Future encrypted

Why post-quantum cryptography tops the new cybersecurity agenda

Capgemini RESEARCH INSTITUTE

#GetTheFutureYouWant

Table of contents

Executive summary

Quantum computing is rapidly advancing, threatening to break today's encryption standards such as RSA and ECC. Sensitive data intercepted now could be decrypted later—posing a serious risk to privacy, compliance, and national security. To stay ahead, organizations must prioritize quantum-safe cryptography today, ensuring long-term cyber resilience and trust in a post-quantum world.

Why quantum safety is a priority: The rapid progress of quantum computing has left traditional methods and public-key cryptography vulnerable. "Harvest-now, decrypt-later" attacks, together with tightening regulations and changes in the technology stack have elevated quantum safety from a technical concern to a C suite mandate. Becoming quantum-safe is a complex, multi-year effort that must begin now. Delaying action could expose critical assets and erode trust. Regulatory demands, customer expectations, and competitive advantage all favor early movers. In cybersecurity, being early means being safe.

Most organizations have quantum safety on their radars: Seven in 10 organizations we surveyed are assessing or deploying quantum-safe measures (we refer to these as "early adopters"). Six in ten early adopters believe that quantum breakthroughs can occur within the next decade. Over half recognize that early investment will yield advantages. Most recognize post-quantum cryptography (PQC) as the best option with which to address quantum-security risks.

However, 30% of the overall sample still underestimate the threat, risking future data exposure and regulatory penalties.

Organizations are gradually exploring PQC transition: Roughly half of early adopters are running pilots, but skills gaps, budget uncertainty, and limited availability of solutions have slowed progress. Most lean on specialist vendors and cloud providers for proofs-of-concept (PoCs), hardware upgrades, and hybrid-transport layer security (TLS) services.

Executive summary

Few organizations are ready for PQC transition: Only a minority (16% of early adopters and 11% of the overall sample) qualify as "quantum-safe champions," who combine mature governance with strong technical execution. Gaps typically lie in organizational strategy, cryptographic inventory, supply-chain engagement, and hardware infrastructure. The practices of the quantum-safe champions offer a blueprint for others.

How organizations can be quantum-safe: PQC demands a strategic, long-term approach—it's not a one-time compliance checkbox but a continuous journey toward resilience. Embracing crypto-agility ensures organizations can adapt swiftly as quantum-safe standards and threats evolve.

- **Conduct quantum risk assessment:** Maintain a live cryptographic inventory and rank every asset by sensitivity to guide risk-based mitigation.
- **Create awareness of PQC:** Drive enterprise-wide education and establish a governance structure that keeps quantum security on the C-suite agenda.
- **Plan for transition:** Launch targeted PQC pilots and craft a phased migration roadmap that scales lessons learned across the enterprise.
- **Focus on crypto-agility:** Equip teams, design infrastructure, and software so cryptographic algorithms can be swapped efficiently as standards mature.
- **Ensure system protection:** Apply quantum-safe controls to both edge devices and legacy systems, with secure-update mechanisms built in.
- **Invest in capacity development and performance:** Fund dedicated teams and upskill staff to sustain PQC adoption without sacrificing system throughput while investing in developing computational, bandwidth, and storage capacity.
- **Strengthen collaboration:** Insert quantum-safe clauses as standard in supplier contracts and foster cross-industry partnerships to accelerate joint readiness.

Who should read this report and why?

This report is essential reading for CISOs, CIOs, CTOs, and Heads of Information Security responsible for safeguarding critical infrastructure, sensitive data, and long-term digital trust. As quantum computing advances, cryptographic systems that underpin secure communications, authentication, and key exchange are at risk. Leaders in security, compliance, and enterprise architecture must understand the timeline, technical landscape, and strategic decisions required to adopt post-quantum cryptography (PQC) and ensure crypto-agility across systems.

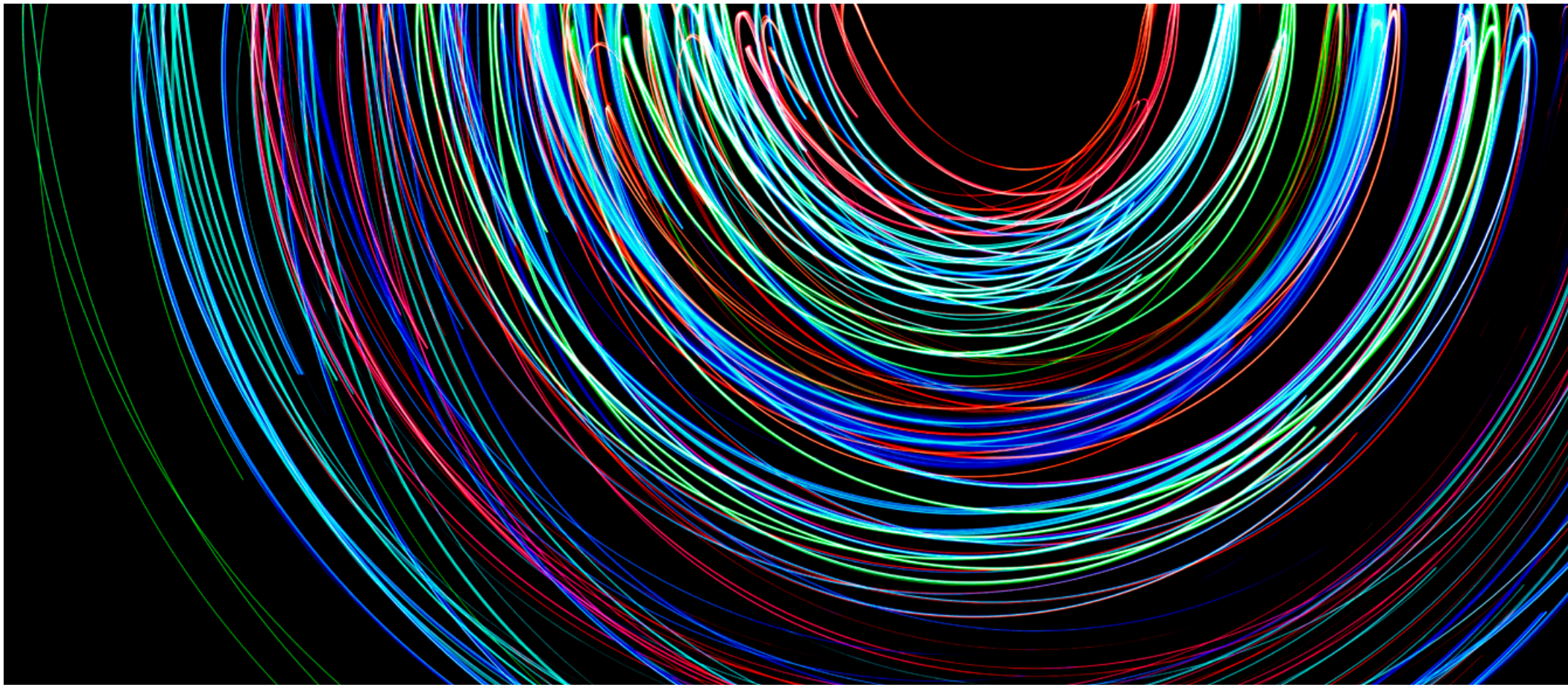
It is also highly relevant for IT infrastructure leaders, PKI managers, and product security teams working in organizations where data confidentiality and integrity must be preserved over extended timeframes. For organizations with complex supply chains or global regulatory exposure, this report offers a roadmap to assess quantum readiness, launch effective PQC pilots, and manage cross-functional transformation. Whether you're just beginning to explore quantum threats or advancing toward full migration, this report provides actionable insights grounded in research, industry benchmarks, and expert guidance.

This report is based on the findings of a comprehensive survey of 1,000 organizations with annual revenue of $1 billion across 13 sectors and 13 countries in Asia–Pacific, Europe, and North America and in-depth interviews with 16 selected executives. 70% of those surveyed that we refer to as "early adopters" in this report, are either working on or planning to work on quantum-safe solutions in the next five years.

