

AUSTRALIAN DIRECTORS' DUTIES AND THE DEPLOYMENT OF ARTIFICIAL INTELLIGENCE

(Offensive and Defensive Actions)

BY: Dr. Adrian McCullagh Ph.D. LL.B. (Hons)

Contents

I. Introduction	3
II. The General Framework of Directors' Duties	4
A. The statutory duty of care and diligence	4
B. Officers, not only directors	5
C. Good faith, proper purpose, and the remaining Chapter 2D duties	6
D. The business judgment rule and the statutory safe harbours	6
III. Directors' Duties Applied to the Deployment of AI Tools	7
A. ASIC v Bekier: [Star Entertainment Case]	7
B. AI-washing and misleading statements	9
C. ASIC's regulatory guidance on AI governance: Beware the Gap	10
D. Practical content of the duty in the AI-deployment context	10
IV. Does Listing on the ASX Change the Position?	11
A. The Corporations Act duties are the same	11
B. Continuous disclosure	12
C. The ASX Corporate Governance Council's Principles and Recommendations	12
D. Enforcement patterns and reputational exposure	13
V. AI as a Tool of Cybercrime: A Distinct but Related Risk	14
A. The threat landscape	14
B. The duty of care extends to cybersecurity risk	15
C. Applying the duty to AI-enabled attacks	16
VI. Conclusion	17

I. Introduction

Artificial intelligence (“AI”) is no longer a peripheral tool in Australian boardrooms¹. It is being deployed across credit decisioning, fraud and scam detection, customer service, financial advice, cybersecurity monitoring, and increasingly board and management decision-support itself.² This uptake proceeds against a regulatory backdrop in which Australia has, to date, chosen not to enact AI-specific statutory duties for directors, relying instead on the existing, technology-neutral framework of *Chapter 2D of the Corporations Act 2001 (Cth)* (“the Act”).³ The Australian Securities and Investments Commission (“ASIC”) has been explicit that this framework already extends to AI by stating that “the current law applies to the use of AI ... the same legal obligations continue to apply, irrespective of the technology used.”⁴

This article examines how the general law and statutory duties of directors apply to a board’s decision to deploy AI tools within an Australian registered company. The article covers whether, and to what extent, those duties are elevated for a company admitted to the official list of the ASX; and the distinct but related risk that AI is being weaponised by criminals to attack⁵ the very companies whose boards are simultaneously being urged to adopt it⁶. The issue forms a catch 22 in that there are possible conflicting obligations where board are required to act in the best interest of the company that they oversee, which may require them to deploy business enhancing technology such as AI tools and at the same time to manage regulatory obligations such as privacy and data security. The central issue revolves around director’s duties and AI governance policy development⁷.

¹ Australian Institute of Company Directors. “A Director's Guide to AI Governance Version 2”, 29 June 2026, <https://www.aicd.com.au/news-media/research-and-reports/a-directors-guide-to-ai-governance.html>

² Australian Securities and Investments Commission (ASIC), Report 798: “Beware the Gap: Governance Arrangements in the Face of AI Innovation” (October 2024) <https://download.asic.gov.au/media/mtllqjo0/rep-798-published-29-october-2024.pdf>.

³ Corporations Act 2001 (Cth) ch 2D.1; ASIC, *We're Not There Yet: Current Regulation Around AI May Not Be Sufficient* (Speech, 2024) <https://asic.gov.au/about-asic/news-centre/speeches/we-re-not-there-yet-current-regulation-around-ai-may-not-be-sufficient/>.

⁴ Above note 3.

⁵ Church, Z., “AI cyberattacks and three pillars for defense”, MIT Management – Sloan School, 8 September 2025, <https://mitsloan.mit.edu/ideas-made-to-matter/ai-cyberattacks-three-pillars-defense>

⁶ Bombalier, J., “The Competitive Advantage of Using AI in Business” Florida International University. <https://business.fiu.edu/academics/graduate/insights/posts/competitive-advantage-of-using-ai-in-business.html>

⁷ Hadfield, G., “Legal infrastructure for transformative AI governance”, Proceedings of the National Academy of Sciences, 2026 <https://www.pnas.org/doi/pdf/10.1073/pnas.2509742123>

II. The General Framework of Directors' Duties

A. The statutory duty of care and diligence

Section 180(1) of the Act requires a director or other officer of a corporation to “exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise” if they occupied the office and had the responsibilities of that director or officer within that corporation, in the corporation’s circumstances.⁸ The standard is objective and calibrated to the individual’s actual role;⁹ it is not a duty owed personally to shareholders but a public duty enforceable by ASIC by way of civil penalty, reflecting what the Full Federal Court in *Cassimatis v Australian Securities and Investments Commission* described as the “well-recognised public interest” underpinning the section.¹⁰ In the *Cassimatis* case, the Full Court (Greenwood, Rares and Thawley JJ) upheld a finding that the sole directors of Storm Financial Pty Ltd, Mr and Mrs Cassimatis, had contravened s 180(1) by failing to take precautions to prevent the company’s financial model being applied to financially vulnerable investors, notwithstanding that s 180(1) was the only duty ASIC alleged had been breached.¹¹ The primary judgment, delivered by Edelman J in *Australian Securities and Investments Commission v Cassimatis (No 8)*, confirms that liability under s 180(1) turns on whether the director failed to guard against a reasonably foreseeable risk of harm to the company, balanced against the burden of taking alleviating action. This is a classical orthodox negligence-style calculus applied to the corporate context.¹²

Two doctrinal features of s 180(1) matter directly for AI deployment.

