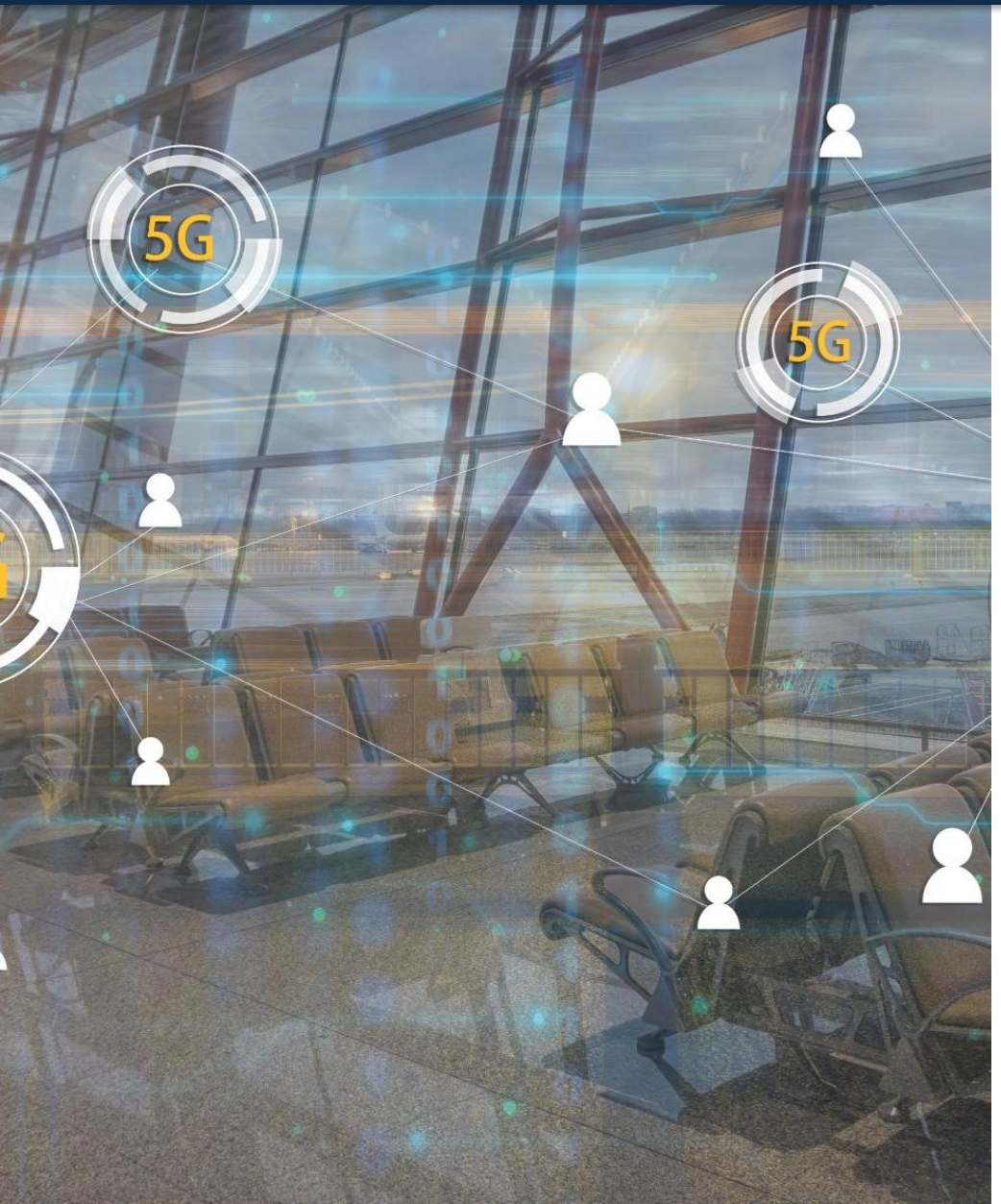
BeforeTheBreach.au



Challenging Assumptions

Effective oversight tools help leaders identify blind spots and test assumptions in cyber risk management, improving security posture.

Clear Communication

Jargon-free communication empowers informed questions and decisions, even without deep technical expertise, enhancing governance.

Stronger Governance

A deeper cyber risk understanding supports robust decision-making and strengthens overall governance at the board level.

5 Cybersecurity Questions Every Director Must Ask

BeforeTheBreach.au

❓ **What is our current exposure to third-party cyber risk — and how are we independently verifying it?**

❓ **Are we seeing today's threats — or last year's trends?**

❓ **Does our board receive direct briefings from the CISO — or filtered updates through the CIO or risk team?**

❓ **How are we tracking our response time to cyber incidents — and does that include board-level escalation speed?**

❓ **Have we mapped our most sensitive data assets — and reviewed whether they're appropriately classified and protected?**

Question 1

What is our current exposure to third-party cyber risk?

Why it matters: Supply chain attacks are now common. Boards must know whether vendor risk is audited or assumed.

What to listen for:
- A clear inventory of third-party vendors and platforms
- Independent security assessments, not just self-attestations
- Identification of high-risk vendors and how they're monitored
- Use of contracts, insurance clauses, or scorecards to enforce standards

Question 2

Are we seeing today's threats – or yesterday's trends?

Why it matters: Many cyber dashboards focus on historical incidents. Boards need visibility of current threat vectors, such as AI-enhanced phishing or CI/CD pipeline compromise.

What to listen for:
- Threat intelligence is current, contextual, and curated — not just generic monthly reports.
- Emerging risks such as AI-driven social engineering, supply chain breaches, or zero-day exploits.
- Use of external threat feeds, peer benchmarking, or official alerts (e.g. ACSC, ASD).
- The ability to pivot quickly based on evolving threats — not a fixed, 12-month risk plan.

Question 3

Does our board receive direct briefings from the CISO or filtered updates through the CIO or risk team?

Why it matters: Too many boards operate through proxy relationships. Effective oversight requires direct engagement and unfiltered dialogue.

What to listen for:
- Confirmation that the CISO has direct access to the board or audit/risk committee.
- Signs of a trusted, two-way relationship — not just compliance updates or project reports.
- Evidence the board is hearing about risks, weaknesses, and trade-offs, not just success stories.
- Indicators that the CISO can speak plainly, without relying on technical jargon or filtered summaries.

Question 4

How are we tracking our response time to cyber incidents?
(Does that include board-level escalation speed?)

Why it matters: Supply chain attacks are now common. Boards must know whether vendor risk is audited or assumed.

What to listen for:
- A clear inventory of third-party vendors and platforms
- Independent security assessments, not just self-attestations
- Identification of high-risk vendors and how they're monitored
- Use of contracts, insurance clauses, or scorecards to enforce standards

Question 5

Have we mapped our most sensitive data assets and reviewed whether they're appropriately classified and protected?

Why it matters: Misclassification often leads to overexposure. Boards must challenge assumptions — not just sign off on policies.

What to listen for:
- Existence of a data classification framework, and a recent effort to map critical assets.
- Specific examples of crown jewels — such as customer data, intellectual property, financial systems, or operational controls.
- Clarity on access controls and monitoring, including internal staff and external providers.
- Confirmation that classification is reviewed and tested regularly, not defined once and filed away.

Bonus: ChatGPT Prompts to support your preparation

- What are the **top 3 emerging cyber threats** for boards this quarter?
- Summarise this technical incident report in board-level language. *(you would provide the report)*
- How would a regulator critique our current cyber governance disclosures?
- Create a checklist of board-level red flags in cybersecurity reporting.
- What are 5 key questions a director should ask after a cyber breach?