See the research methodology at the end of the report for more details on the organizations surveyed.

70%

of the organizations surveyed that we refer to as "early adopters" in this report, are either working on or planning to work on quantum-safe solutions in the next five years.



Definitions

Terminology	Acronym/definition
PQC	Post-quantum cryptography
Quantum safety	Protecting data from future quantum computers that break encryption
Harvest-now, decrypt-later	Attackers steal encrypted data now, expecting to decrypt it later using future, more powerful technologies
Q-Day	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
PKC	Public key cryptography
CRQC	Cryptographically relevant quantum computer
Cryptographic inventory	A comprehensive list of all cryptographic assets, algorithms, and protocols in use
Crypto-agility / cryptographic agility	Ability to quickly switch cryptographic algorithms without major system or software changes
NCSC – UK	National Cyber Security Centre – UK
NIST	National Institute of Standards and Technology
NSA	National Security Agency

Terminology	Acronym/definition
TLS	Transport layer security
RSA	Rivest–Shamir–Adleman (a public-key cryptosystem, an asymmetric encryption algorithm, used for secure data transmission and digital signatures)
ECC	Elliptic curve cryptography (a type of public-key cryptography that uses elliptic curves to generate keys)
QKD	Quantum key distribution
MFA	Multi-factor authentication
PKI	Public-key infrastructure
AES	Advanced Encryption Standard
VPN	Virtual private network
SHA-256	Secure hash algorithm 256-bit (a cryptographic hash function that produces a 256-bit hash value (32 bytes) from any input data)
FIPS	Federal Information Processing Standard
Mosca's theorem	Mosca's theorem highlights that if quantum computers can solve factoring and discrete logarithms, then all current public-key cryptography becomes insecure, urging quantum-safe alternatives. According to this theorem, (X+Y)>Z, the amount of time that data must remain secure (X) plus the time it takes to upgrade cryptographic systems to become quantum-safe (Y) is greater than when large-scale quantum computers will be available with enough power to break cryptography (Z), you have already run out of time.

Why is quantum safety a priority?

Quantum computing harnesses quantum mechanics to solve problems far beyond the reach of classical computers. It can bring greater efficiencies in risk management, discovery of lightweight materials or new drugs, addressing climate change, among other areas. Our research on "quantum technologies" explored how organizations can prepare to leverage this quantum advantage.[1] However, this potential of quantum also comes with risks it can pose to today's cybersecurity.

As quantum power grows, so does the urgency for quantum-resilient security. Organizations must assess their readiness to safeguard sensitive data against quantum threats. Cryptographic agility – the ability to adapt swiftly and implement new cryptographic solutions – is essential to counteract

the vulnerabilities posed by quantum computing. To ensure long-term data security and foster trust in digital systems, the adoption of quantum-safe measures is paramount.

- **Harvest-now, decrypt-later attacks are already stealing data**

Harvest-now, decrypt-later attacks rely on the acquisition of currently unreadable data with the possibility of decrypting it after "Q-Day."[2] Sensitive data such as customer, health, or financial data siphoned off now could be exposed once Q-Day arrives. Our research has shown that this is a concern for 65% of organizations. In June 2025, researchers reported the leakage of 16 billion compromised login credentials from 30 exposed databases, giving cybercriminals unprecedented access to identity theft, account takeovers.[3] The scale of this highlights the massive problem organizations will need to tackle once the encryption algorithms can be broken down by quantum computers.

- **Regulators are encouraging the transition to quantum-safety**

In August 2024, the US National Institute of Standards and Technology (NIST) announced the first three (CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+) post-quantum algorithms. These were formulated as the result of a huge eight-year effort, and NIST encourages system administrators to begin integrating them immediately.[4] Further, the National Security Agency (NSA) has released guidance recommending the deprecation of the Rivest–Shamir–Adleman (RSA) algorithms with key lengths shorter than 2048 bits – equivalent to approximately 112 bits of symmetric security strength – as well as elliptic curve cryptography (ECC), by 2030. The use of these algorithms is expected to be disallowed entirely by 2035.[5] The European Union issued a roadmap recommending its member states to start transitioning to PQC by the end of 2026. At the same, it recommends that critical infrastructures should be transitioned to PQC as soon as possible and no later than by the end of 2030.[6]

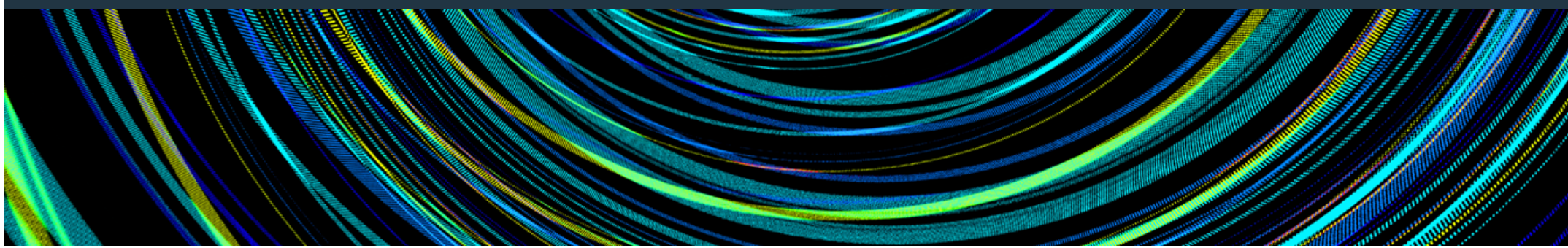
- **The ecosystem is already adapting**

Major cloud providers are rolling out support for transition to PQC. AWS began enabling Kyber-based (a post-quantum algorithm standardized by NIST) key exchange for clients;[7] Cloudflare has deployed support for hybrid key agreements for TLS handshakes and has announced the rollout of PQC across its whole platform.[8] Apple announced PQ3, which provides defenses against quantum attacks, for its iMessage platform.[9] Microsoft announced PQC support for its Windows Insiders Canary builds (27852 and above), allowing developers to experiment with PQC.[10] And one of the widely used software libraries, OpenSSL, released its final version (3.5) in April 2025 with support for PQC algorithms.[11]

- **Time is running out**

The quantum threat isn't a distant concern – it's a present and pressing one. Most CISOs still underestimate the scale of transformation required: from recompiling thousands of custom applications to replacing cryptographic libraries, rotating keys, updating HSMs, and reissuing certificates. For sectors like banking, this is a monumental lift. And with everyone soon scrambling for the same scarce quantum-safe talent, the window to act is rapidly closing. By planning for the multi-year migration and budgeting for the transition early, organizations can avoid regulatory penalties and expensive hardware upgrades in the case of a quantum breakthrough. Further, this migration also signals a strong cybersecurity posture to stakeholders.

Marco Pereira, Global Head of Cybersecurity at Capgemini, summarizes, *"Quantum readiness isn't about predicting a date–it's about managing irreversible risk. Every encrypted asset today could become tomorrow's breach if organizations delay adopting post-quantum protections. Transitioning early ensures business continuity, regulatory alignment, and long-term trust."* The transition to quantum is no longer purely theoretical. While it is estimated that building a CRQC – capable of breaking RSA-2048 or ECC – is likely within five to 10 years, focusing solely on when Q-Day will occur is a risky maneuver; by the time a quantum adversary emerges, it will be too late for organizations to retrofit their cryptographic foundations. Regulations, technological changes, and the market mandate that organizations embed quantum-safe solutions into their strategy and operations, with urgency.



“Quantum readiness isn’t about predicting a date–it’s about managing irreversible risk. Every encrypted asset today could become tomorrow’s breach if organizations delay adopting post-quantum protections. Transitioning early ensures business continuity, regulatory alignment, and long-term trust.”

