Capgemini RESEARCH INSTITUTE

Future encrypted

Why post-quantum cryptography tops the new cybersecurity agenda

Why is quantum safety a priority

Harvest-now, decrypt-later attacks

- These attacks rely on the acquisition of currently encrypted data with the possibility of decrypting it after 'Q-Day'*
- 65% of organizations are concerned about "harvest-now, decrypt-later" attacks

Global regulatory mandates

- NIST (US): Standardized PQC algorithms (Kyber, Dilithium, SPHINCS+); urges immediate integration
- NSA: RSA <2048-bit & ECC to be deprecated by 2030; disallowed completely by 2035
- EU: Recommends starting the PQC transition by end of 2026; critical infrastructures to transition as soon as possible and no later than by the end of 2030.

The ecosystem is already adapting

- AWS: Kyber-based key exchange
- Cloudflare: Hybrid PQC-TLS handshakes
- Apple: PQ3 for iMessage
- Microsoft: PQC in Windows Insider builds
- OpenSSL 3.5: PQC algorithm support

Time is running out

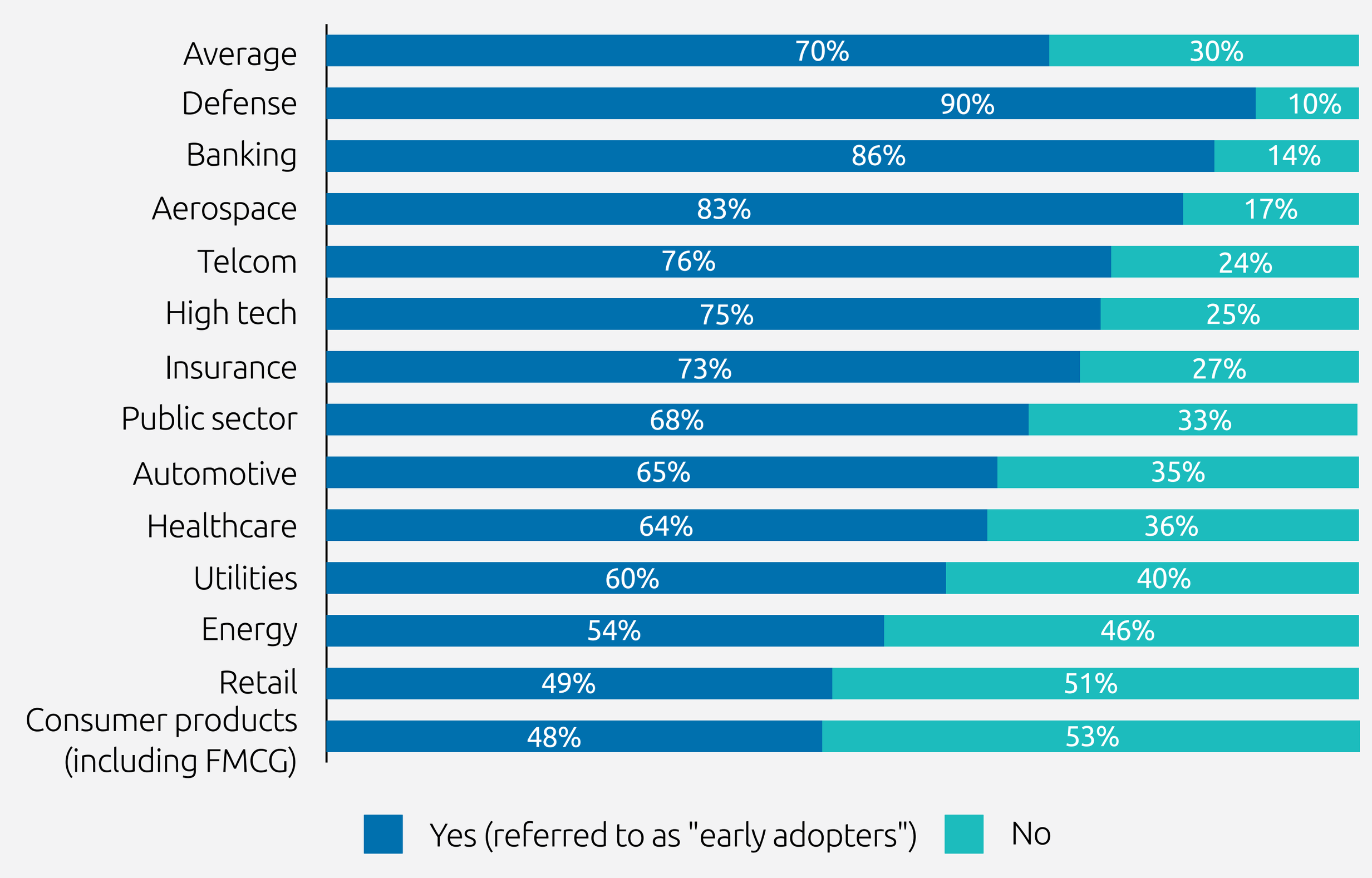
- CISOs underestimate the scale of transformation. Migration involves recompiling apps, replacing crypto libraries, rotating keys and updating HSMs, reissuing certificates
- Everyone soon will be scrambling for the same scarce quantum-safe talent

Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 1,000 organizations; online sources. *Q-Day is the hypothetical future date when quantum computers will become powerful enough to break the cryptographic algorithms that currently secure most of the world's digital data and communications.

