systems and data stores containing personal information, including type, sensitivity, purpose and owner.
   b. Assign classification that is consistent and reviewed whenever systems or processes change.
3. **Data retention, deletion, and minimisation**
   a. Provide for documented and operational retention and disposal schedules that ensure personal information is retained only as long as necessary.
   b. Automate or evidence deletion/de-identification, with approvals for exceptions and logs maintained.
4. **Access control and identity management**
   a. Enforce multi-factor authentication for all users, especially privileged accounts.
   b. Maintain a least-privilege access model consistent with the 'need to know' concept in the APPs, quarterly reviews, and automated joiner-mover-leaver processes.
   c. Manage controls with recognised frameworks such as NIST CSF and/or ISO 27001.
5. **Vulnerability and patch management**
   a. Conduct regular vulnerability scanning and risk-based patching (e.g. critical issues remediated within 14 days).
   b. Establish clear SLAs and metrics reported to management; exceptions documented and risk-accepted.
6. **Incident detection, response, and recovery**
   a. Provide for tested incident response and data breach plans with defined roles, escalation paths, and playbooks.
   b. Monitor logs for abnormal activity on high-value assets.
   c. Encrypt all data, including backups that are offline or immutable, and perform restoration tests quarterly.
   d. Ensure data breach assessments completed within 30 days and notification is timely.
7. **Third-party and supply-chain security**
   a. Establish a risk-based vendor management framework categorising vendors by data sensitivity.

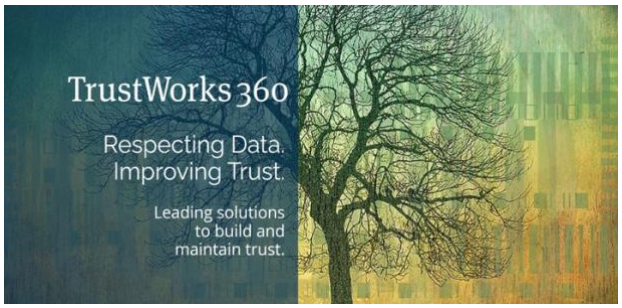
For Executives

b. Provide for pre-contract due diligence, annual reassessment and ongoing monitoring of vendor risk changes, with evidence-based assurance.
c. Ensure contracts include clear obligations for personal information protection and breach notification.

8. **People, training and culture**
   a. Provide role-specific privacy and cyber security awareness training at onboarding and annually, supplemented by ongoing campaigns (e.g. phishing simulations).
   b. Report on completion and behavioural outcomes to executives.
9. **Privacy by Design (PbD) and Privacy Impact Assessments (PIAs)**
   a. Use PbD principles for projects and complete PIAs for new or significantly changed systems or processes involving personal information.
   b. Assess proportionality, necessity, and security measures, with privacy lead sign-off before deployment.
10. **Independent assurance and continuous improvement**
    a. Perform annual independent review of key privacy and cyber security controls. Findings tracked to closure and lessons learned inform uplift programs.
    b. Continuous monitoring of control metrics (e.g. MFA coverage, patch SLAs, incident response tests) reported to the board.

This summary outlines the key personal information data protection capabilities and practices that a senior executive should expect to have in-place. These are designed to meet the expectations of 'reasonable steps' derived from our analysis of recent cases / findings by ASIC and OAIC. This is example set of actions, sufficiently executed, could be considered reasonable for a large organisation holding significant volumes of personal information.

Trustworks360 can assist with solutions across key capability domains required to support strong, automated data governance and protection, privacy, security, and compliance.



https://www.trustworks360.com

Appendix A – Case summaries

***ASIC v RI Advice* (2022) – Decided case**	
Allegations (ongoing) or findings (decided)	Federal Court found RI Advice breached ss 912A of the *Corporations Act 2001* (Cth) by failing to have adequate cybersecurity documentation and controls across its authorised representative network (May 2018 to August 2021). This was the first enforcement of cyber security obligations for an Australian Financial Services Licence holder.
Security practices that should have been taken	Operationalise and enforce cybersecurity controls; ensure ongoing supervision and review of control effectiveness; maintain oversight of external IT/service providers; regularly uplift frameworks to address emerging cyber security risks.
Legal exposure	Declaration of contravention; compliance orders under s 1101B to engage a cyber security expert to identify, implement and report on further measures; ordered to pay $750,000 in costs.
Lessons for Boards	Cyber security risk management is an ongoing obligation. Boards must maintain continuous assurance and oversight.

***McClure v Medibank* (2025) – Decided case**	
Allegations (ongoing) or findings (decided)	Federal Court found Deloitte's post-incident review was not privileged because it served multiple purposes (PR, ops, regulatory) beyond legal advice.
Security practices that should have been taken	No technical controls were at issue, but the case highlights the need for disciplined post-incident processes and controlled information flows.
Legal exposure	Although unrelated to a Privacy Act contravention, the loss of privilege exposed sensitive forensic findings to plaintiffs in ongoing litigation and regulators – creating litigation and reputational risk.
Lessons for Boards	Boards must ensure post-incident reviews are properly scoped and instructed through counsel if privilege is sought. Governance over investigations is critical.