Marco Pereira
Global Head of Cybersecurity at Capgemini

01 Quantum safety is on the radar of most organizations

A conventional computer is estimated to require (a notional) 300 trillion years to break RSA-2048 by factoring public keys. Craig Gidney from Google estimates that factoring a 2048-bit RSA key could take under a week using fewer than a million noisy qubits. With advances in error correction, hardware, and algorithms, the task might be completed in hours or days – marking a 1,000x improvement over the past 15 years.[12] Recent advancements in quantum computing include Microsoft's Majorana 1 chip,[13] which leverages a novel "topoconductor" material to reduce qubit error rates, and China's Tianyan-504 system, featuring a 504-qubit superconducting chip named Xiaohong.[14] These developments showcase progress in both qubit fidelity and scalability. Additionally, China's Zuchongzhi-3, a 105-qubit superconducting processor, has demonstrated quantum advantage in specific sampling tasks.[15]

A cryptographically relevant quantum computer (CRQC) would render today's public key cryptography obsolete. Widely used algorithms such as RSA, ECC, and Diffie-Hellman – core to secure key ex-change and digital signatures – would be broken by quantum attacks, compromising secure communications across email, VPNs, websites, financial transactions and critical infrastructure. Protocols such as TLS/SSL, SSH, and many blockchain implementations would become vulnerable. The impact would ripple across sectors, undermining confidentiality and operational continuity.

Seven in ten organizations are either currently working on or are planning to use quantum-safe solutions in the next five years

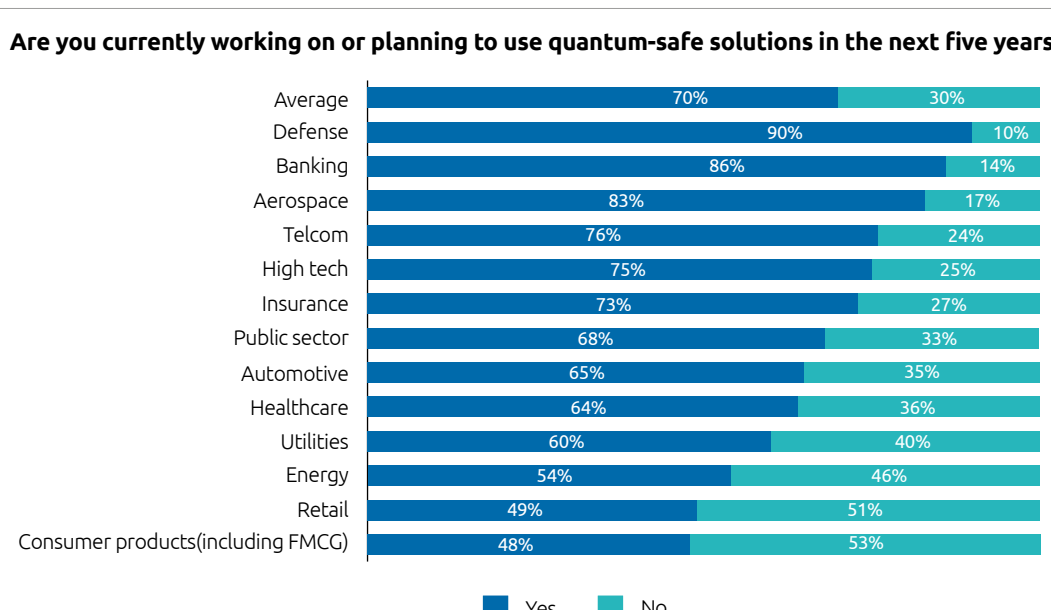
Our survey of 1,000 executives from global organizations with revenues over $1 billion, with key C-suite leaders such as CTOs, CIOs, and CISOs, reveals that 70% of these organizations are either working on or planning to implement quantum-safe solutions within the next five years. These are the "early adopters" (see figure 1). Our previous cybersecurity research[16] indicates that 92% of organizations had experienced a cybersecurity breach in the preceding 12 months. This underscores the importance of quantum security as businesses prepare to safeguard their digital infrastructures.

30%

of surveyed organizations are not working on quantum-safe solutions currently and don't plan to do so within the next five years.

"Once quantum computers are operational, they could breach all existing encrypted communications," says Rinat Zilberstein, AT&T Israel General Manager and VP R&D at AT&T.[17] Over 80% of early adopters have global revenue exceeding $10 billion, reflecting the imperative to secure future digital infrastructures.

Figure 1.
Seven in 10 organizations say they are 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.

The defense sector leads in adopting quantum-safe solutions, with 90% of organizations planning to implement within the next five years. Banking follows at 86%, while aerospace also shows strong interest at 83%. In contrast, both the consumer products and retail sectors lag significantly, with only 48% and 49%, respectively, planning to adopt these solutions.

90%

of defense sector organizations are currently working on or planning to adopt quantum-safe solutions in the next five years

Most early adopters understand the need for quantum safety

There is a consensus that quantum computing threats are not imminent but are expected to become significant within the next decade, as anticipated by 61% of early adopters, while 17% expect breakthroughs within the next five years (see figure 2).

Many organizations recognize the critical importance of ensuring their systems are secure against quantum computing threats. Huawei, for example, is testing quantum encryption to improve internet security.[18] This proactive approach is vital for safeguarding sensitive data and maintaining robust cybersecurity measures. *"Early PQC adoption isn't just about security – it's a strategic advantage. It builds customer trust, avoids costly retrofits, and positions us ahead of regulatory mandates,"* adds Vivek Sharma, Head of Global Partner Management at Bosch.

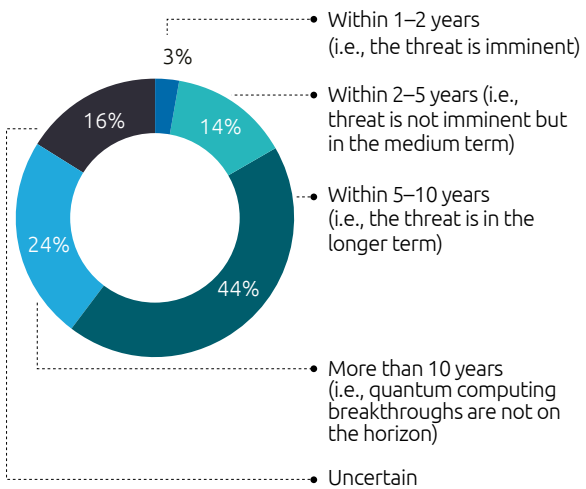
61%

of early adopters believe that quantum computers will achieve the capability to break current encryption methods within the next 10 years

Figure 2.

Around six in ten early adopters believe Q-Day can happen within the next decade

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

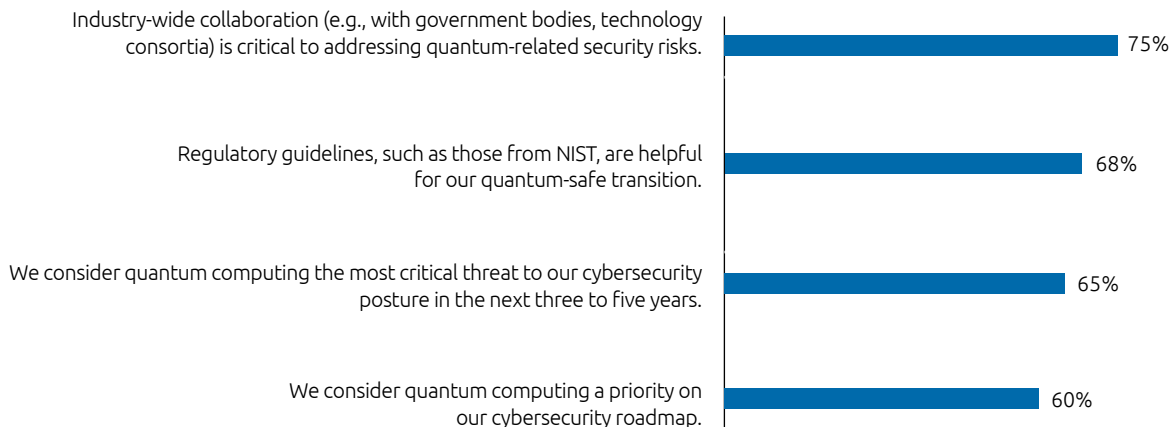


Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 703 early adopters.