Quantum safety is on the radar of most organizations

Seven in 10 organizations say they are currently working on or planning to use quantum-safe solutions in the next five years

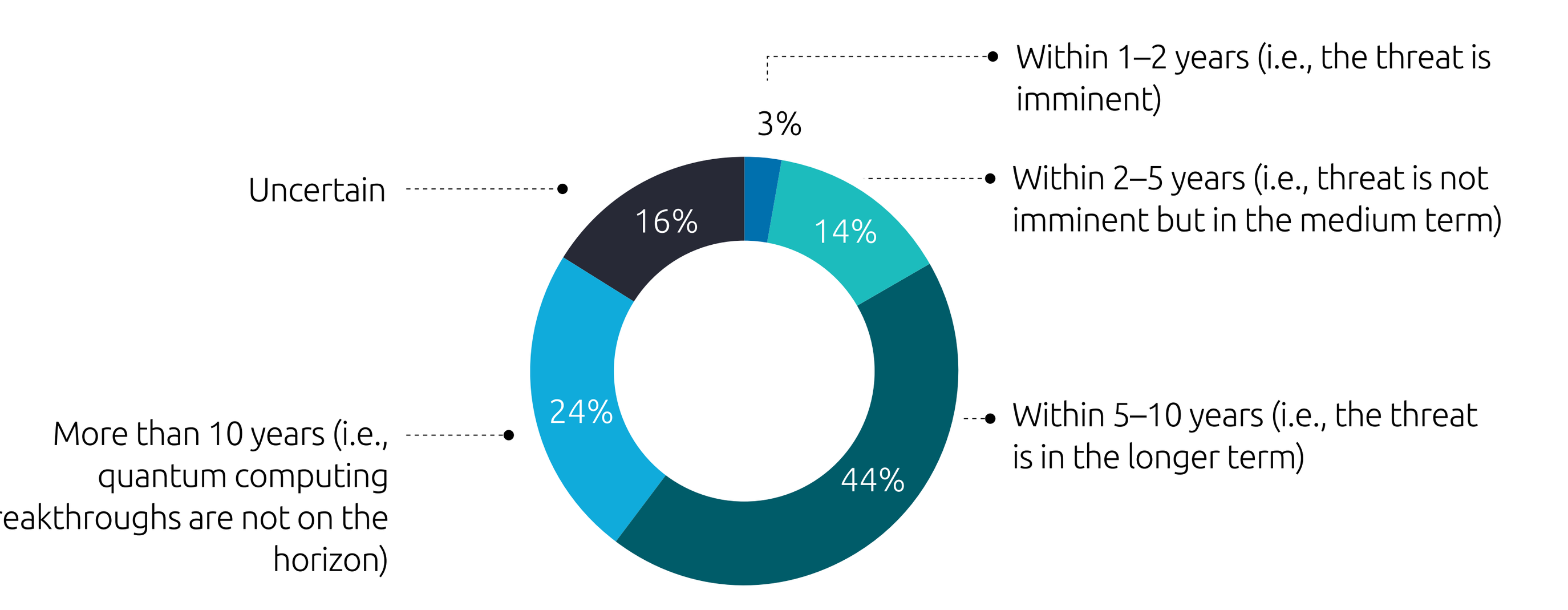
Are you currently working on or planning to use quantum-safe solutions in the next five years?



Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 1,000 organizations.

Around six in ten early adopters believe that the Q-day could occur within the next decade

In your organization's view, how soon will quantum computers achieve the capability to break current encryption methods?



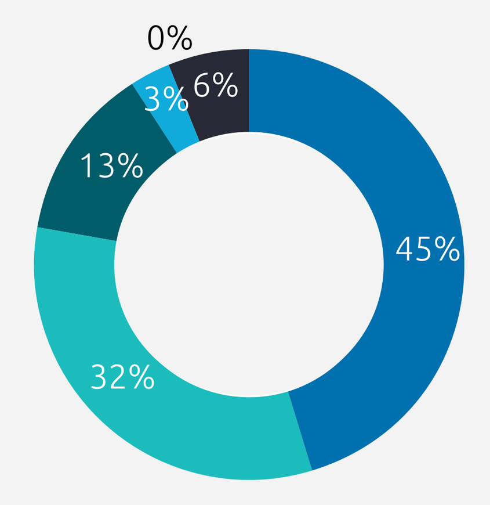
Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 703 early adopters. Q-Day is the hypothetical future date when quantum computers will become powerful enough to break the cryptographic algorithms that currently secure most of the world's digital data and communications

70% of early adopters view the transition to PQC as essential to maintaining their competitive edge and long-term data security

Organizations are exploring a potential transition to PQC

Nearly half of early adopters are exploring PQC concepts

Which stage is your organization at in terms of PQC adoption?



