TheCyberGuild

Executive Questions on AI & Post-Quantum Cyber Risk

Board / C-Suite Discussion Guide

Use these questions to drive structured conversation at the board and executive level, covering strategy, risk, governance, technology, people, and investment priorities across AI and post-quantum cryptography.

STRATEGY, RISK, AND GOVERNANCE

Q1

Are AI and post-quantum (PQC) risks explicitly on our risk register and board agenda?

- How often are they discussed at board and executive level (quarterly, annually, ad hoc)?

Q2

Do we treat AI and PQC as one integrated risk domain, or as disconnected technical projects?

- How are they tied into our enterprise risk management and business continuity plans?

Q3

Who is accountable for AI governance and for post-quantum transition?

- Do we have named executive owners and a cross-functional governance body?

CURRENT EXPOSURE AND PREPAREDNESS

Q4

Do we have an inventory of where cryptography is used across our organization and supply chain?

- What percentage coverage do we believe we have (even if approximate)?
- How often is that inventory updated?

Q5

What is our current exposure to "harvest now, decrypt later" risk?

- Which classes of data (e.g., health, financial, IP, operational technology) must remain secure for 5-10+ years?

Q6

How are we measuring and monitoring AI-driven threats today?

- Identity attacks, social engineering, data exfiltration speed, model misuse, shadow AI, etc.

VENDORS, ECOSYSTEM, AND SUPPLY CHAIN

Q7

What are we asking of our key vendors regarding AI and post-quantum readiness?

- Are we consistently asking: "What is your post-quantum roadmap and AI-risk roadmap?"
- Is that reflected in RFPs, contracts, and ongoing vendor reviews?

Q8

Do our critical partners (cloud, identity, payments, OT/ICS, health, etc.) have credible PQC and AI security plans?

- How are we validating those claims (attestations, certifications, technical evidence)?

CONTROLS, ARCHITECTURE, AND ZERO TRUST

Q9

Where are we on our zero-trust journey, specifically for identity and data?

- Do we have phishing-resistant authentication in place for high-risk users and systems?
- Are session tokens bound to users/devices/networks to prevent replay?

Q10

How will our architecture handle PQC migration without breaking the business?

- Have we identified high-risk / high-value systems that must be upgraded first?
- Do we understand dependencies between servers, clients, protocols, and certificates?

PEOPLE, EDUCATION, AND CULTURE

Q11

How are we demystifying AI and quantum for non-technical leaders and staff?

- Are we framing this as data care and business resilience, not just "cybersecurity"?

Q12

What is our plan to build and retain talent in AI- and PQC-aware cybersecurity?

- Are we protecting training and upskilling budgets, even in cost-cutting cycles?
- How are we engaging with external communities, nonprofits, and universities?

PRIORITIZATION AND INVESTMENT

Q13

If we had to invest $1 of new spend today, how would we allocate it between AI risk and PQC readiness and why?

- What is our short-term vs long-term risk tradeoff?

Q14

What does "good enough for now" look like in the next 12-24 months?

- What concrete milestones (inventories, pilots, vendor commitments, control rollouts) will we hold ourselves accountable to?