# The Director's Cyber Governance *Question Card*

s.180

Five questions that expose the gap between "implemented" and "effective", and protect your personal liability in the age of autonomous threats.

**WHY ASK THESE** Your board pack measures human effort ("MFA deployed"), not adversarial outcomes. These questions are built so that honest answers from management immediately reveal whether you are receiving genuine security oversight or compliance theatre.

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

**THE EXPOSURE** Frontier AI models are already finding decades-old flaws in mature, widely-audited codebases, and can weaponise them far faster than a monthly patch cycle. If detection assumes human-speed attackers, it is calibrated to the wrong adversary.

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** Australia's banks are now intercepting synthetic-document fraud at a scale measured in the billions. Mid-market finance teams rarely hold the systemic, human-verified protocols that catch AI fraud after it sails past digital controls.

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

**THE EXPOSURE** Insurers are actively penalising AI-attribution gaps, non-uniform MFA and silent endpoint coverage. A policy carrying unpriced risk is not a transfer of risk; it leaves the directors personally holding it.

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

**THE EXPOSURE** GRC frameworks reward "control deployed", not "control validated under adversarial conditions". The result is watermelon reporting: **green** on the outside, **red** underneath.

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

**THE EXPOSURE** Under the Cyber Security Act 2024, failure to report a ransomware payment within 72 hours carries civil penalties. Building a board-approved compliance process from scratch, under crisis conditions, is not a plan.

**IF THE ANSWERS CONCERN YOU**

A two-hour **Shadow Board Pack Review** exposes where the gaps between reported and actual posture sit in your environment. Fixed fee, direct with Dean.
**vyfority.com.au/ned**

**DEAN KASTELIC**

Former enterprise CISO. Ex-KPMG Director, Cyber Advisory. Advises boards and NEDs on defensible cyber governance across listed, private and NFP sectors.
**dean.kastelic@vyfority.com.au**