- We are exploring PQC concepts, running pilot studies, discussing with our partners, or conducting feasibility research.
- We have identified the preferred PQC algorithms (e.g., from NIST) and are aligning our internal standards accordingly.
- We are actively integrating PQC algorithms into selected systems and conducting performance, security, and compatibility tests.
- We are augmenting legacy encryption methods with PQC across multiple parts of our infrastructure.
- PQC is fully deployed and operational across all relevant operations.
- Not started/no plans currently.

Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 703 early adopters.

Few organizations are ready for the transition to PQC

Elements needed for transition to PQC

Organizational foundations

- Strategy and readiness
- Team preparedness
- Threat assessment
- Preparedness of supply partners

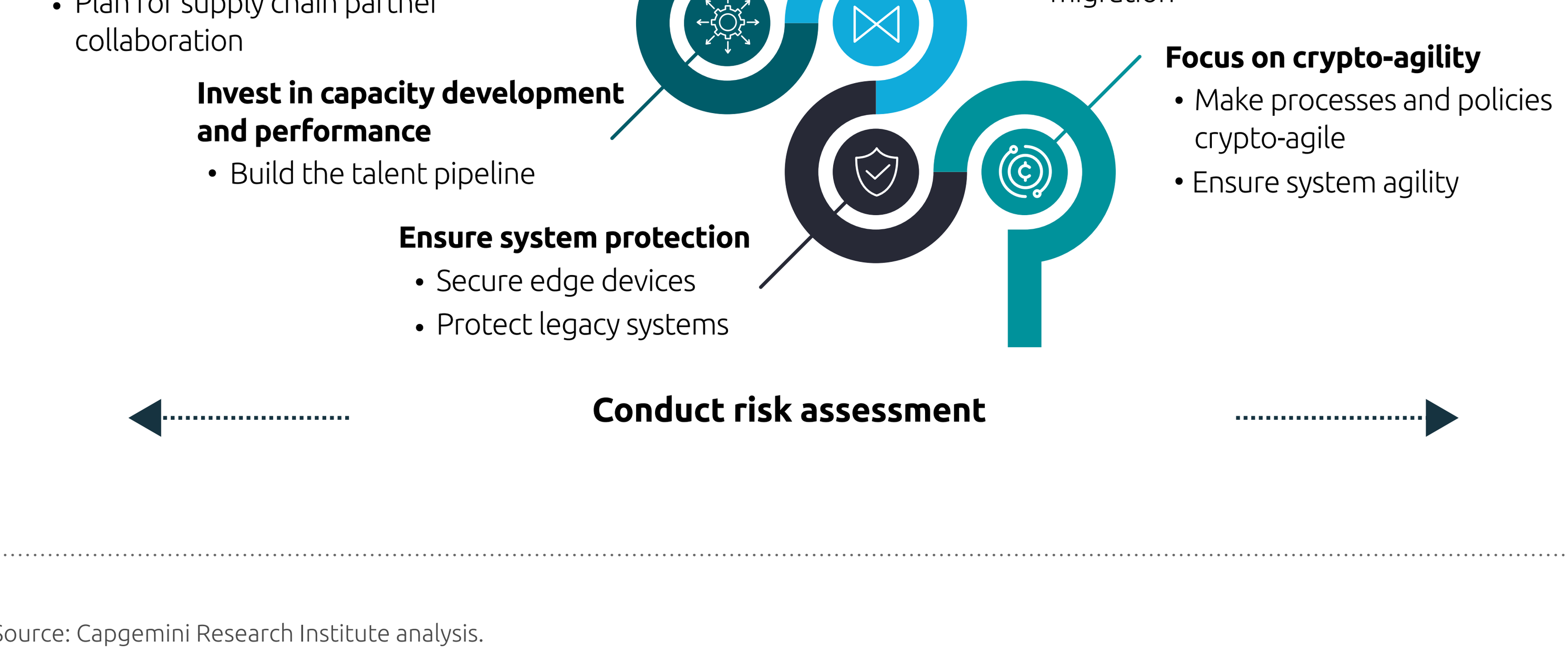
Technical foundations

- Understanding of algorithms
- Cryptographic inventory
- Hardware infrastructure
- Physical products and embedded systems
- Enterprise systems and security layer

Source: Capgemini Research Institute analysis.

15% of early adopters are quantum-safe champions that lead in both organizational and technical foundations

How organizations can make themselves quantum-safe



Source: Capgemini Research Institute analysis.

Download report

Subscribe to our research