Questions Every Board Should Ask About Cyber and AI Risk

September 10, 2026

01 What Could Hurt Us Most?

What AI or cyber risk could seriously disrupt our revenue, customers, operations or reputation?

02 What Don't We Know?

Where are our hidden dependencies, third parties, AI systems and supply-chain risks we cannot currently see?

03 Who Is Responsible?

If AI or a cyber incident causes harm, who owns the decision, the risk and the response?

04 Are We Investing in the Right Things?

Are we spending on controls that actually reduce our biggest risks, or simply buying more tools?

05 Can We Recover?

If something we depend on fails tomorrow, how quickly can we continue operating and protect our customers?

What Could Hurt Us Most?

Three impact areas where AI and cyber risk could cause serious disruption

Revenue & Operations

What AI or cyber risk could seriously disrupt our core business processes and income streams?

- Ransomware halting critical operations
- AI system failure causing financial or service loss

Customers & Data

Which risks could expose customer data, erode trust, or trigger regulatory and legal consequences?

- Breach exposing sensitive customer or employee data
- AI bias leading to harm or regulatory penalties

Reputation & Strategy

How could an AI failure or cyber incident damage our brand, leadership credibility and long-term strategy?

- Public incident destroying stakeholder confidence
- AI misuse undermining board-level credibility

What Don't We Know?

Where are the hidden dependencies and risks we cannot currently see?

Unmapped Vendors

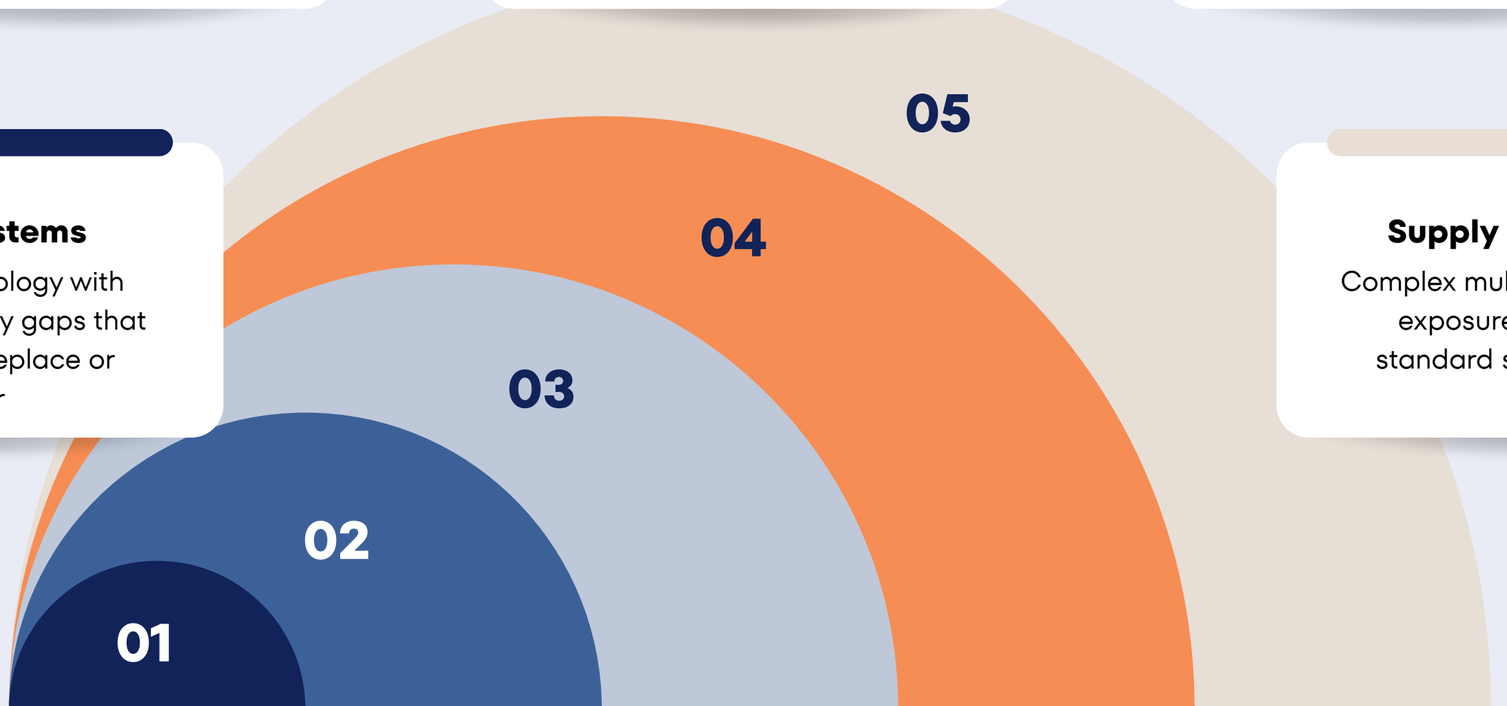
Third-party suppliers and partners with unknown access to critical systems and data