AIC v Medibank (2024) – Ongoing case	
Allegations (ongoing) or findings (decided)	The Commissioner alleged Medibank failed to take reasonable steps (APP 11.1) to protect the personal and health information of ~9.7 million people between 2021 and 2022, amounting to serious interference with privacy.
Security practices that should have been taken	Mandatory MFA for remote access; stronger privileged-access and credential controls; timely alert triage and escalation; continuous monitoring; operate monitoring and response proportionate to the nature of the data.
Legal exposure	Civil penalty proceedings under s 13G of the Privacy Act. Maximum $2.22 million per contravention (applying pre-2022 penalty caps).
Lessons for Boards	'Reasonable steps' scale with data sensitivity and volume. Boards must demand proof that controls are effective, not just documented, and ensure incident readiness and third-party access oversight match the organisation's risk profile.

AIC v Optus (2025) – Ongoing case	
Allegations (ongoing) or findings (decided)	The Commissioner alleged Optus seriously interfered with the privacy of ~9.5 million people from October 2019 to September 2022 by failing to take reasonable steps to protect personal information (APP 11.1). Information exposed included contact details, dates of birth, and government identifiers and documents.
Security practices that should have been taken	Governance over internet-facing domains; access controls; layered security controls to avoid single point of failure; robust security monitoring processes; appropriately resourced privacy and cyber security functions; regularly review practices and systems.
Legal exposure	Civil penalty proceedings under s 13G of the Privacy Act. Maximum $2.22 million per contravention (applying pre-2022 penalty caps).
Lessons for Boards	Boards must evidence that 'reasonable steps' scale with organisational size and sensitivity of data. They must be extremely vigilant to significant threats and risks in today's cyber security landscape.

AIC v Australian Clinical Labs (2025) – Decided case	
Allegations (ongoing) or findings (decided)	Federal Court ordered ACL to pay $5.8 million for failing to protect personal information (APP 11.1) and for delays in breach assessment and notification (ss 26WH, 26WK of the Privacy Act). ACL knew the acquired Medlab systems were outdated and un-tested yet did not remediate before a 2022 attack exposed ~223,000 records.
Security practices that should have been taken	Implement and evidence adequate cyber security controls proportionate to the volume/sensitivity of the data and threat environment; identify and uplift inherited systems promptly post-acquisition; run timely breach assessment process; notify the OAIC as soon as practicable once aware an eligible data breach has occurred.
Legal exposure	First Privacy Act civil penalty judgment for a data breach. Penalty ($5.8 million + costs) reflects old limits; future cases may reach $50 million under amended penalty regime. Also deemed a serious contravention of the Corporations Act. ACL could face further multi-million-dollar penalties; court-mandated reforms to its risk management and data governance; or potential director disqualifications for poor oversight.
Lessons for Boards	Cyber security due diligence is critical in acquisitions. Boards must ensure timely breach assessment and notification and cannot ignore known vulnerabilities in inherited systems

Appendix B – Excerpts from OAIC Guidelines on APP 11

Key points

- An APP entity must take such steps as are reasonable in the circumstances to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take such steps as are reasonable in the circumstances to destroy the information or ensure that it is de-identified.
- This requirement applies except where:
  - the personal information is part of a Commonwealth record, or
  - the APP entity is required by or under an Australian law or a court/tribunal order to retain the personal information.
- Reasonable steps include technical and organisational measures.
- Many of the issues discussed in this Chapter are discussed in more detail in the OAIC's Guide to Securing Personal Information.[1]

What does APP 11 say?

- APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information.[2]
- An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1).
- An APP entity must take reasonable steps in the circumstances to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by or under an Australian law or a court/tribunal order to retain the personal information (APP 11.2).
- The reasonable steps an APP entity must take, for the purposes of ensuring the security of personal information and destroying or de-identifying personal information that is no longer needed, include technical and organisational measures (APP 11.3).[3]

---

[1] See: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information>.

[2] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 86.

[3] APP 11.3 was introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth). APP 11.3 applies to personal information held from 11 December 2024, regardless of whether the information was acquired or created before or after this date. APP 11.3 does not limit APP 11.1, APP 11.2 or any other provision in the Privacy Act.

Bibliography

[1] AISA CyberCon 2025 – From courtroom to control room: Regulatory lessons for security

Panellists: Stephen Fracalossi (Head of Cyber Security and Privacy at OES), Warren Jacobs, (Director of Investigations in the Regulatory Action Division at OAIC), David Roberts (Director Trustworks360), and Malcolm Crompton AM, Founder and Lead Privacy Advisor at IIS Partners and former Australian Privacy Commissioner.

[2] *Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022]* FCA 496. Available: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2022/2022fca0496. [Accessed 23 October 2025].

[3] *McClure v Medibank Private Limited [2025] FCA 167.* Available: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2025/2025fca0167. [Accessed 23 October 2025].

