Cyber Partners

BOARD ADVISORY & TRAINING

Independent Cyber, Technology & AI Governance for Boards

Governing cyber, technology and AI risk is a director's duty. Most boards have no independent expert in the room to discharge it.

Since the Australian Federal Court's 2022 decision in ASIC v RI Advice Group, cyber risk sits squarely inside a director's duty of care under section 180 of the Corporations Act. The AICD and Cyber Security Cooperative Research Centre's Cyber Security Governance Principles, now in their second version, have become the benchmark against which that duty is assessed. Very few boards have a director, or an independent advisor, able to discharge that oversight with genuine authority. We close that gap.

> *The Federal Court found that reliance on digital systems means cybersecurity risk forms a significant risk connected with the conduct of a business, placing it firmly within the board's duty of oversight.*
>
> **ASIC V RI ADVICE GROUP PTY LTD [2022] FCA 496**

Independent cyber, technology and AI governance and training for boards

Through Cyber Partners, experienced Board Director and Cybersecurity and AI risk specialist Tony Barnes works directly with boards and individual directors, not as a technical vendor, but as a boardroom peer who has sat on both sides of the table. He delivers both training to help Directors close their own gaps, as well as direct advisory services to ensure Directors' Duties are fulfilled in relation to the oversight of cyber and technology risk. Every engagement is delivered personally, face to face or remotely, and translated into the language a board needs to discharge its duty with confidence.

RETAINED BOARD ADVISOR — CYBER, TECHNOLOGY & AI GOVERNANCE

Ongoing, independent advice to the board or risk committee across cyber, technology and AI governance. Priority access between meetings, briefing papers ahead of board cycles, and a standing point of independent expertise the board can call on.

BOARD & DIRECTOR TRAINING — CYBER, TECHNOLOGY & AI RISK

One-off or programmed sessions, in person or remote, that build director fluency in cyber, technology and AI risk. Built for the board table rather than the server room: what to ask, what a credible answer sounds like, and where the red flags sit.

CYBER CRISIS SIMULATION FOR BOARDS

Board-level crisis simulations, including ransomware scenarios, that test the decisions directors actually have to make: whether to pay, when to notify, and what to tell the market, not only whether a technical playbook was followed.

CYBER & AI MATURITY ADVISORY — NIST CSF, ESSENTIAL EIGHT, ISO27001, ISM

Independent review of maturity against the NIST Cybersecurity Framework, the ASD Essential Eight and related standards, translated out of technical language and into a position the board can state with confidence, to itself, to regulators and to the market.

INDEPENDENT GOVERNANCE ASSURANCE

External expert assurance where the board has a gap in its own cyber, technology or AI governance capability: a named, independent practitioner the board can point to as evidence it has taken its oversight duty seriously.

Board Director Cyber, Technology & AI Governance

Selected engagements

Four engagements illustrative of work delivered directly to boards, executives and government stakeholders. Further detail available on request.

QUEENSLAND GOVERNMENT COMMISSION → NATIONAL ROLLOUT

CyberFi — Statewide Cyber Training Platform

Commissioned by the Queensland Government to design and build a comprehensive cyber security training programme for businesses across the state. Personally developed the full training content and the technology platform used to deliver it, combining face-to-face and online delivery. The programme's success led to its expansion into a national offering for businesses across Australia.

Government-commissioned | Later expanded nationally

TEC / VISTAGE CEO PEER NETWORKS

Cyber Crisis Simulations for CEOs and Senior Executives

Designed and personally facilitated more than twenty cyber crisis simulations for TEC and Vistage, Australia's peer advisory networks for chief executives and senior leaders, reaching several hundred participants nationally. Each simulation placed executives in the decision seat of a live ransomware or major incident scenario, rather than as an audience for a technical briefing. Many of these sessions were followed with a further deep dive session into practical cyber risk mitigation, business continuity and technology risk management guidance.