First, a company’s own breach of another law is not a necessary element of a director’s breach of duty, but it may be relevant evidence of what a reasonable director in the company’s circumstances ought to have foreseen and guarded against. This is commonly referred to the so-called “stepping stones” analysis.¹³

⁸ *Corporations Act 2001 (Cth) s 180(1)*.

<https://www.legislation.gov.au/C2004A00818/latest/text>

⁹ *Cassimatis v ASIC* [2020] FCAFC 52, [1] (Greenwood, Rares and Thawley JJ)

<https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2020/2020fcafc0052> .

¹⁰ above note 9; see also Ian Ramsay and Miranda Webster, 'An Analysis of the Use of Stepping Stones Liability against Company Directors and Officers' (2021) 50(1) Australian Bar Review 168,

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811196 .

¹¹ *Cassimatis v ASIC* [2020] FCAFC 52 above note 9.

¹² *ASIC v Cassimatis (No 8)* [2016] FCA 1023 (Edelman J), discussed in Lacey, A., 'The Risk of a Director/Officer of a Corporation Assuming Vast Responsibilities' (2016).

<https://www.lexology.com/library/detail.aspx?g=c7c195ab-5b7f-4902-9fba-ccb588204b83> .

¹³ Ramsay and Webster (above note 10) pp. 169-70.

Ramsay and Webster’s analysis of stepping-stones liability observes that ASIC has increasingly relied on a company’s contravention of the Act, or of other statutes, as the evidentiary foundation for establishing that a director failed to meet the s 180(1) standard, and that this technique, while controversial, was substantially endorsed by the Full Court in *Cassimatis*.¹⁴

Where a company deploys an AI system that produces discriminatory credit decisions, misleading advice, or privacy breaches in contravention of the Australian Consumer Law, the Privacy Act 1988 (Cth) or sectoral licensing obligations, that contravention is capable of being used as a stepping stone to establish that the responsible directors failed to exercise reasonable care in permitting or failing to prevent the AI’s deployment.¹⁵

Second, the application of the s 180(1) standard is not static. It has consistently been treated by the courts as evolving with “the changing profile of the duty of care” and with contemporary technology and community expectations, such that what counted as reasonable diligence a decade ago will not necessarily suffice today.¹⁶ The recent decision of the Federal Court in *ASIC v Bekier (Liability Judgment)* [*Star Entertainment case*], discussed further below, is the first Australian judgment to comment directly, albeit obiter, on directors’ use of AI, and confirms that this evolutionary reading of s 180(1) is squarely engaged by the technology.¹⁷

B. Officers, not only directors

The duty of care in s 180(1), together with the duties in ss 181–183, applies to “officers” as defined in s 9 of the Act. The position of a corporate officer is a category that extends beyond the board and includes to any person who participates in decisions affecting the whole or a substantial part of the corporation’s business, or who has the capacity to significantly affect the corporation’s financial standing.¹⁸ The High Court’s decision in *Shafron v ASIC*¹⁹ is authority that a person occupying a dual role, such as a general

¹⁴ *Cassimatis v ASIC* [2020] FCAFC 52 p. 187, above note 9.

¹⁵ Teele Langford, R., “Dystopian Accessorial Liability’ or the End of ‘Stepping Stones’ as We Know It?”, (2020) 37(5) Company and Security Law Journal, pp. 362-369.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3583169, applying the same reasoning to contraventions of laws other than the Corporations Act.

¹⁶ *ASIC v Bekier (Liability Judgment)* [2026] FCA 196, discussed in ‘Board Information Overload, Directors’ Duties and the Responsible Use of AI’ (2026)

<https://anzlaw.thomsonreuters.com/w-049-6305>.

¹⁷ above note 16

¹⁸ Corporations Act 2001 (Cth) s 9 (definition of ‘officer’).

¹⁹ <https://www.hcourt.gov.au/cases-and-judgments/judgments/judgments-1998-current/australian-securities-and-investments-commission-v-hellicar>

counsel and company secretary, is an officer in respect of the entirety of the responsibilities actually performed, not merely those attaching formally to one of the titles held.²⁰ This matters for AI governance because, in practice, oversight of an AI deployment programme is frequently exercised not by the board as a whole but by a chief technology officer, chief risk officer, or general counsel who may fall within the extended statutory definition of “officer” and therefore be personally exposed under s 180(1) in the same way as a director.²¹

C. Good faith, proper purpose, and the remaining Chapter 2D duties

Section 181 requires directors to act in good faith in what they believe to be the best interests of the corporation and for a proper purpose.²² Sections 182 and 183 prohibit the improper use of position or information to gain an advantage or cause detriment.²³ These duties are less directly engaged by the technical deployment of an AI system than s 180(1), but both these sections have become relevant where AI is used, for example, to generate synthetic communications designed to mislead the market²⁴, to entrench management’s position against shareholders, or where confidential information is fed into a third-party large language model in circumstances that expose it to the AI vendor or to competitors conduct capable of breaching ss 182–183.²⁵