Quantum computers could soon advance to the point where they can break current encryption standards, prompting a shift to quantum-resistant algorithms. A CISO at a global provider of customer relationship management and business-process outsourcing services says, *"In two years, quantum will become a common discussion at the C-level. Things are moving too fast to ignore it much longer."* Around 65% of organizations in our research consider quantum computing the most significant threat to their cybersecurity in the next three to five years. Organizations in the UK (68%), US (69%), Australia (75%) and France (68%) view quantum computing as a significant cybersecurity threat in the next three to five years, particularly in the aerospace (71%) and defense (68%) sectors.

As shown in figure 3, 75% say industry-wide collaboration (e.g., with government bodies, technology consortia) is critical to addressing quantum-related security risks.[19] For example, BTQ Technologies, a quantum company offering PQC solutions, signed a memorandum of understanding (MOU) with South Korean quantum organizations to support global collaboration in industrial standards, events, and industry-academic programs, advancing quantum technology innovation.

Figure 3.
Two in three early adopters of quantum safety consider quantum computing the most critical threat to their cybersecurity posture in the next 3–5 years



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

Considering the improvements to error-correcting codes, hardware fidelities, and algorithmic improvements, Q-Day does not seem theoretical anymore. Over half (57%) of organizations say they are preparing for Q-Day by adopting quantum-safe practices, regardless of when large-scale quantum computing becomes a reality. Commenting about the urgency and awareness, Julio Padilha, CISO of Volkswagen & Audi, South America, said *"People don't believe it will happen until it happens. The first public attack breaking encryption will trigger urgency. Until then, it's hard to justify investment in something we can't yet see."* Quantum threats are real and imminent. Without serious investment in quantum-safe initiatives today, we risk being blindsided tomorrow. The race is on – act now or fall behind in securing our digital future.

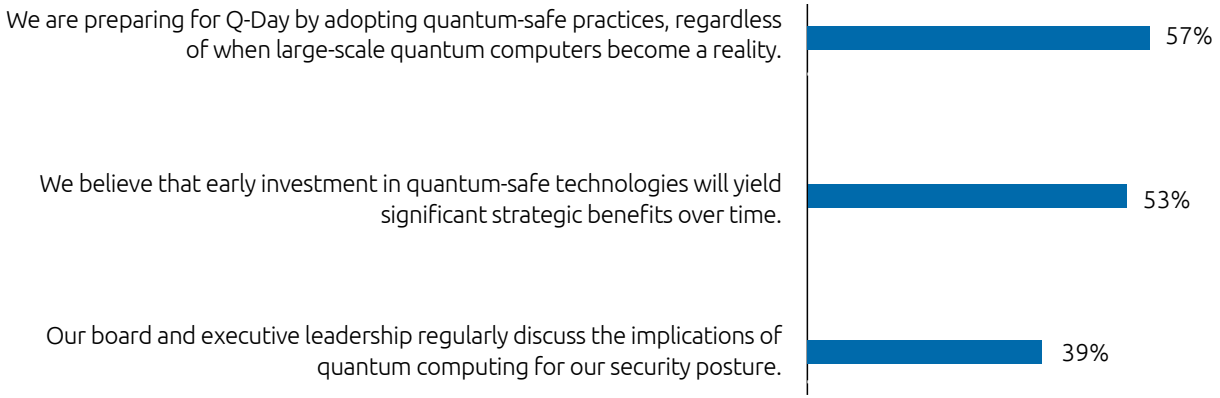
57%

of early adopters say they are preparing for Q-Day by adopting quantum-safe practices, regardless of when large-scale quantum computing becomes a reality.

“People don’t believe it will happen until it happens. The first public attack breaking encryption will trigger urgency. Until then, it’s hard to justify investment in something we can’t yet see.”

Julio Padilha
CISO of Volkswagen & Audi, South America.

Figure 4.
Over half of early adopters believe that early investment in quantum-safe technologies will yield significant strategic benefits



Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 216 senior-level executives from early adopters.

Three-quarters (75%) of executives cite “regulatory compliance” and 71% “futureproofing against quantum attacks” as key factors driving their organization’s consideration for adopting quantum-safe technologies. We also see federal bodies such as NIST and the UK’s National Cyber Security Centre (NCSC) issue regulatory guidance and recommendations (for example, the NCSC focuses on quantum-resistant encryption to protect critical sectors by 2035).[20]

Among the organizations we surveyed, 70% of early adopters cite data encryption among the top five cryptographic functions to be transitioned to quantum-safe alternatives, suggesting that quantum computing could change how organizations approach data encryption forever.[21]

The “harvest-now, decrypt-later” threat is immediate. On the surface, no breach is visible, no alarms sound, and encryption holds – for now. Though undetected now, the breach threatens long-term confidentiality – especially for sensitive assets like medical records, trade secrets, or classified information. Data stolen today may be decrypted by future quantum computers.

The shift to quantum-safe encryption is more than a technical upgrade—it’s a strategic imperative. While symmetric cryptography is expected to remain secure with longer key lengths, replacing today’s public-key systems (e.g., RSA, ECC) is far more complex. Emerging solutions like quantum key distribution (QKD) show promise for specific use cases but aren’t yet broadly scalable. At the same time, key management in hybrid cryptographic environments (where classical and post-quantum algorithm s coexist) remains a challenge.

71%

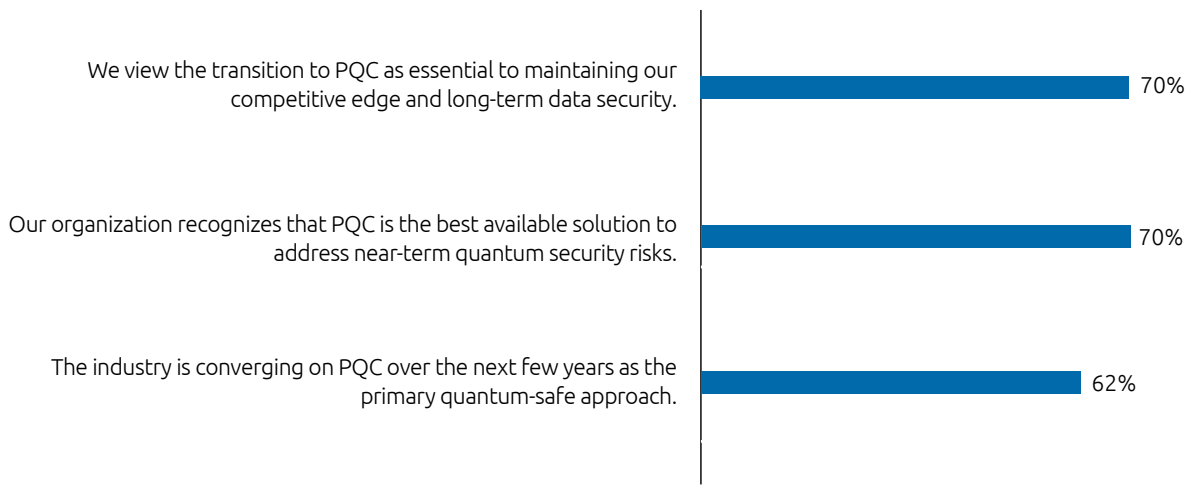
of early adopters cite "futureproofing against quantum attacks" as a key factor driving their organization's consideration for adopting quantum-safe technologies.

Seven in 10 executives view the transition to PQC as essential

Quantum computing poses a significant threat to traditional cryptographic systems such as RSA and ECC, which quantum algorithms can decrypt "easily." PQC migration is preferred over other quantum-security solutions because it provides a comprehensive approach to securing data. While other solutions such as QKD offer specific benefits, they also bring scalability challenges, hardware dependencies, etc. PQC offers broader applicability across various cryptographic functions, making it a more practical and robust solution.

