VYFORITY · BOARD GOVERNANCE & LIABILITY

S.180

The Director's Cyber Governance Question Card

Five questions that expose the gap between *"Implemented"* and *"Effective"* — and protect your personal liability against autonomous threats.

WHY ASK THESE: GRC frameworks cannot measure autonomous risk. Your board pack measures human effort (e.g., "MFA deployed"), not adversarial outcomes. The following questions are designed so that honest answers from management will immediately reveal whether you are receiving genuine security oversight or compliance theatre.

01 "With AI models autonomously discovering zero-days, do we have the telemetry to detect an AI-driven breach today?"

The Exposure: Anthropic's new AI model autonomously uncovered a 27-year-old flaw in OpenBSD. AI models execute exploits in seconds. If your team manually applies patches monthly, you are vulnerable.

02 "If our AP workflow is targeted by AI-generated deepfake invoices today, what specific, non-technical gates guarantee we won't pay?"

The Exposure: CBA recently intercepted $1B in suspected synthetic document fraud. Mid-market finance teams often lack systemic, human-verified protocols to catch AI fraud that easily bypasses digital security.

03 "Has our broker confirmed that 'Attribution Gaps' won't leave us with unpriced risk that voids our cyber insurance?"

The Exposure: The $20B cyber insurance market is actively penalising for AI-attribution gaps, non-uniform MFA, and silent EDR. Relying on an insurance policy carrying unpriced risk leaves directors personally exposed.

04 "Are the cyber risk metrics presented in this board pack measuring pure activity, or actual financial and operational outcomes?"

The Exposure: GRC frameworks reward "control deployed", not "control validated under adversarial conditions." This creates watermelon reporting — green on the outside, red underneath.

05 "If a major incident occurred tonight, does our response documentation legally satisfy the 72-hour mandatory reporting requirement?"

The Exposure: Under the Cyber Security Act 2024, failure to report within 72 hours carries severe penalties. Building a board-approved compliance process from scratch under crisis conditions is impossible.

IF THE ANSWERS CONCERN YOU

A 2-hour **Shadow Board Pack Review** exposes where the gaps between reported and actual posture reside in your specific environment. Fixed fee, direct with Dean.

vyfority.com.au/ned

DEAN KASTELIC

Former Enterprise CISO. KPMG Director, Cyber Advisory. Advises boards and NEDs on defensible cybersecurity governance across ASX-listed, private, and NFP sectors.

dean@vyfority.com.au