D. The business judgment rule and the statutory safe harbours

Section 180(2) provides a business judgment rule: a director or officer who makes a business judgment in good faith, for a proper purpose, without a material personal interest, after informing themselves to the extent they reasonably believe appropriate, and who rationally believes the judgment to be in the best interests of the corporation, is taken to have satisfied the s 180(1) duty.²⁶ Basically, Section 180(2) dealing with the business judgement rule creates a safe harbour protection for corporate officers.

²⁰ *Shafron v Australian Securities and Investments Commission* [2012] HCA 18, <https://www.hcourt.gov.au/cases-and-judgments/judgments/judgments-1998-current/shafron-v-australian-securities-and-investments-commission>

²¹ above note 18.

²² above note 18 Corporations Act 2001 (Cth) s 181.

²³ above note 18 Corporations Act 2001 (Cth), ss 182-3.

²⁴ An example of this is the Canadian case of *Moffat v. Air Canadian* 2024 BCCRT 149, where an AI agent misled an Air Canada customer (Moffat) in relation to an airline booking concerning a bereavement discount. <https://www.canlii.org/en/bc/bccrt/doc/2024/2024bccrt149/2024bccrt149.pdf>

²⁵ above note 2, ASIC REP 798, noting risks of AI models producing outputs difficult to explain and licensees’ data governance obligations

²⁶ above note 18, Corporations Act 2001 (Cth) s 180(2).

Sections 189 and 190 provide further related protections: s 189 allows a director to rely in good faith on information, advice or reports prepared by an employee, professional adviser, expert or fellow director whom the director reasonably believes to be reliable and competent, provided the director makes an independent assessment; whilst s 190 allows a director to delegate a power and rely on the delegate, again subject to a reasonable belief that the delegate would exercise the power in accordance with the director's duties.²⁷

A recent extra-curial analysis of *Bekier* observes that AI-assisted board preparation strains each of these three statutory safe-harbour protections.²⁸ Business judgment under s 180(2) requires the director to have “informed” themselves to the extent they believed appropriate; if an AI-generated summary of board papers omits or misstates a material matter and the director relied on it without independent verification, the “informed” limb is difficult to satisfy.²⁹ Reliance under s 189 is available only in respect of information prepared by specified categories of person (an employee, an adviser, an expert, or a fellow director) and it remains untested and doubtful, whether a generative AI system itself falls within any of those categories, since s 189 was drafted for reliance on persons, not software.³⁰ Delegation under s 190 likewise presupposes a “delegate” capable of bearing the duties of a director, which an AI system, lacking legal personality, is not.³¹ The practical consequence is that a director cannot discharge the s 180(1) duty by pointing to reliance on an AI tool in the way they might point to reliance on a qualified auditor or actuary. Consequently, the duty “remains personal, and it requires informed human judgment.”³²

III. Directors' Duties Applied to the Deployment of AI Tools

A. ASIC v Bekier: [Star Entertainment Case]

On 5 March 2026 Lee J of the Federal Court handed down judgment in *ASIC v Bekier (Liability Judgment)*, arising from ASIC's civil penalty proceedings against eleven former directors and senior officers of The

²⁷ above note 18 Corporations Act 2001 (Cth) ss 189-90.

²⁸ 'AI & Directors' Duties: Do the Safe Harbours Still Protect You?' (2026) <https://betterboards.net/governance/ai-directors-duties-chief-justice-bell/> .

²⁹ above note 28, discussing *ASIC v Bekier (Liability Judgment)* [2026] FCA 196.

³⁰ above note 18; Corporations Act 2001 (Cth) s 189.

³¹ above note 18, Corporations Act 2001 (Cth) s 190; 'se also – “AI in the Boardroom: Why Directors' Safe Harbours May Not Hold”, CJ Bell (NSW Court of Appeal), extra curial comment.

<https://betterboards.net/governance/ai-directors-duties-chief-justice-bell/> .

³² 'AI Disputes: AI in the Boardroom - Practical Tips for Boards and Directors' (2026), quoting Lee J in *ASIC v Bekier (Liability Judgment)* [2026] FCA 196

<https://www.gtlaw.com.au/insights/ai-disputes-ai-in-the-boardroom> .