As shown in figure 5, 70% of early adopters of quantum-safe solutions say they view the transition to PQC as essential to long-term competitiveness and data security. Vodafone, for example, has trialed quantum-safe tech to protect smartphone browsing, applying PQC standards to current encryption algorithms.[22]

Figure 5.
Seven in 10 early adopters of quantum-safe solutions view the transition to PQC as essential to maintain their competitive edge



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

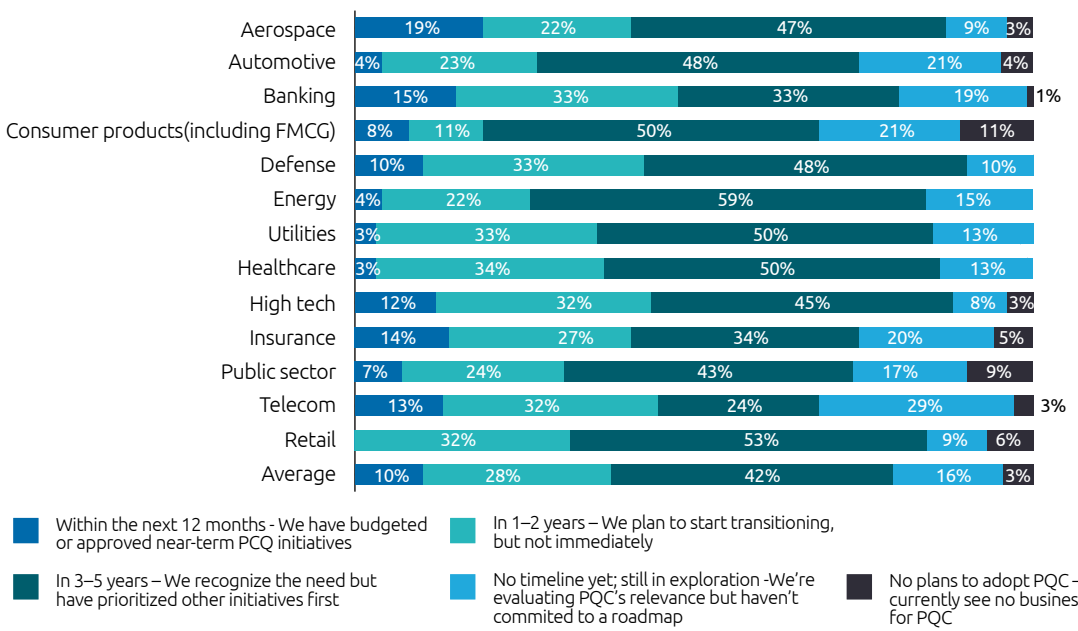
As shown in figure 5, 62% say the industry is reaching consensus on PQC as the primary quantum-safe approach over the next few years. This includes 71% of organizations in the aerospace industry, and utilities (70%) and healthcare (69%) sectors. Healthcare, for example, is a frequent target for cyberattacks, with patient data highly vulnerable. In 2024, a ransomware attack involving Change Healthcare, a provider of revenue and payment services, impacted as many as 190 million individuals.[23]

The NCSC suggests organizations should have in place an initial plan for PQC migration by 2028 and carry out their early, highest-priority PQC migration activities by 2031, which is in another two- to six-year timeline.[24] In parallel, we see nearly two in five early adopters plan to start their PQC transition in the next two years. Luciano Carolino, IT security specialist at Bradesco bank in Brazil, adds, *"We began our quantum-safe journey in 2023 with a cryptographic posture and maturity assessment. It's a long-term roadmap, starting with building a full inventory of cryptographic assets, using a risk-based approach for prioritization, across infrastructure and applications."* Figure 6 shows that banking (47%) and telecom (45%) sectors are leading the charge in planning for PQC adoption within the next two years (in terms of budgeting for PQC initiatives and plans for transition). Defense (43%) and high tech (43%) sectors follow closely, indicating a growing awareness of future cryptographic threats across industries.

Figure 6.

Nearly two in five early adopters will have budgeted and planned for transition in the next two years

When do you anticipate your organization will initiate (or has initiated) a formal plan to adopt PQC?



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

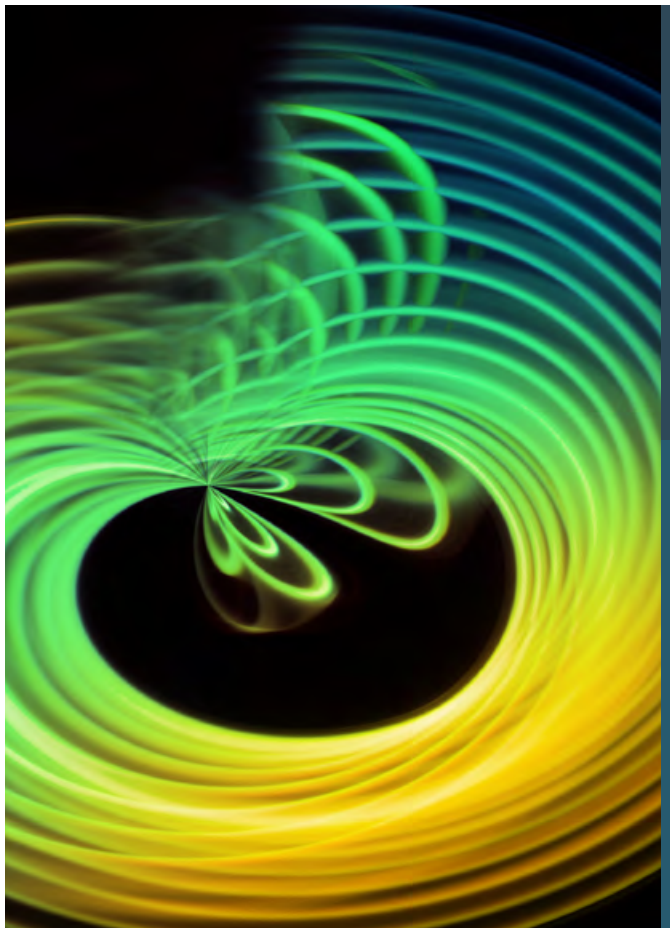
62%

of early adopters say the industry is reaching consensus on PQC as the primary quantum-safe approach over the next few years.

Organizations are preparing for the quantum threat, and the pace of PQC adoption is accelerating. But there remains uncertainty around how much time security teams have to prepare. *"If quantum cryptography is embedded in quality assurance for new programs, we'll be ready for the unknown. That's the best strategy – to be prepared before the change is forced upon us,"* adds Adriano Luiz de Oliveira, Head of cybersecurity, CNP Seguradora, a subsidiary of the CNP Assurances group, a multinational insurance company.

"Early PQC adoption isn't just about security – it's a strategic advantage. It builds customer trust, avoids costly retrofits, and positions us ahead of regulatory mandates."

