Cyber security in 2026:
Priorities for C-suite action

The cyber security landscape is entering a new era where technology, regulation and leadership will determine resilience and growth.

"The future of cyber security is not about choosing between security and innovation; it is about achieving both simultaneously."

Jan Matto
Partner and Group Head of Cyber Security
Forvis Mazars

01

Regulatory evolution

Regulation is accelerating and diverging globally, with DORA, NIS2 and CMMC already reshaping requirements. Compliance alone is no longer enough — businesses must adopt a risk-based approach that prioritises critical assets, integrates third-party risk management and turns compliance into competitive advantage. Cyber maturity is now a deciding factor in tenders, partnerships and trust.

C-suite action: Commission a risk-based compliance review and ensure cyber requirements are built into supplier and partner contracts.

02

Artificial intelligence

AI is both weapon and defence. It powers advanced detection, automation and code security, but also enables attackers to scale and personalise threats. The bigger risk is "Shadow AI" — uncontrolled employee use of AI tools. Leaders must set governance frameworks, embed oversight for agentic AI and balance innovation with security.

C-suite action: Put in place an AI governance framework and require all teams to report how they are using AI.

forvis mazars

Cyber security in 2026:
Priorities for C-suite action

03

Quantum computing

Quantum risks may feel distant, but adversaries are already stealing encrypted data to decrypt later. Waiting is no longer an option. Firms should start quantum preparation today: build a cryptographic inventory, prioritise critical data, assess supply chain readiness and plan for migration to quantum-safe encryption.

C-suite action: Ask security leaders to complete a cryptographic inventory this year and prepare a roadmap for quantum-safe migration.

04

Resilience in 2026 and beyond

Resilience will define the winners. Security by design, adaptive governance and ecosystem-wide risk management are becoming non-negotiable. Companies must embed security into every initiative, train their workforce beyond specific tools, and measure resilience in business terms — not just technical metrics.

C-suite action: Require every new initiative to demonstrate security by design and track resilience against business outcomes.

44%

of executives say they are only **partially prepared** for EU cyber legislation such as NIS2 and DORA.

1 in 5

report spending more than **20%** of their IT budget on cybersecurity.

2/3

of leaders believe their organisation's data is "completely" protected - yet most cite improving **data quality systems** as a top priority.

Jan Matto
Partner and Group Head of Cyber Security
Forvis Mazars
jan.matto@forvismazars.com

forvis mazars