Star Entertainment Group Ltd (“Star”), an ASX-listed casino operator, over the handling of money-laundering and criminal-infiltration risk in Star’s junket operations.³³ The Court found that Star’s former Chief Executive Officer, Mr Bekier, and its former General Counsel, Chief Legal and Risk Officer and Company Secretary, Ms Martin, had each contravened s 180(1) of the Corporations Act. The Court dismissed the claims against the seven non-executive directors and the chair. The Court accepted that the Board had reasonably relied upon senior management to escalate and inform the board of all the relevant risks.³⁴ Mr Bekier was disqualified from managing corporations for six years and ordered to pay a \$700,000 penalty; whilst, Ms Martin was disqualified for seven years and ordered to pay \$400,000.³⁵

Although the substantive contraventions in Bekier concerned anti-money-laundering governance rather than AI, Lee J used the judgment described by ASIC Chair Joe Longo as “probably the most significant corporate governance case we have taken”.³⁶ Joe Longo’s comment directly impacts the informal use of AI by directors to digest board papers, observing that many individual directors are already using AI “informally to prepare for meetings,” that AI may assist comprehension but “cannot displace judgment,” and that any board use of AI needs to be “controlled and transparent” and governed by formally adopted policies.³⁷ That is, directors cannot remove or diminish their responsibilities imposed by the law by attempting to rely upon some AI tool. AI tools can be used to assist directors, but their use does not alter the director’s primary fiduciary obligation of acting in the best interest of a company with due diligence and competency.

Consequently, all Corporate boards should ensure that they have developed an AI usage policy that meets the corporation’s requirements and the policy must address the business being operated by the corporation. That is, the deployed AI policy must be fit for purpose and complied with, which means that it must be

³³ ASIC, '26-040MR Federal Court Finds Two Star Entertainment Senior Executives Breached Duties, Non-Executive Directors Did Not Breach Duties' (Media Release, 2026) <https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-040mr-federal-court-finds-two-star-entertainment-senior-executives-breached-duties-non-executive-directors-did-not-breach-duties/> .

³⁴ above note 16.

³⁵ ASIC, '26-123MR Former Star Entertainment Executives Mathias Bekier and Paula Martin Disqualified and Ordered to Pay Penalties' (Media Release, 2026) <https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-123mr-former-star-entertainment-executives-mathias-bekier-and-paula-martin-disqualified-and-ordered-to-pay-penalties/> .

³⁶ When Management Fails the Board: Lessons from ASIC v Bekier' (2026) <https://www.ashurst.com/en/insights/when-management-fails-the-board-lessons-from-asic-v-bekier/> .

³⁷ AI & Directors' Duties' (n 22) <https://betterboards.net/governance/ai-directors-duties-chief-justice-bell/> .

monitored and enforced. An AI policy is not simply a “tick and flick exercise” but must be regularly reviewed and updated to make sure it is fit for purpose.

His Honour reiterated the orthodox content of the s 180(1) standard: a director is required to take reasonable steps to place themselves in a position to guide and monitor management, to take a diligent and intelligent interest in the information available, to understand that information, and to apply an enquiring mind. The imposed obligations that, in his Honour’s assessment, AI can support but AI will not perform or replace a director’s obligations.³⁸ Commentary on the decision by the Australian Institute of Company Directors likewise emphasises that boards “must control the information they receive” and that AI use “must be controlled and formally governed by the board” and must not displace independent judgement.³⁹

The Bekier case also confirms, applying the Cassimatis reasoning, that a company’s actual contravention of the law is relevant to, but not an essential ingredient of, a director’s breach of s 180(1). This reinforces that a poorly governed AI deployment need not itself breach a separate statute, but it can be used as a stepping-stones-style liability for the directors who permit it.⁴⁰

B. AI-washing and misleading statements

A second, distinct exposure arises where a company or its directors make public statements about the capability, safety or governance of the corporations deployed AI. It has become an increasing issue that corporations make rash statements which are, or become, misleading. Conduct of that kind may contravene the misleading and deceptive conduct provisions of the *Australian Consumer Law in Schedule 2 to the Competition and Consumer Act 2010 (Cth)*, independently of any duty under the Corporations Act; but where directors cause or permit such statements to be made, the same stepping-stones logic that operated in Cassimatis and was applied in Bekier is capable of converting the contravention into a breach of s 180(1) or s 181 by the responsible directors.⁴¹ ASIC’s own market conduct guidance for 2024 flagged this practice.

³⁸ Star Entertainment Decision - Key Takeaways for Directors and Officers' (2026)

<https://addisons.com/article/star-entertainment-decision-key-takeaways-for-directors-and-officers/> .

³⁹ 'Star Entertainment Group Judgment: Implications for Directors' (Australian Institute of Company Directors, 2026)

<https://www.aicd.com.au/board-of-directors/duties/liabilities-of-directors/star-entertainment-group-judgment.html> .

⁴⁰ 'When Management Fails the Board' (n 30), citing Cassimatis v ASIC [2020] FCAFC 52

<https://www.ashurst.com/en/insights/when-management-fails-the-board-lessons-from-asic-v-bekier/> .

⁴¹ Competition and Consumer Act 2010 (Cth) sch 2 (Australian Consumer Law); 'Navigating AI: Minimising Misleading and Deceptive Exposure for Australian Directors' (2026)

<https://www.minterellison.com/articles/navigating-ai-misleading-and-deceptive-exposure-for-australian-directors> .