Vivek Sharma
Head of Global Partner Management, Bosch



Understanding quantum-safe solutions

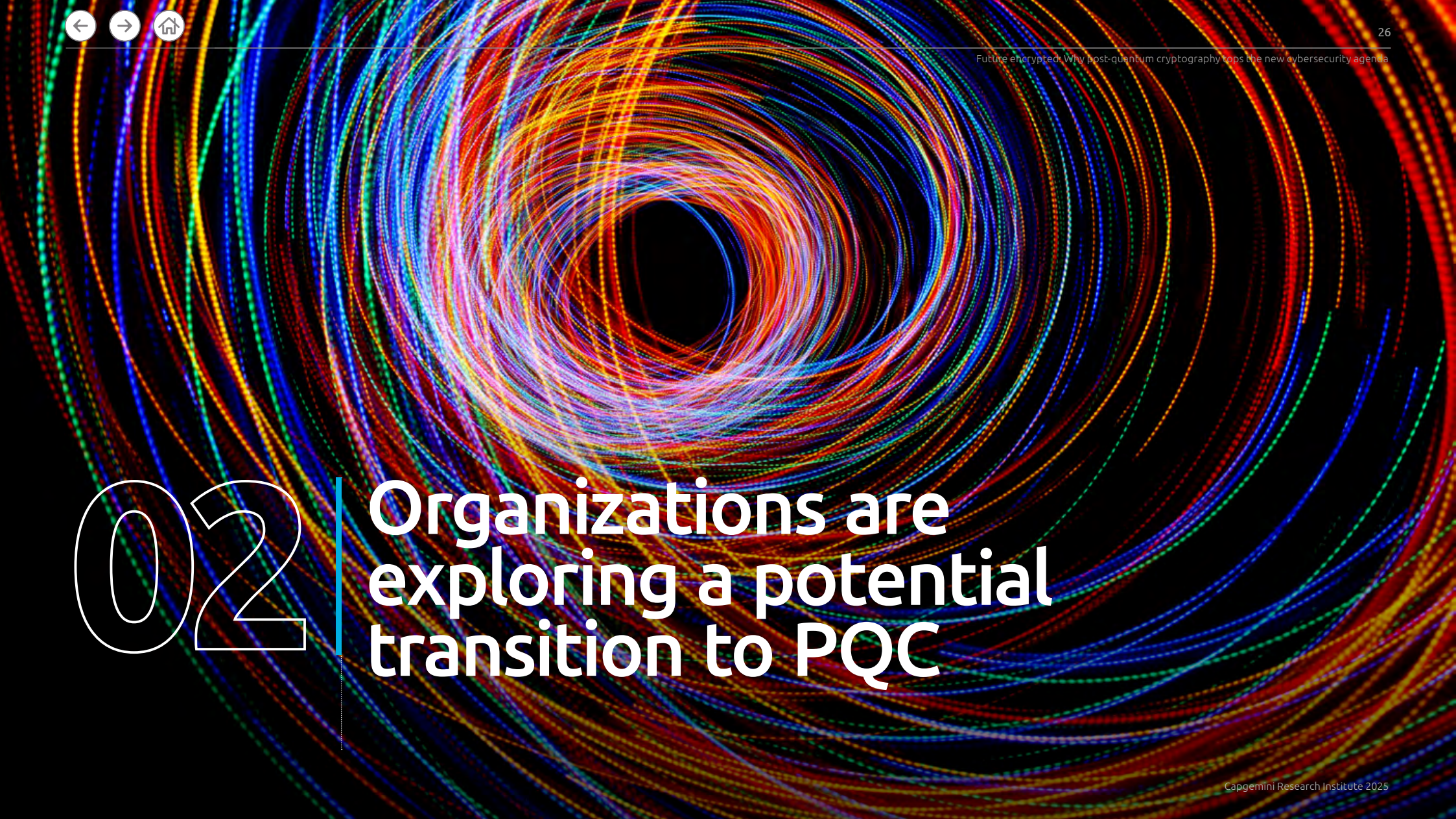
Post-quantum cryptography (PQC) is structured to ensure robust cybersecurity against the computational power of quantum computers. As quantum computing progresses, traditional cryptographic methods are expected to be gradually sidelined, though classical algorithms will likely persist alongside PQC in hybrid models like cascaded encryption – at least in the near term, making PQC a prerequisite. The below section compares various quantum security solutions currently available, highlighting PQC's importance to organizations' achieving cryptographic agility.

1. **PQC:** Cryptographic algorithms designed to resist quantum computing attacks, including lattice-based, hash-based, code-based, and multivariate polynomial cryptography.[25]
2. **Quantum key distribution (QKD):** Uses quantum mechanics to securely distribute encryption keys, inherently detecting and thwarting any eavesdropping attempts.[26]
3. **Fully homomorphic encryption:** Allows computations to be performed on encrypted data without decrypting it, ensuring data privacy even during processing.[27]
4. **Quantum random number generators (QRNG):** Generates "truly random" (i.e., completely unpredictable) numbers using quantum processes, enhancing encryption security.[28]
5. **Hardware security modules (HSMs):** A hardened, tamper-resistant device designed to protect cryptographic keys and manage cryptographic operations, making them resistant to attacks from quantum computers.[29]

Figure 7.
A comparison of quantum-safe solutions

Solution	Example	Maturity	Quantum hardware	Use case
PQC	ML-KEM (Kyber), ML-DSA (Dilithium), SPHINCS+ (FIPS 203-205 finalized in August 2024); FALCON (draft)	Commercially emerging. Open-source crypto library implementations; First FIPS-approved algorithms published; cloud (AWS), CDN (Cloudflare) and network vendors already piloting hybrid TLS/VPN modes	No – can run on classical central processing units (CPUs)/ HSMs	Public-key exchange, digital signatures, code-signing, public key infrastructure (PKI), secure email
QKD	BB84 protocol, E91 protocol, MadQCI	Technical limitations exist (needs classical/PQC authentication, specialized equipment, higher infrastructure costs), commercially available but niche	Yes – single-photon sources/ detectors, trusted-node or satellite links	Datacenters in finance, defense, telecom, and other critical infrastructure
Fully homomorphic encryption (lattice-based BFV/BGV/CKKS)	Gentry's fully homomorphic encryption	Emerging; production libraries exist	No	Privacy-preserving computations
QRNG	Photonic QRNGs	Higher costs and specialized hardware; 2024–25 silicon-photonic chips now reach 9–20 Gb/s and shrink size/cost dramatically; commercially available (with limitations)	Yes – quantum entropy source (laser, photon)	Cryptographic key generation, simulations, secure communications
PQC-capable (HSMs) and crypto-agile solutions	Thales SafeNet Luna HSM	Major vendors (Thales nShield, Entrust, Utimaco, IBM) ship firmware supporting ML-KEM/ML-DSA and hybrid TLS toolkits	No	Secure key generation/storage, root-of-trust for PQC rollouts

Source: Multiple online sources.



02 Organizations are exploring a potential transition to PQC

To ensure long-term protection of sensitive data, organizations must start integrating PQC alongside existing systems now. Waiting until quantum computers are fully capable could expose archived and in-transit data to decryption later.

Around half of early adopters are exploring PQC or running pilots

The White House's Office of Management and Budget (OMB) and Office of the National Cyber Director (ONCD) jointly finds that federal agencies will need approximately $7.1 billion (in USD) to transition their prioritized information systems to PQC between 2025 and 2035.[30] Meanwhile, the Quantum Insider's latest report projects the quantum security market to grow from ~$700 million today to ~$10 billion by 2030, driven by a CAGR of over 50%, with core segments including PQC, QKD, the quantum internet, and QRNGs.[31] We believe that the shift to PQC is not a matter of if, but when. Nearly 50% of early adopters are already exploring or assessing feasibility or piloting PQC solutions. Organizations must evaluate their cryptographic readiness and develop a clear roadmap for PQC adoption.

In 2024, NIST standardized a set of encryption algorithms for use against a notional quantum cyberattack. In March 2025 NIST selected a backup algorithm that can provide a second line of defense for internet traffic and stored data alike.[32] Unsurprisingly, 32% of organizations in our research say they have identified the preferred PQC algorithms (e.g., from NIST) and are aligning their internal standards accordingly.

As shown in figure 8, 13% of organizations say they are actively integrating PQC algorithms into selected systems and conducting performance, security, and compatibility tests. For example, Vodafone, in collaboration with a consortium GSMA and companies including SandboxAQ, is actively exploring and implementing PQC.[33]

13%

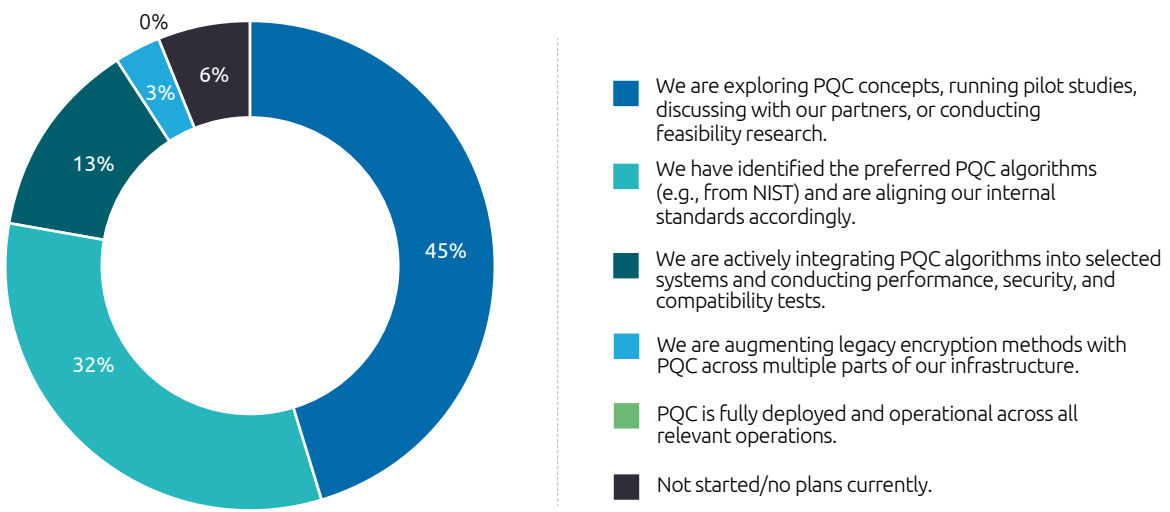
of early adopters say they are actively integrating PQC algorithms into selected systems and conducting performance, security, and compatibility tests.