AI Vulnerabilities

AI model risks including bias, data poisoning, and unpredictable failure modes

Hidden Dependencies

Undocumented internal and external system dependencies creating invisible single points of failure

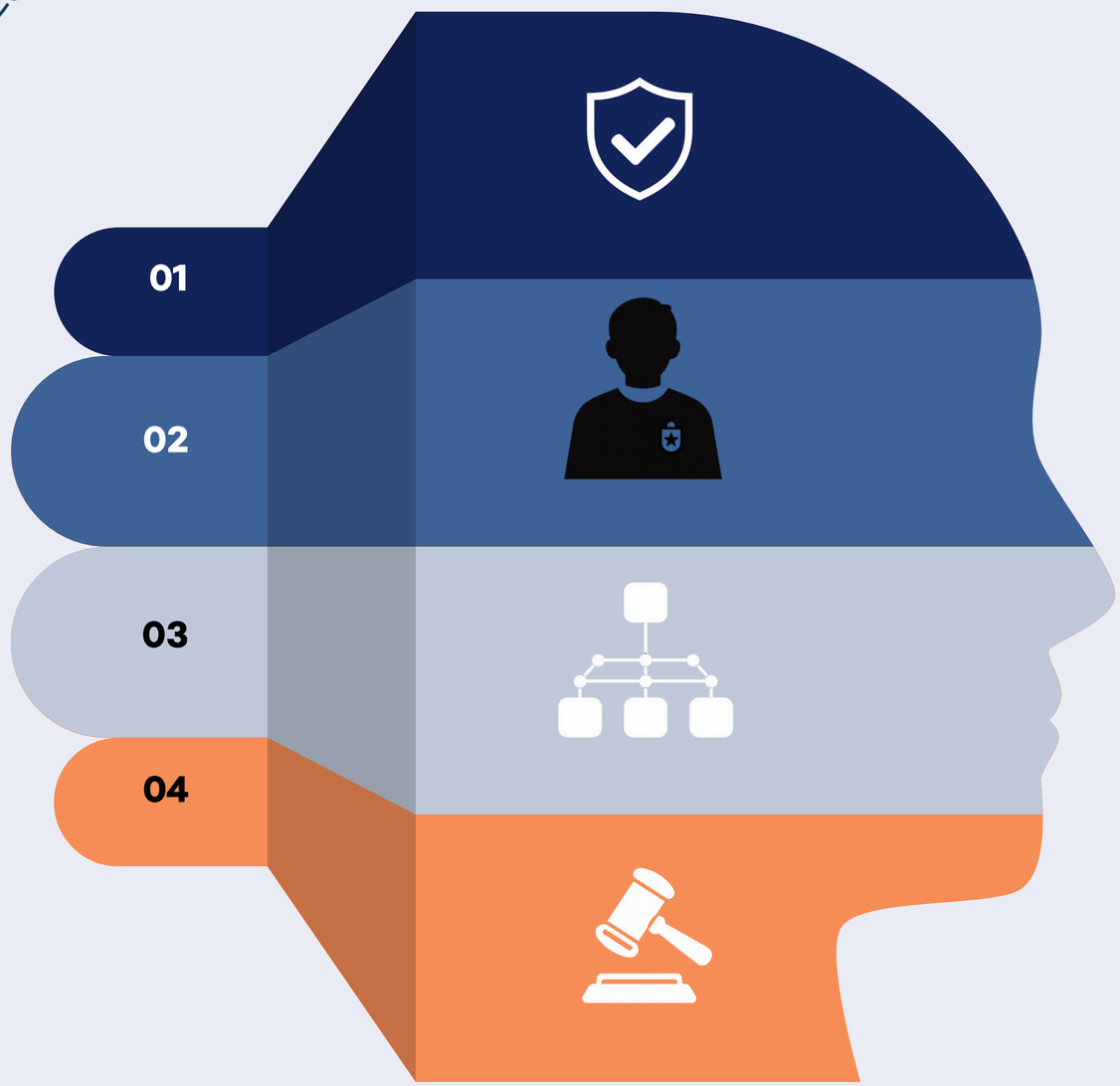


Legacy Systems

Outdated technology with unpatched security gaps that are difficult to replace or monitor

Supply Chain Risks

Complex multi-tier supply chain exposures that bypass standard security controls



Who Is Responsible?

If AI or a cyber incident causes harm, who owns the decision, the risk and the response?

Define Risk Ownership

Assign clear accountability at board and executive level for AI and cyber risk decisions

Establish Response Roles

Define incident response responsibilities across teams before a crisis occurs

AI Governance Framework

Implement accountability structures that govern AI deployment, monitoring and risk escalation

Board-Level Oversight

Ensure the board retains decision authority and visibility over critical cyber and AI risk outcomes

Are We Investing in the Right Things?

Are we spending on controls that reduce our biggest risks, or simply buying more tools?

Right Investment

01 Invest in controls mapped directly to your highest-priority cyber and AI risks

02 Align spending with board-approved risk appetite and overall strategy

03 Measure effectiveness of every control investment against risk reduction outcomes

04 Consolidate vendors and platforms to reduce complexity and attack surface

05 Continuously review investment portfolio as the threat landscape evolves

Wrong Investment

01 Purchasing tools without clear alignment to identified risk priorities

02 Accumulating redundant or overlapping solutions that add cost not protection

03 Chasing compliance checkboxes rather than addressing real business exposures

04 Proliferating point solutions that create integration gaps and hidden vulnerabilities

05 Locking budgets into legacy tools that no longer address current AI and cyber threats

Can We Recover?

Three pillars of resilience and continuity

Business Continuity