20+ simulations delivered | Several hundred CEOs and senior executives nationally

RETAINED OR APPOINTED BASIS

Independent Audit & Risk Committee Contributor

Engaged as an independent expert contributor to Audit and Risk Committees, providing assessment of technology control gaps, cyber programmes, digital transformation initiatives, and third-party vendor and major programme oversight. Appointed on a retained basis to augment existing committee and director expertise wherever independent technical assurance is required.

Retained or appointed | ARC and major programme oversight

12–36 MONTH APPOINTED MANDATES

Independent Technology, Cyber & AI Risk and Governance Specialist Advisor

Appointed as an independent specialist board advisor on technology, cyber and AI risk and governance, providing quarterly risk updates to the board, written, in person or both. Reviews progress against IT, AI and cyber programmes, tests risk documentation and register currency, and gives the board assurance that complex technical programmes are on track, or, where they are drifting, the evidence and recommendations needed to bring them back under control. Mandates typically run twelve to thirty-six months, or align to a specific transformation project such as year one of a multi-year cyber uplift, with oversight extending to the detail underneath the reports the board receives.

12–36 month mandates | Quarterly board reporting

ENGAGEMENT & PRACTITIONER

Board Director Cyber, Technology & AI Governance

Engagement models

Four ways to engage, individually or in combination, structured around the board's cycle rather than a project timeline.

STANDING ENGAGEMENT

Retained Advisor

Ongoing appointment to the board or risk committee. Quarterly briefings as a minimum, direct access between meetings, and input ahead of major technology or AI decisions.

Annual retainer

ONE-OFF OR PROGRAMMED

Board & Director Training

A single director briefing, or a structured programme delivered across the year. In person or remote, sized to a single board or a portfolio of boards.

Per session or programme

HALF-DAY, BOARD-ONLY

Crisis Simulation

A ransomware or major incident simulation built around your organisation, run at the board table with the directors themselves in the decision seat, not a technical team.

Fixed fee, per simulation

POINT IN TIME

Independent Assurance Review

A one-off review of cyber, technology or AI governance maturity, benchmarked against the frameworks below and delivered as a board-ready report.

Fixed fee, per review

AICD CYBER SECURITY GOVERNANCE PRINCIPLES V2 · ASD ESSENTIAL EIGHT · NIST CSF · CORPORATIONS ACT S180

Why an independent boardroom practitioner

Most cyber advice that reaches a board today arrives in one of two forms: a technical vendor or managed security provider running a scripted programme built for an IT audience, or guidance filtered upward through the same management the board is meant to be overseeing. Neither is independent, and neither is built for the boardroom. What boards are increasingly seeking, and what the market has been slow to supply, is a practitioner who can sit at the table as a peer: someone who understands the technology and the threat, has actually held governance accountability as a director, and can translate both into a position the board can act on and defend. That is the gap this service fills.

Tony Barnes

LLM (Ent. Gov) | MBA | MBLaw | MIS (Cyber) | CISSP | FGIA | MAICD

Tony Barnes has more than three and a half decades of business experience, including 25 years as a senior executive and non-executive director in critical infrastructure, technology and cybersecurity, and holds four postgraduate degrees spanning enterprise governance, business law, business administration and information systems security. He has trained more than 1,000 Board Directors over the past decade, designed and delivered cyber training at state and national scale, and has facilitated dozens of executive crisis simulations nationally. He engages personally on every mandate: no junior team, no handoff.

BOARD EXPERIENCE

Non-executive director, critical infrastructure and not-for-profit boards; independent Audit & Risk Committee contributor

EXPERIENCED CYBER OPERATOR

More than a delivering cyber strategy, cyber maturity uplift and cyber protective services to enterprises across board business sectors and government.

DELIVERY

Face to face and remote, individual boards and multi-board portfolios

INDEPENDENCE

No vendor relationships, no product to sell, no remediation pipeline

Arrange a confidential conversation

For retained advisory, board training or an independent assurance review, contact Tony Barnes directly.

Tony Barnes
Managing Partner, Cyber Partners
tony@cyberpartners.com.au