32%

of early adopters say they have identified the preferred PQC algorithms (e.g., from NIST) and are aligning their internal standards accordingly.

Figure 8.
Nearly half of early adopters are exploring PQC concepts

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



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

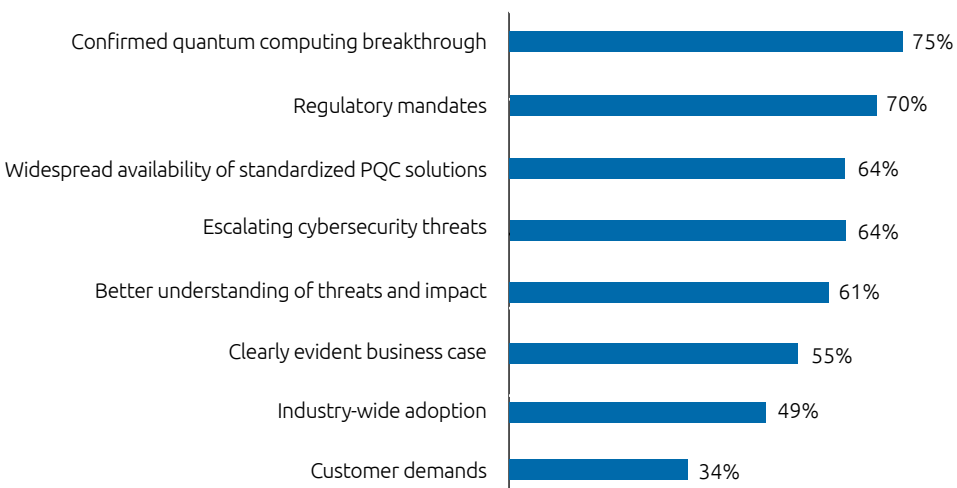
Our research also found that 14% of organizations have a structured team with defined roles and objectives. Currently, quantum-safe initiatives receive 2% of cybersecurity budgets, so organizations may need to prioritize quantum-safe technologies.

2%

percentage of cybersecurity budgets that is allocated to quantum-safe initiatives, on average.

Figure 9.
Three in four organizations say a confirmed quantum computing breakthrough would increase their organization's urgency to adopt PQC

How significantly would each of the following factors increase your organization's urgency to adopt PQC?



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

Ben Packman, Chief Strategy Officer at PQShield, a company offering quantum-resistant hardware and software solutions, says, *"We are not going to know when a cryptographically relevant quantum computer arrives – no one's issuing a press release. We'll either be ready or we won't."* The urgency of adopting PQC is heightened by significant government investments and the emergence of new cybersecurity threats. To mitigate the nascent risks posed by quantum advancements, organizations must prioritize their critical assets and implement phased actions. Strategic planning for PQC shifts is crucial to being prepared as new quantum capabilities materialize. The UK's £121 million investment in quantum technologies highlights the urgency for organizations to prepare for PQC.[34] We see that 70% of organizations cite a "regulatory mandate" as a top factor in increasing urgency to adopt PQC. Some of the notable regulatory and government guidelines include:

- The NCSC has set a 2035 deadline for national migration to PQC.[35]
- NIST's Transition to Post-Quantum Cryptography Standards (public draft) details the expected approach to transitioning from quantum-vulnerable cryptographic algorithms to post-quantum digital signature algorithms and key-establishment schemes.[36]

- The Cybersecurity and Infrastructure Security Agency (CISA), the NSA, and NIST jointly created a fact sheet to inform organizations, especially those that support critical infrastructure, about the impacts of quantum capabilities, and to encourage early planning for migration to PQC standards by developing a quantum-readiness roadmap.[37]
- In the United States, the June 2025 Executive Order directs that existing federal regulations and policy be revised to focus on securing third-party software supply chains, quantum cryptography, artificial intelligence, and internet of things ("IoT") devices. It also requires the Cybersecurity and Infrastructure Security Agency (CISA) to maintain a list of product categories where PQC-enabled tools are widely available.[38]
- European Telecommunications Standards Institute's (ETSI) Technical Report QSC 0024 (April 2024) proposes a repeatable framework for quantum-safe migrations.[39]
- GSM Association (GSMA), the trade association that represents the interests of mobile network operators (MNOs) worldwide, has published PQC guidelines for the telecom sector.[40]
- The EU Agency for Cybersecurity (ENISA) outlines the current state and mitigation strategies for quantum threats, in its Post-Quantum Cryptography: Current state and quantum mitigation report.[41]
- Singapore's Cyber Security Agency (CSA) is set to introduce guidelines in 2025 to help organizations prepare to manage quantum-computing risks.[42]

70%

of early adopters cite a "regulatory mandate" as a top factor in increasing urgency to adopt PQC.

"We began our quantum-safe journey in 2023 with a cryptographic posture and maturity assessment. It's a long-term roadmap, starting with building a full inventory of cryptographic assets, using a risk-based approach for prioritization, across infrastructure and applications."

Luciano Carolino
IT security specialist at Bradesco bank

Organizations must overcome a multitude of barriers

Organizations face numerous barriers in adopting PQC to strengthen their quantum-security postures. Challenges include a lack of awareness and expertise; integration complexities with existing infrastructure; limited standardization; lack of availability of mature solutions; lack of clear timelines; and uncertainty around cryptographic agility.

Credit rating agency, Moody's also notes the likely protracted and expensive nature of the transition to PQC, forecasting that implementing new cryptographic standards across devices could take 10–15 years. While the cost of the transition is hard to estimate, parallels can be drawn with the expensive, large-scale efforts required to address the Y2K bug.[43] And as figure 4 shows, only 39% of the organizations say their board discusses the implications of quantum computing for their security posture. This limited awareness will hinder the funding of transition programs. Additionally, the transition requires careful inventory of cryptographic assets, risk assessments, and long-term planning that balances performance, compliance, and cost considerations.