Ensure critical operations continue even when core systems or services fail unexpectedly

- Map all critical business processes and dependencies
- Test continuity plans regularly with realistic scenarios

Incident Recovery

Minimise downtime by executing rapid, tested recovery processes across all systems

- Define recovery time objectives for every key system
- Rehearse incident response with cross-functional teams

Customer Protection

Safeguard customer data, trust and experience throughout any disruption or recovery event

- Protect customer data with isolation and backup protocols
- Communicate clearly with customers during any incident

The Board-Level Formula

Five steps from risk visibility to sustainable growth

01

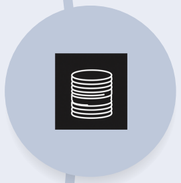
See the Risk

Identify and map all cyber and AI risks across the organisation, including hidden dependencies and third-party exposures

02

Prioritise

Focus board attention on the risks that could cause the greatest harm to revenue, customers, operations and reputation



03

Invest

Direct spending toward controls and capabilities that genuinely reduce the highest-priority risks, not simply more tools

04

Resilience

Build the capacity to absorb disruption, recover rapidly and protect customers when incidents inevitably occur

05

Trust & Growth

Demonstrate responsible governance of cyber and AI risk to earn lasting stakeholder confidence and enable sustainable growth

Invisible Exposure

Risks we have not mapped cannot be managed. Unseen dependencies silently grow into critical vulnerabilities.

Blind Spot Culture

Organisations that assume safety are most at risk. Complacency in AI and cyber governance invites catastrophic failure.

What Risk Are We Accepting Today?

Simply because we cannot see it a call to action for deeper board engagement

Board Accountability

The board must demand clarity on what is unknown. Accepting risk by default is still a decision own it deliberately.

Act Before Crisis

Ask the hard questions now. Resilience, trust and growth depend on seeing what others choose to ignore today.