This is sometimes labelled “AI-washing” by analogy with greenwashing. This is becoming an emerging area of enforcement focus, alongside cybersecurity governance.⁴²

C. ASIC’s regulatory guidance on AI governance: Beware the Gap

In October 2024 ASIC published *Report 798 Beware the gap: Governance arrangements in the face of AI innovation*, the first output of a market-wide review of AI use across twenty-three Australian financial services and credit licensees.⁴³ ASIC found that licensees were adopting generative AI and other AI tools more rapidly than they were updating the risk and governance frameworks needed to manage it. According to ASIC this was creating a real risk that created lag in proper AI Governance adoption.⁴⁴ The report catalogued 624 AI use cases as at December 2023 that directly or indirectly affected consumers, and identified risks including “black box” models whose outputs could not be explained to the individuals affected by them, algorithmic bias, and inadequate testing and monitoring regimes.⁴⁵ Critically, ASIC framed the regulatory response not as a call for new AI-specific laws, but as a reminder that the existing, technology-neutral regulatory framework, which includes the general obligation to provide services “efficiently, honestly and fairly,” and, by clear implication, the directors’ duties in Chapter 2D already applies in full to AI-driven conduct and decision-making.⁴⁶ REP 798 is, in substance, a template for what a court applying the Cassimatis stepping-stones analysis to an AI-caused harm is likely to treat as the benchmark of reasonable AI governance: documented risk classification, human oversight of high-impact use cases, testing before and monitoring after deployment, and board-level visibility of material AI risks.⁴⁷

D. Practical content of the duty in the AI-deployment context

Synthesising Bekier, Cassimatis, Shafron, and REP 798, the s 180(1) duty in the context of AI deployment requires directors to satisfy themselves, on a continuous and documented basis, that:

⁴² above note 35.

⁴³ above note 2, ASIC REP 798, p. 2

⁴⁴ ASIC, '24-238MR ASIC Warns Governance Gap Could Emerge in First Report on AI Adoption by Licensees' (Media Release, 2024)

<https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-238mr-asic-warns-governance-gap-could-emerge-in-first-report-on-ai-adoption-by-licensees/> .

⁴⁵ above note 2, ASIC REP 798 pp.4-6

⁴⁶ above note 2,; ASIC, 'We're Not There Yet'

<https://asic.gov.au/about-asic/news-centre/speeches/we-re-not-there-yet-current-regulation-around-ai-may-not-be-sufficient/> .

⁴⁷ above note 2, ASIC REP 798

- (a) the company has classified its AI use cases by the degree of risk they pose to consumers, the company, or third parties;
- (b) material or high-risk use cases are subject to human oversight commensurate with that risk⁴⁸;
- (c) the board receives, and understands, reporting on AI performance, incidents and near-misses sufficient to allow it to exercise an “enquiring mind”;
- (d) any board or management reliance on AI-generated summaries or analysis is disclosed and independently tested rather than accepted uncritically; and
- (e) public statements about the company’s AI capability or safety are accurate and kept current.⁴⁹

A director who can point to none of these, and who instead treats AI adoption as a matter left entirely to management or to the technology itself is substantially exposing himself/herself to an unnecessary regulatory risk. As such a director is in a materially weaker position to defend an action. Further, the lack of due diligence on the part of a director could impede a director in relying on s 180(2) business judgment rule or the s 189 reliance defence. Whereas a director who can demonstrate active, informed oversight of the kind Lee J described in *Bekier* is in a stronger position to fall within the safe harbour protection afforded by section 180(2), section 189 or section 190.⁵⁰

IV. Does Listing on the ASX Change the Position?

A. The Corporations Act duties are the same

Section 180(1) does not impose a different, or heightened standard of care merely because the corporation is listed on the ASX. What changes for a listed entity is the surrounding lattice of continuous disclosure,

⁴⁸ In a different context the issue of Automated Decision-Making technology as it the Robodebt case must be considered. The Hayne Royal commission clearly concluded that ADM technology must involve some human oversight.

<https://robodebt.royalcommission.gov.au/>

The same principal will, it is suggested, apply to AI deployed technology. That is, directors cannot simply rely upon the output of an AI tool but must undertake reasonable actions to investigate whether the output is correct. There must exist some human oversight dealing with any AI deployment.

⁴⁹ Above note 2, Synthesis of ASIC REP 798 (n 1) and *ASIC v Bekier (Liability Judgment)* [2026] FCA 196 as discussed in 'Board Information Overload' above note

<https://anzlaw.thomsonreuters.com/w-049-6305> .

⁵⁰ 'AI & Directors' Duties' (n 22)

<https://betterboards.net/governance/ai-directors-duties-chief-justice-bell/> .

governance-reporting and market-integrity obligations that interact with, and in practice elevate the practical stringency of, the s 180(1) standard.