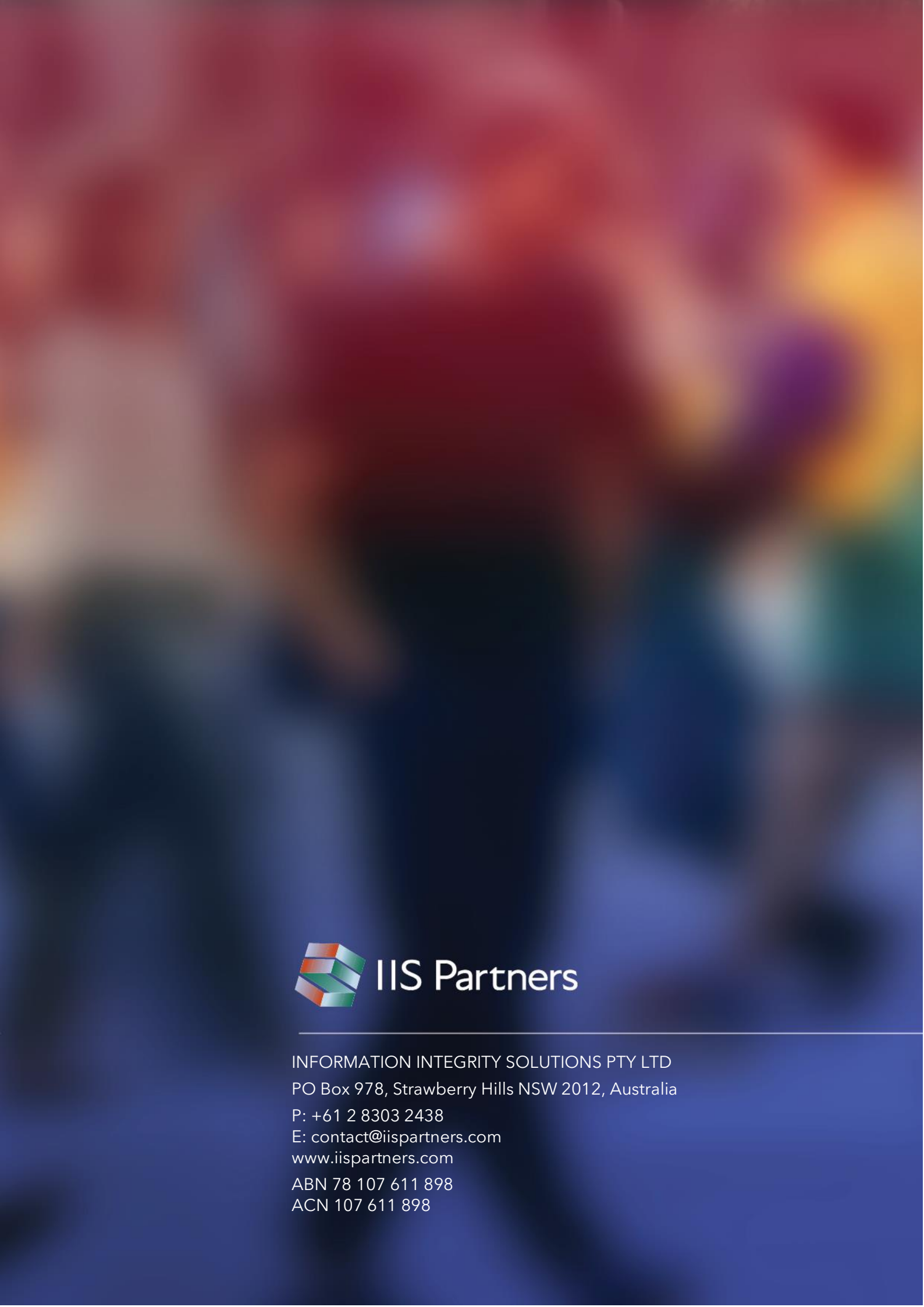
[4] Office of the Australian Information Commissioner, "OAIC takes civil penalty action against Medibank," 5 June 2025. [Online]. Available: https://www.oaic.gov.au/news/media-centre/oaic-takes-civil-penalty-action-against-medibank. [Accessed 20 October 2025].

See also OAIC's Notice of Filing, available: https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf. [Accessed 20 October 2025].

[5] Office of the Australian Information Commissioner, "Australian Information Commissioner takes civil penalty action against Optus," 8 August 2025. [Online]. Available: https://www.oaic.gov.au/news/media-centre/australian-information-commissioner-takes-civil-penalty-action-against-optus. [Accessed 20 October 2025].

[6] *Australian Information Commissioner v Australian Clinical Labs Limited (No 2) [2025] FCA 1224.* Available: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2025/2025fca0167. [Accessed 23 October 2025].

See also OAIC's press release: "Australian Clinical Labs ordered to pay penalties in relation to Medlab Pathology data breach in first for Privacy Act," 9 October 2025. [Online]. Available: https://www.oaic.gov.au/news/media-centre/australian-clinical-labs-ordered-to-pay-penalties-in-relation-to-medlab-pathology-data-breach-in-first-for-privacy-act. [Accessed 20 October 2025].



IIS Partners

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com
ABN 78 107 611 898
ACN 107 611 898