



NAVIGATING PERSONAL LIABILITY AND DIRECTOR DUTIES IN
AUSTRALIA'S CYBER LANDSCAPE

Whose Fault Is It Anyway?

INTRODUCTION: THE EVOLUTION OF ACCOUNTABILITY

For many years, the Australian SME sector perceived cybersecurity as a technical hurdle. It was often considered a matter of firewalls, passwords, and “leaving it to IT”. However, the digital world has changed, and so has the legal framework governing corporate responsibility. Cybersecurity has transitioned from a back-office technicality to a core fiduciary duty.

For business owners and directors, the “corporate veil”, the legal barrier that has traditionally separated personal assets from company liabilities, is becoming increasingly transparent in the event of a significant data breach. Regulators and courts now view the protection of digital assets with the same gravity as the management of a company’s financial solvency. The fundamental question for leadership is no longer “Are we secure?” but “Are we defensible?”

This shift in accountability was underscored by Joe Longo, Chair of the Australian Securities and Investments Commission (ASIC):

“*Let me be especially clear here, it is a foreseeable risk that your company will face a cyber attack... as a director you have to make it your business to be across questions of cyber resilience and make cyber security a priority.*

JOE LONGO, CHAIR, ASIC

For the Australian SME, this means that ignorance of cyber risks is no longer a valid legal defence. Understanding the intersection of statutory duties, privacy obligations, and digital resilience is now a critical component of governance.



THE LEGAL FOUNDATION

1 Statutory Duties and Cyber Risks

The foundation of director liability in Australia rests primarily within the Corporations Act 2001 (Cth). Specifically, Section 180(1) mandates that directors and officers exercise their powers with a degree of “care and diligence” that a reasonable person would exercise in their position.

The Duty of Care and Diligence

The provisions of Section 180 of the Corporations Act do not require a director to be a technical expert, but regulators and courts increasingly expect them to be “cyber-literate”. This term has become the judicial benchmark for whether a leader has exercised “care and diligence” as per the act.

A “reasonable person” in a leadership role is expected to understand the company’s risk profile and ensure that adequate resources are allocated to mitigate those risks. If a company suffers a catastrophic breach because its leadership ignored warnings or failed to implement industry-standard protections, it can be argued that the directors breached their statutory duty of care.

The “Stepping-Stone” Liability Principle

A significant development in Australian case law is the “stepping-stone” theory of liability. This principle allows regulators to use a company’s breach of a specific law, such as the Privacy Act, as a “stepping stone” to hold directors personally liable for a breach of their duties under the Corporations Act.

If a company fails to protect consumer data, it exposes itself to regulatory penalties, remediation costs, and reputational damage. Courts have ruled that by *allowing* the company to engage in conduct that leads to such a contravention, the directors have failed to act with the required care and diligence to protect the company’s interests. This effectively places the legal focus directly on the individuals in the boardroom.

THE SHIFT IN FOCUS

A breach of one law can become the stepping stone to personal liability under another. The legal focus moves from the company to the individuals in the boardroom.

2 Defining “Reasonable” Security

To avoid personal liability, a director must demonstrate that “reasonable steps” were taken to secure the business. However, the definition of “reasonable” is not static; it is informed by current industry standards and landmark legal precedents.

ASIC v RI Advice Group: Establishing the Minimum Standard

The landmark case of *ASIC v RI Advice Group Pty Ltd* provided the first clear signal from the Federal Court that cybersecurity is legally considered a foreseeable business risk. RI Advice, a large financial advisory firm, was found to have breached its obligations by failing to put adequate documentation and controls in place across its network. Notably, the court didn’t demand “impregnable” systems, acknowledging that zero risk is impossible. Instead, it emphasised that “adequacy” is measured by the implementation of recognised security frameworks and the active management of known vulnerabilities.

Australian Clinical Labs: The Cost of Over-Reliance

\$5.8m

Federal Court penalty against Australian Clinical Labs in late 2025, the first ruling of its kind under the Privacy Act following a cyber breach

In late 2025, the Federal Court issued a \$5.8 million penalty against hospital pathology company Australian Clinical Labs. This was the first ruling of its kind under the Privacy Act following a cyber breach. A critical takeaway from this judgement was the court’s rejection of “delegated responsibility”. The court noted that a company’s obligation to protect data is not discharged simply by hiring a third-party IT provider and doing nothing more.

ACCOUNTABILITY CANNOT BE OUTSOURCED

In other words, accountability cannot be outsourced. Engaging an external IT provider may be necessary, but leadership still has an obligation to ensure appropriate protections are actually in place, operating as intended, and reviewed over time.

3 Personal Rights and “Recklessness”

The landscape of privacy law in Australia has been significantly strengthened through various reforms, including the introduction of a statutory tort for serious invasions of privacy.

The Statutory Tort for Privacy

Under the statutory tort for privacy, individuals, such as customers or employees, can directly sue a director or owner if their privacy was invaded in an “intentional or reckless” way. In a digital context, “recklessness” is defined by the courts as a state of mind where a leader is aware of a substantial risk that a breach will occur and consciously chooses to ignore it. A common example is being advised by a security expert to update systems but failing to do so.