B. Continuous disclosure

ASX Listing Rule 3.1 requires a listed entity, once it becomes aware of information that a reasonable person would expect to have a material impact on the price or value of its securities, to immediately notify ASX of that information, subject to limited carve-outs in Listing Rule 3.1A.⁵¹ The High Court's decisions in *ASIC v Hellicar*⁵² and the companion decision in *Shafron v. ASIC*,⁵³ arose directly out of a failure of the corporation concerning the release to the ASX of a misleading announcement in relation to the adequacy of funding for an asbestos compensation trust. The Court held that the board directors and the company secretary/general counsel had breached their respective duty of care because the disclosure was structured in a misleading manner and as such the disclosure should not have been made in that form.⁵⁴

Applied to AI, an ASX-listed company that experiences a material AI-driven incident, for example, a large-scale algorithmic mispricing, a consumer-harm event of the kind ASIC's REP 798 anticipates, or a cyber-incident of the kind discussed in Part V below that compromises AI systems handling market-sensitive data is exposed to a continuous disclosure obligation that has no equivalent for an unlisted proprietary company, and directors who cause or permit non-disclosure, or a misleading disclosure, of such an incident face the same Hellicar/Shafroon-style exposure under s 180(1) as they would for any other misleading market announcement.⁵⁵

C. The ASX Corporate Governance Council's Principles and Recommendations

Listing Rule 4.10.3 requires a listed entity to state in its annual report the extent to which it has followed the recommendations of the ASX Corporate Governance Council during the relevant reporting period, and if not, why not, on an "if not, why not" basis.⁵⁶ The fourth edition of the Corporate Governance Principles

⁵¹ ASX Limited, ASX Listing Rules r 3.1, 3.1A

<https://www.asx.com.au/about/regulation/rules-and-guidance-notes.htm> .

⁵² <https://www.hcourt.gov.au/cases-and-judgments/judgments/judgments-1998-current/australian-securities-and-investments-commission-v-hellicar>

⁵³ <https://www.hcourt.gov.au/cases-and-judgments/judgments/judgments-1998-current/shafron-v-australian-securities-and-investments-commission>

⁵⁴ *Shafron v Australian Securities and Investments Commission* [2012] HCA 18, Above note 20 .

⁵⁵ Above note 46, applied by analogy to a market-sensitive AI-related incident.

⁵⁶ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations (4th ed, February 2019) r 4.10.3

and Recommendations, in force for financial years commencing on or after 1 January 2020, requires listed boards, among other things, to establish policies for the oversight and management of material business risk (Recommendation 7.2) and to disclose whether the entity has any material exposure to environmental or social risks and, if so, how it manages those risks (Recommendation 7.4).⁵⁷ Although the fourth edition predates the current wave of generative AI adoption and does not mention AI by name, its risk-oversight recommendations are technology-neutral in the same way as s 180(1) itself, and a listed board's decision not to bring a material AI risk within its Recommendation 7.2/7.4 risk-oversight and disclosure framework is a further evidentiary marker. A court could treat such a failure as falling short of the standard expected of a reasonable director of a listed entity.⁵⁸ The ASX Corporate Governance Council's Advisory Group is, presently, consulting on a fifth edition of the Principles, indicating that the ASX itself regards the governance framework for emerging risks, including AI, as due for updating.⁵⁹

D. Enforcement patterns and reputational exposure

As a matter of practice rather than strict legal doctrine, ASIC's public enforcement priorities and the practical consequences of a governance failure differ materially for listed entities. Bekier itself demonstrates this as Star's status as one of Australia's two ASX-listed casino operators, and the scale of public and regulatory attention that followed, was treated by Lee J as relevant to the gravity of the contravention. His Honour observed that "public companies conducting enterprises pregnant with risks more broadly" must understand that governance failures may attract substantial personal consequences.⁶⁰ Listed entities are also subject to continuous market and analyst scrutiny, mandatory periodic reporting, and under Recommendation 5 of the fourth edition Principles an obligation to make timely and balanced disclosure of all matters concerning the entity that a reasonable person would expect to have a material

<https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf> .

⁵⁷ Above note 48 Recommendations 7.2, 7.4.

⁵⁸ Above note 2, ASIC REP 798

⁵⁹ ASX Limited, 'Corporate Governance Principles and Recommendations' (Draft 5th edition consultation) <https://www.asx.com.au/about/regulation/corporate-governance-principles-and-recommendations> .

⁶⁰ ASIC, '26-123MR' (n 29)

<https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-123mr-former-star-entertainment-executives-mathias-bekier-and-paula-martin-disqualified-and-ordered-to-pay-penalties/> .

effect on the price or value of its securities, reinforcing rather than displacing the Listing Rule 3.1 obligation discussed above.⁶¹

The cumulative effect is that, while the content of the s 180(1) duty of care does not formally differ between a listed and an unlisted company, an ASX-listed company's directors face a materially denser set of overlapping statutory and quasi-regulatory obligations with continuous disclosure, "if not, why not" governance reporting, and heightened regulatory and market visibility. All of which interact with s 180(1) to make an inadequately governed AI deployment more likely to be detected, more likely to be the subject of a market-sensitive disclosure obligation, and more likely to attract stepping-stones-style scrutiny of the directors' oversight than the equivalent deployment within an unlisted company.

