Cyber

Top 10 Technical Cybersecurity tips for the IT Leaders in the AI era.

A KYOCERA **Cyber**Guide for CISOs,
IT Directors & Digital Transformation Leaders

These are the technical must-dos every senior IT leader should prioritise.

01. Identity is the New Perimeter. Treat it like one.

Compromise almost always begins with identity.

- Implement strong identity governance, continuous authentication, MFA enforcement and role hygiene.
- Deploy User & Entity Behaviour Analytics (UEBA) to spot anomalies early.
- Audit privileged accounts relentlessly. No 'temporary exceptions' without an expiry.

Identity maturity consistently correlates with breach resistance.

02. Secure the Cloud Control Plane (and don't forget SaaS)

Most cloud breaches are caused by misconfiguration, change drift or insufficient monitoring.

- Treat the control plane as a crown jewel asset.
- Enable continuous configuration scanning across clouds and SaaS platforms.
- Monitor for cross domain attacks: identity pivoting, lateral movement and privilege escalation.

If you don't secure the control plane, you haven't secured the cloud.

The threat landscape is changing faster than ever, accelerated by AI, multicloud, SaaS sprawl and increasingly aggressive adversaries.

03. Prepare for AI Accelerated Attacks

Attackers are using AI to operate faster, more convincingly and with lower skill barriers.

- Shorten your Mean Time To Detect (MTTD) with high-fidelity telemetry, enriched analytics and automated detection workflows.
- Secure your own AI usage: ensure prompt controls, model protections, data governance and DLP are aligned to AI enabled processes.
- Validate where AI tools integrate with sensitive business functions.

AI raises the speed of attack. Detection speed must rise with it.

04. Governance still beats tools. Every time.

Weak governance neutralises even the best technology stacks.

- Embed strong change control, access review cycles and configuration management.
- Standardise security patterns across teams to avoid 'creative config'.
- Validate that processes are being followed, not just documented.

Good governance prevents more breaches than the flashiest tool ever will.

KYOCERA

kyoceracyber.com

Top 10

Cybersecurity tips for the Board in the AI era.

Cyber AI

05. Treat Vulnerability Management as a daily habit, not a monthly task

You can't secure an environment that isn't patched.

- Operate a continuous vulnerability and remediation programme. No lag, no exceptions.
- Prioritise based on exploitability, internet exposure, and business criticality.
- Review your software controls: who installs what, how, and why?

Your environment shouldn't be the only house on the street with the windows open.

06. Hygiene: The boring stuff that actually stops attacks

When attackers choose targets, they choose the easiest ones.

- Enforce network segmentation and strict access control.
- Use JIT access for administrative rights.
- Patch aggressively, especially zero-days (now up 42% YoY).
- Harden endpoints, servers and developer environments with standardised baselines.

90% of breaches exploit poor hygiene, not sophisticated techniques.

07. Modern monitoring: Hunt, detect, respond. Proactively.

Your SOC must assume compromise.

- Conduct continuous threat hunting, not just alert triage.
- Build a realistic baseline of 'normal' behaviour.
- Close blind spots: if the logs don't exist, you can't defend that surface.
- Prioritise endpoint, identity, network and cloud telemetry as essentials.

Visibility gaps are attacker opportunities.

08. Zero-Day Preparedness & Threat Intelligence

Zero-days are increasing, and exploitation is faster than ever.

- Build capability for rapid triage and patching of high risk exposures.
- Prioritise internet facing systems and critical workloads.
- Operationalise threat intelligence: make it actionable, not academic.

Your response speed to emerging threats defines your survivability.

09. Configuration, Misconfiguration & Legacy Systems

Misconfiguration remains one of the top breach vectors.

- Continuously audit configurations, especially as vendors push new features.
- Validate guardrails in IaC, CI/CD and deployment pipelines.
- Isolate or retire legacy systems, they drag your risk profile upward daily.

Misconfigurations are the breach that you built yourself.

10. Education isn't optional, even for Technical Teams

People assume technical teams 'already know', but evidence contradicts this.

- Enforce mandatory training, simulation and continual refreshers.
- Gamify secure behaviour adoption and make it competitive.
- Where users repeatedly fail, intervene early and decisively.

Security culture must be engineered, not assumed.

Summary

Modern defence is about speed, visibility & discipline. For technical leaders, resilience is less about tools and more about:

- Reducing exposure
- Hardening identity
- Eliminating misconfiguration
- Automating detection
- Governing consistently
- Responding faster than attackers can pivot

Get in touch

steve.doust@duk.kyocera.com

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

kyoceracyber.com

KYOCERA