Removal of Small Business Exemptions

Historically, many small businesses with a turnover under \$3 million were exempt from the Privacy Act. However, recent legislative shifts have narrowed these exemptions, particularly for businesses handling sensitive data or those acting as contractors to larger entities. In the eyes of the law, the size of the business does not diminish the director’s responsibility to protect the information they steward.

The Notifiable Data Breaches Scheme

Since its commencement in February 2018, the Notifiable Data Breaches scheme has required directors and organisations covered by the Privacy Act to notify affected individuals and the OAIC “as soon as practical” when an “eligible data breach” occurs.

An “eligible data breach” is generally defined by three criteria:

THE THREE CRITERIA

- 1 There is unauthorised access to or disclosure of personal information, or a loss of information where such access/disclosure is likely.
- 2 This is likely to result in serious harm to one or more individuals.
- 3 The organisation has been unable to prevent the likely risk of serious harm with remedial action.

Mandatory Ransomware Reporting

While the Privacy Act focuses on the *protection of data*, the Cyber Security Act 2024 introduces a separate, highly urgent reporting obligations regarding *extortion payments*.

72 hrs

to report a ransomware or extortion payment to the Australian Signals Directorate

\$3m+

annual turnover threshold for “reporting business entities”, alongside critical infrastructure operators

Commencing on 30 May 2025, this law requires “reporting business entities”, generally those with an annual turnover exceeding \$3 million or those managing critical infrastructure, to notify the Australian Signals Directorate (ASD) if they make a ransomware or cyber extortion payment.

The 72-Hour Reporting Window

Unlike the “as soon as practical” timeline of the Privacy Act, the Cyber Security Act is prescriptive. A report must be submitted within 72 hours of:

- 1 Making the ransomware or extortion payment; or
- 2 Becoming aware that a payment has been made on the entity’s behalf.

Governance and Compliance Interaction

In practice, these overlapping obligations, the Privacy Act’s focus on data harm and the Cyber Security Act’s focus on payments, mean a cyber incident can quickly shift from a “technical disruption” to a time-critical director governance issue. Directors are now required to manage two distinct statutory clocks simultaneously: one for notifying affected customers and another for reporting the financial response to the attack. Failing to report a ransomware payment within the 72-hour window can result in civil penalties, reinforcing that accountability for cyber decisions now rests firmly in the boardroom.

4 Scenarios of Personal Exposure

Personal liability often materialises when a cyber incident intersects with other areas of corporate, regulatory, or civil law.



The Insolvency Trigger: Under the Corporations Act, directors have a duty to prevent a company from trading while insolvent. If a ransomware attack halts production for an extended period, the company may become insolvent. If the directors knew their lack of cyber resilience made the company vulnerable to such a “foreseeable” event, they may be held personally liable for debts incurred.



The Insurance “Attestation” Trap: Many cyber insurance policies require directors to sign an “attestation of controls”. This is a legal declaration that specific security measures, such as multi-factor authentication (MFA), are active. If a forensic investigation reveals these controls were not actually in place, the insurer can void the policy for misrepresentation, leaving the director personally responsible for the financial fallout.



Shareholder Derivative Actions: Shareholders or partners can sue directors personally on behalf of the company for the loss in company value following a data leak. The claim is not that the attack happened, but that the *lack of preparation* caused unnecessary financial ruin.



D&O Insurance and Coverage Disputes: Directors often assume that directors and officers (D&O) insurance will respond to cyber-related claims. However, coverage can become contentious where governance failures, misstatements, or poor record-keeping create questions about what was represented, what was known, and what was reasonably managed.

A Governance Roadmap

To protect both the business and personal assets, Australian SME owners must move beyond a “set and forget” mentality. Being “defensible” means being able to prove that leadership took the risk seriously through a documented, proactive approach.

1

Digital Literacy and Active Oversight

Cybersecurity should be a standing item on the agenda of regular leadership meetings. Directors should interrogate their risk posture, understand material exposures, and ensure the current position is recorded.

2

Adopting Recognised Frameworks

Aligning with a framework like the ASD Essential Eight provides a practical and widely recognised benchmark for “reasonable” controls. Implementing strategies such as MFA, regular patching, and restrictive administrative privileges creates a robust defence that courts would be very unlikely to see as negligent.

3

Documentation as a Defence

Maintaining a “paper trail” of cybersecurity measures is essential. This includes documented risk assessments, incident response plans, and records of board-level security discussions. If a director can show they acted on professional advice and consistently prioritised resilience, their legal position is significantly bolstered.

4

Managing Third-Party Risk

Directors must ensure that contracts with IT providers include clear service level agreements regarding security updates and incident reporting. Regular reviews should be conducted to confirm that the expected measures exist in practice and remain effective over time.

Conclusion

The era of treating cybersecurity as an optional IT expense is over. Cyber resilience is now an inseparable component of a director's fiduciary responsibility. While no business will ever be entirely unhackable, every business must be legally defensible.

The evolution of Australian law shows that the community and the government hold leaders accountable for the data they manage. By treating cyber risk as a foreseeable and manageable business priority, leaders do more than just avoid liability; they build "digital trust." Digital trust is a competitive asset that allows the business to thrive in an increasingly volatile online economy. Leadership is no longer defined by the absence of attacks, but by the presence of a robust, documented, and resilient governance strategy.



GET IN TOUCH

**Helping Australian businesses turn cyber risk into
a defensible position.**



02 9071 2345



info@etsau.com



etsau.com