V. AI as a Tool of Cybercrime: A Distinct but Related Risk

A. The threat landscape

The same generative AI capability that boards are being encouraged to deploy is being used by criminals to attack Australian companies. This development is now formally recognised by Australia's peak cybersecurity agency. The Australian Signals Directorate's Australian Cyber Security Centre ("ASD's ACSC"), in its Annual Cyber Threat Report 2024–25, notes that Australian entities lodged 84,700 cybercrime reports in the 2024–25 financial year. This amounts to one reportable incident every six minutes. Further the ASD's ACSC responded to over 1,200 cybersecurity incidents, which is an 11 per cent increase on the previous year. The average self-reported financial cost of cybercrime to large business increased by 219 per cent over the same period.⁶²

The report devoted a dedicated section to generative AI, concluding that while GenAI "has the potential to generate significant benefit for the Australian economy and society, it also creates an avenue for cybercriminals to streamline and scale their activities," including by automating the analysis of large stolen datasets to identify high-value targets, and by generating "high-quality videos, fake voices, websites, know-your-customer records and spearphishing emails" to impersonate legitimate actors and defeat identity-verification controls.⁶³ Independent commentary on the same report notes a 280 per cent increase in denial-

⁶¹ ASX Corporate Governance Council (n 48) Principle 5 <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf>.

⁶² Australian Signals Directorate, Annual Cyber Threat Report 2024-25 (October 2025) <https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf>

⁶³ Above note 62 (GenAI discussion).

of-service incidents and confirms that AI-generated phishing and deepfake-enabled scams are allowing attackers to operate “at greater speed, scale, and believability.”⁶⁴

B. The duty of care extends to cybersecurity risk

Directors’ duties in respect of cybersecurity risk generally, as distinct from AI-enabled cybercrime specifically, are now well established in Australian law. The landmark decision in *ASIC v RI Advice Group Pty Ltd* held that RI Advice, an Australian Financial Services Licensee, had contravened ss 912A(1)(a) and (h) of the Act by failing to have documentation, controls and risk management systems adequate to manage cybersecurity risk across its network of authorised representatives, following nine cybersecurity incidents. The relevant incidents included third party hacking, ransomware and phishing attacks between June 2014 and May 2020.⁶⁵ Rofe J accepted that, given the pervasive reliance of financial services businesses on digital and computer technology, “cybersecurity risk forms a significant risk connected with the conduct of the business,” such that adequate risk management systems must extend to that risk. The Court ordered RI Advice to engage a cybersecurity expert to identify further necessary measures and to pay \$750,000 towards ASIC’s costs.⁶⁶ While RI Advice concerned a corporate AFSL obligation rather than a personal director’s duty, commentary on the decision is consistent with the stepping-stones analysis discussed above. The relevant commentary treats such risk as establishing the foreseeability limb of the Shirt calculus⁶⁷ for corporate cybersecurity risk generally, from which a director’s own s 180(1) obligation to take reasonable

⁶⁴Australia's 2024-25 Cyber Threat Report: Key Insights for Small and Medium Businesses' (2025)

<https://www.managedservices.com.au/australia-cyber-threat-report-2024-25/> .

⁶⁵Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496; Australian Securities and Investments Commission, '22-104MR Court Finds RI Advice Failed to Adequately Manage Cybersecurity Risks' (Media Release, 2022)

<https://download.asic.gov.au/media/zhodijpp/22-104mr-2022-fca-496.pdf> .

⁶⁶ ASIC v RI Advice Group Pty Ltd [2022] FCA 496 [58]; 'Federal Court Finds Cyber Risk Management Is a Critical Obligation for Financial Services Licensees' (2022)

<https://www.allens.com.au/insights-news/insights/2022/05/Federal-Court-finds-cyber-risk-management-is-a-critical-obligation/> .

⁶⁷ While it seems acceptable to say that a person should not be liable for failure to take precautions against unforeseeable risks, it may not be reasonable to expect a person to take precautions against a risk of very low probability simply because it was foreseeable. In order to overcome this problem, the High Court in *Wyong Shire Council v Shirt* (1980) 146 CLR 40 held, in effect, that a person cannot be held liable for failure to take precautions against a risk that could be described as ‘far-fetched or fanciful’, even if it was foreseeable. This is known as the “Shirt” principal. What this amounts to is that there are some risks that are of such low probability that the reasonable person would ignore them, regardless of the balance of the other considerations in the negligence calculus. That is, no matter how serious the harm was likely to be if the risk materialised, no matter how cheap or easy it would have been to take precautions that would have prevented the risk materialising, and no matter how socially worthless the risk-creating activity was, if the likelihood of the risk materialising is so low that a reasonable person would ignore the risk then it is permissible to ignore such risk.

steps to guard against that foreseeable risk follows.⁶⁸ Academic commentary from UNSW Business School on cybersecurity governance similarly concludes that “directors each have a personal duty to take reasonable care to ensure the risks are being properly managed,” that disengagement or complacency is not an option once a risk of attack is clearly foreseeable, and that directors must, at minimum, maintain a working understanding of the Essential Eight cyber risk mitigation strategies published by the Australian Signals Directorate.⁶⁹

C. Applying the duty to AI-enabled attacks

The ASD’s ACSC findings mean that AI-enabled social engineering, deepfake business-email-compromise fraud, and AI-accelerated exploitation of stolen data are no longer speculative or remote risks but a documented, government-reported feature of the current threat environment, squarely within the class of “reasonably foreseeable risk of harm” that s 180(1), as construed in *Cassimatis*, requires a director to weigh against the burden of taking alleviating action.⁷⁰

Two consequences follow.

