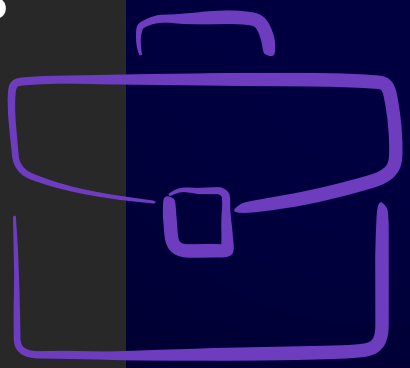
Cyber

CyberGuide

Top 10 Cybersecurity tips for the Board in the AI era.

A KYOCERA **Cyber**Guide for CEOs, CFOs & Board leaders.



Here are the 10 essentials every Board must own in today's AI accelerated threat landscape.

01. Spend vs. Risk: Demand clarity, not complexity

Cyber budgets should always map to the risks they are designed to reduce.

- Ask: "What risk does this investment actually remove or reduce?"
- Challenge spend that cannot be linked to measurable risk reduction.
- Expect simple explanations, not technical jargon.

Good governance starts with informed challenge.

02. Make risk visible: Establish clear KPIs & dashboards

Cyber risk must be monitored like financial risk.

- Require a Board level dashboard with simple indicators: exposure, vulnerabilities, incident response speed, supply chain risk, user behaviour.
- Ensure trends (not just numbers) are reviewed regularly.

If you can't see the risk, you can't manage it.

Cybersecurity is no longer an IT issue - it's a strategic, financial and reputational risk that starts with the Board.

03. Lead from the front: Culture is a leadership issue

Your people are your attack surface, and your defence.

- Make cyber training completion a leadership led expectation, not an IT task.
- Support IT by ensuring teams respond to warnings, updates and security requests promptly.

Tone from the top directly shapes cyber resilience.

04. Avoid tool sprawl: More tools ≠ more security

Many organisations are drowning in tools but starving for capability.

- Challenge any request that adds tools without clear ownership or measurable outcomes.
- Avoid complex 'package' services with unclear reporting or accountability.

The best tools in the world are useless if nobody is managing them.

KYOCERA

kyoceracyber.com

Top 10

Cybersecurity tips for the Board in the AI era.

Cyber

05. Be prepared: Tabletop exercises are essential

A breach is not the time to discover your plan doesn't work.

- Insist on annual tabletop exercises using real-world scenarios.
- Ensure the exact people who will be involved during a crisis are the ones who rehearse it.
- Align learnings with business continuity and recovery plans.

Practice prevents panic.

06. It's not the CISO's problem. It's the Board's

Cyber is a strategic business risk, not a technical one.

- Reject the mindset: "I don't understand, but IT does."
- Allocate dedicated Board time to cyber awareness, planning and oversight.
- Own cyber as a leadership team, not a single role.

Shared ownership equals stronger defence.

07. Don't ignore supply chain risk

Your organisation is only as strong as the least secure company you rely on.

- Demand governance, visibility and assurance from your suppliers.
- Require evidence of technical controls, not just promises or policies.
- Treat third party security as a critical Board level risk.
- Most breaches today come through someone else's vulnerabilities.

Most breaches today come through someone else's vulnerabilities.

Get in touch

steve.doust@duk.kyocera.com

linkedin.com/in/steve-doust-95474816/

kyoceracyber.com

KYOCERA

08. Assume you will never have enough resources

Cyber skills are scarce. Attackers are not.

Ensure your IT/security team or provider is using AI and automation to keep pace.
Evaluate partners on their ability to scale, automate and respond rapidly.

The only sustainable defence is augmented, not manual.

09. Integration matters: Security must fit the business

Poorly integrated security slows people down, so people find workarounds.

- Make cyber part of natural business processes, not an obstacle.
- Ensure security is integrated into procurement, onboarding, workflows and approvals.

If security frustrates people, security fails.

10. Trust nothing at face value: AI is rewriting deception

With AI, attackers can now impersonate voices, videos and emails with ease.

- Encourage a culture of 'pause and verify'.
- Instantly question unexpected requests, even from familiar voices.
- Have clear fail-safes for when someone inevitably gets fooled.

Double-checking is now a survival skill.

Summary

Cyber resilience is a board led discipline. The organisations that thrive in the AI era will be those whose Boards:

- Ask the right questions
- Demand clarity
- Lead a security first culture
- Prepare for crisis before one arrives
- Recognise cyber as a strategic business risk