- First, the same AI systems a company deploys for legitimate business purposes are themselves an attack surface: a poorly secured internal large language model, retrieval system, or AI agent with access to company data or payment systems is a new category of cybersecurity risk that a reasonable board is now on notice to consider as part of its existing cybersecurity risk-management obligations under the RI Advice line of authority.⁷¹
- Second, the deepfake and AI-generated impersonation risk identified in the ASD’s Annual Cyber Threat Report 2024–25 raises the practical content of “adequate” controls that a board must have in place. For example, verification protocols for payment instructions or board-level authorisations that no longer treat a familiar voice or video as sufficient authentication, in the same way that the

⁶⁸Cybersecurity Obligations Arising out of *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496 (2022) <https://www.kwm.com/au/en/insights/latest-thinking/cybersecurity-obligations-arising-out-of-asic-v-ri-advice-group.html> .

⁶⁹Pamela Hanrahan, 'Cybersecurity Governance: Are Directors Doing Enough?' UNSW Business Think (2024) <https://www.businessthink.unsw.edu.au/articles/cybersecurity-governance-cyber-risk-management-board-directors-duties> .

⁷⁰ above note 62, Australian Signals Directorate
ASIC v Cassimatis (No 8) [2016] FCA 1023.

⁷¹ Above note 2, ASIC REP 798

incidents catalogued in RI Advice raised the practical content of “adequate” cybersecurity controls for financial advice networks.⁷²

For a listed company, an AI-enabled cyber incident affecting market-sensitive information carries the additional continuous disclosure exposure discussed in Part IV(B) above.⁷³

VI. Conclusion

Australian law does not yet contain, and the Australian Federal Government has not indicated an intention to enact, any AI-specific directors’ duties.⁷⁴ Instead, the existing technology-neutral duties in Chapter 2D of the Act which principally concern the duty of care and diligence in s 180(1), read together with the business judgment rule in s 180(2) and the reliance and delegation protections in ss 189–190 will apply in full to a board’s decisions to deploy, oversee and rely upon AI. Cassimatis and Shafron establish the doctrinal foundations;

- ASIC’s Beware the Gap report supplies the practical benchmark of adequate AI governance; and
- Bekier is the first Australian judicial statement confirming that AI use by directors themselves is squarely within the scope of the s 180(1) enquiry, and that the statutory safe harbours in ss 180(2) and 189–190 are strained, and may fail, where a director has relied on AI output without independent, informed judgment.⁷⁵

Listing on the ASX does not alter the context of these duties, but it materially increases their practical stringency by overlaying continuous disclosure obligations under Listing Rule 3.1, “if not, why not” governance reporting against the ASX Corporate Governance Council’s risk-oversight recommendations, and heightened regulatory and market visibility of the kind that shaped the outcome in Bekier itself.⁷⁶

Even though, there does not presently exist a specific AI law dealing with a director’s duty in the deployment of AI there does exist certain arguable issues that will develop in this regard. AI deployment

⁷² Above note 62, Australian Signals Directorate
See also ASIC v RI Advice Group Pty Ltd [2022] FCA 496.

⁷³ ASX Listing Rules (n 45) r 3.1
<https://www.asx.com.au/about/regulation/rules-and-guidance-notes.htm> .

⁷⁴ ASIC, ‘We’re Not There Yet’ (n 2)
<https://asic.gov.au/about-asic/news-centre/speeches/we-re-not-there-yet-current-regulation-around-ai-may-not-be-sufficient/> .

⁷⁵ *Cassimatis v ASIC* [2020] FCAFC 52; *Shafron v ASIC* [2012] HCA 18; ASIC REP 798 above note 2; *ASIC v Bekier (Liability Judgment)* [2026] FCA 196.

⁷⁶ ASX Listing Rules (n 45) r 3.1; ASX Corporate Governance Council (n 48).

will in some circumstances require a board of directors in acting in the best interest of the company to ensure that their company operates competitively in the marketplace which may result in a necessity to deploy AI as a business tool. Any AI deployment should also include the development any promulgation of an AI policy framework. Failure to do so could be used as evidence of directors failing to meet their duty of care. There have been in Australia and globally sufficient publications dealing with the risks of AI both as an offensive tool to advance competitiveness and as a defensive tool against third parties hacker attacks. It is recommended that most boards should develop an AI policy document and such policy should be reviewed at least annually.

Finally, the same technology boards are being urged to adopt is, on the Australian Signals Directorate's own current assessment, being used at scale by criminals to attack Australian companies through AI-generated phishing, deepfake impersonation and accelerated exploitation of stolen data. This is certainly a risk that falls within the same foreseeability-based duty of care that the Federal Court applied to conventional cybersecurity failures in *RI Advice*, and one that a reasonable director can no longer treat as remote or speculative.⁷⁷ The practical message for Australian boards, listed and unlisted alike, is that AI governance is not a discrete compliance project that can be delegated wholesale to management or to the technology itself; it is an application of directors' existing, personal, non-delegable duty of care.

⁷⁷Australian Signals Directorate (above note 62); *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496.