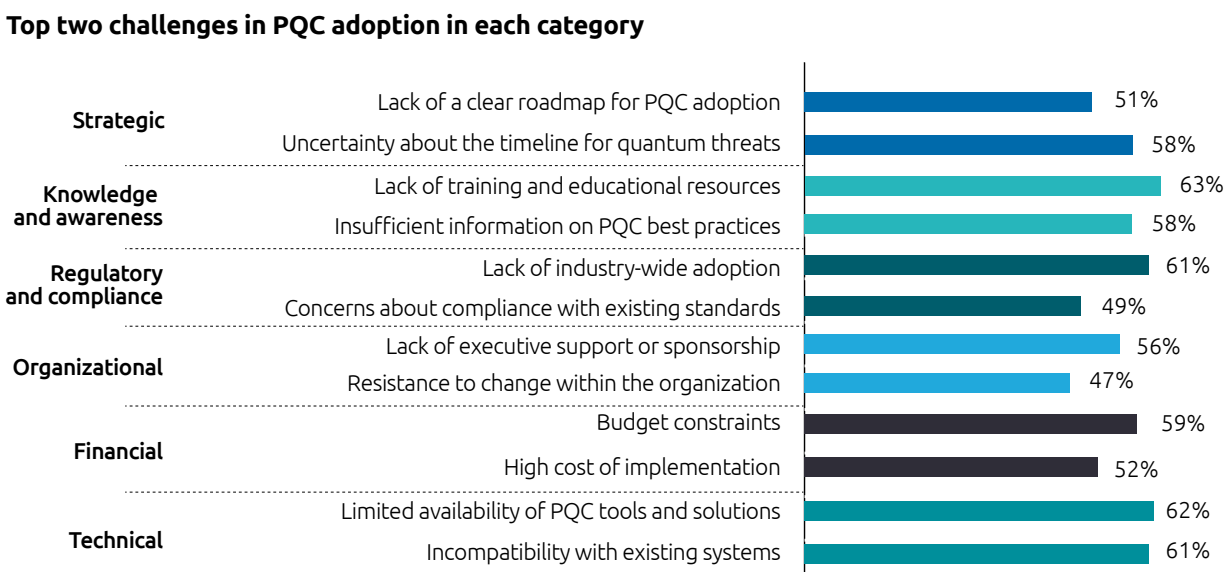
A key challenge in quantum security adoption is the limited availability of mature solutions. While NIST is selecting quantum-resistant algorithms, the security community continues to scrutinize them. PQC algorithms are new compared with RSA and ECC, which have had decades of validation. Dr. Michele Mosca, CEO & Co-founder, evolutionQ, a quantum-safe cybersecurity company, elaborates on the challenge to adoption, *"The hardest part is getting aligned on timelines and the whole ecosystem to agree on making sure the available solutions are secure against known threats and resilient against future code breaking."* This leads to uncertainty among organizations. Many delay adoption, assuming the quantum threat is distant, or the transition will be simple. This assumption risks future breaches, as today's encrypted data could be harvested and decrypted once quantum capabilities emerge.

Another key challenge discussed within most organizations is the lack of a clear timeline. Political and business-related pressure to begin work to mitigate the threat is stymied by a lack of certainty as to when quantum computers will attain that threat level.[44]

39%

percentage of early adopters that say their board discusses the implications of quantum computing for their security posture.

Figure 10.
More than three in five organizations say limited availability of PQC tools and solutions is a key challenge in adoption of PQC



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

Strategic uncertainty – 58% of organizations cite unclear quantum threat timelines, and more than half lack a roadmap – will hinder PQC adoption. A CISO at a global provider of customer relationship management and business-process outsourcing services adds, *"The biggest challenge will be finding people with the right knowledge. Everyone will be looking for the same experts at the same time."* Quantum breakthroughs will trigger a surge in demand for specialized talent. Organizations must act now – hire early, invest in upskilling, and build training pipelines. Collaborating with external experts and partners ensures readiness, resilience, and a competitive edge in the quantum future. Knowledge gaps are stark: 63% report insufficient training, and 58% lack best-practice guidance. Organizations must recompile every application using cryptographic libraries – an enormous task, especially for banks with thousands of custom apps – while also overhauling crypto infrastructure and reissuing all certificates. Starting now is vital to avoid future talent shortages and intense competition for niche skills. Regulatory concerns persist, with 61% noting absent industry guidelines and 49% worried about compliance.

Organizational inertia is also an issue, with 51% citing a lack of executive support for transition. Financially, 52% struggle with high implementation costs, and 59% with budget constraints. Technically, 62% cite limited tools and 61% system incompatibility. The migration process involves updating hardware, software, and extensive testing to avoid introducing new vulnerabilities. The scale of this transition necessitates meticulous planning and execution.[45]

58%

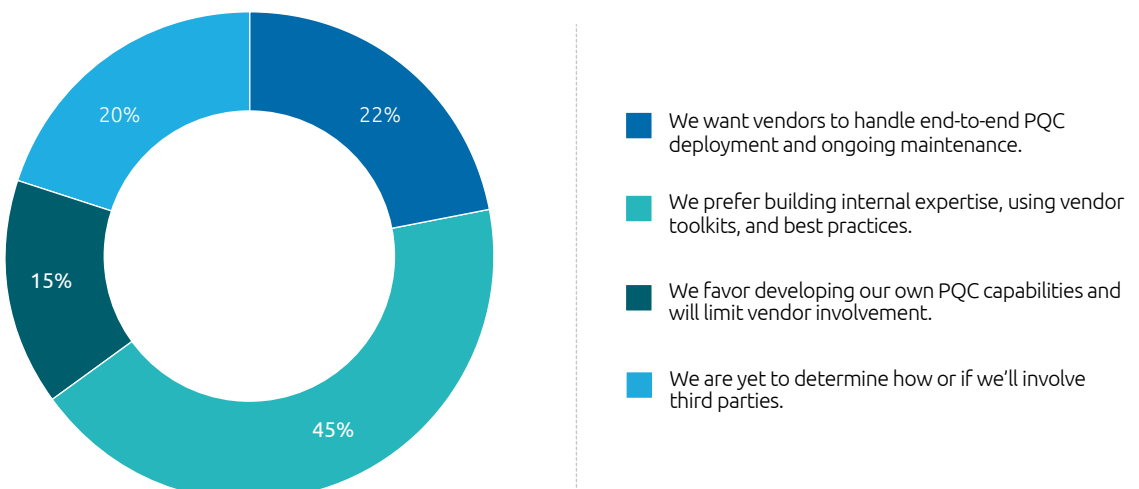
of organizations cite unclear quantum threat timelines will hinder PQC adoption.

Organizations turn to external partners to support the transition

As organizations transition to PQC, many are turning to external partners for guidance. These collaborations help navigate complex cryptographic migrations, ensure compliance with emerging standards, and accelerate the deployment of quantum-safe solutions. One in five (22%) wants external partners to handle end-to-end PQC deployment and ongoing maintenance.

Figure 11.
One in five organizations would like vendors to handle end-to-end PQC deployment

Organizations' view on partnering with external vendors or cloud providers to implement PQC solutions



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

To navigate the post-quantum landscape, organizations must identify or upskill individuals with expertise in quantum-security principles, who can facilitate collaboration with standard-setting bodies, analyze quantum threats, and develop comprehensive quantum-security roadmaps.[46] We see 58% plan to take advantage of vendor-led workshops or webinars to develop the necessary expertise, while 33% plan to partner with external training providers, universities, or industry consortia.

Quantum safety demands speed, scale, and specialization. No organization can do it alone. Engaging external experts is not a choice – it's a strategic imperative for survival in a post-quantum world. Without expert allies, your PQC readiness will fall dangerously behind.

"The hardest part is getting aligned on timelines and the whole ecosystem to agree on making sure the available solutions are secure against known threats and resilient against future code breaking."

Dr. Michele Mosca
CEO, evolutionQ Inc., and co-founder of the Institute for Quantum Computing at the University of Waterloo

Q&A with Michele Mosca, CEO, evolutionQ Inc., and co-founder of the Institute for Quantum Computing at the University of Waterloo, and Christian Schmitz, Managing Director, evolutionQ GmbH

Q: Are there any misconceptions about PQC readiness?

Michele: Yes. People assume PQC is plug-and-play. But some important use cases, and constrained environments like IoT, may not support current PQC standards. You need to test early. If you're not ready to fully trust a quantum-safe solution, use hybrid cryptography—combine classical and quantum-safe algorithms. It's a practical way to transition without losing the security provided by today's cryptography. Hybrid models offer a bridge to full PQC adoption.

Q: What's your recommendation for organizations starting post-quantum migration?

Christian: Run proofs-of-concept early. Understand performance issues, especially larger key sizes in signature algorithms. Don't approach migration blindly. That's definitely the recommendation—you have to take these larger key sizes into consideration.

Q: Are multifactor approaches relevant in a quantum-safe world?

Michele: Absolutely. It's not just about swapping in new cryptography and hoping for the best. The stakes are getting higher and the attackers have increasingly powerful tools like AI and soon quantum computing, so one must architect for resilience. Resilience is about surviving the unknowns. Even with PQC, fallback mechanisms and layered security are essential, for example, also leveraging novel pre-shared key and symmetric key approaches. Similar to how MFA makes end-point authentication more resilient.

Q: How do compliance and regulation influence PQC adoption?

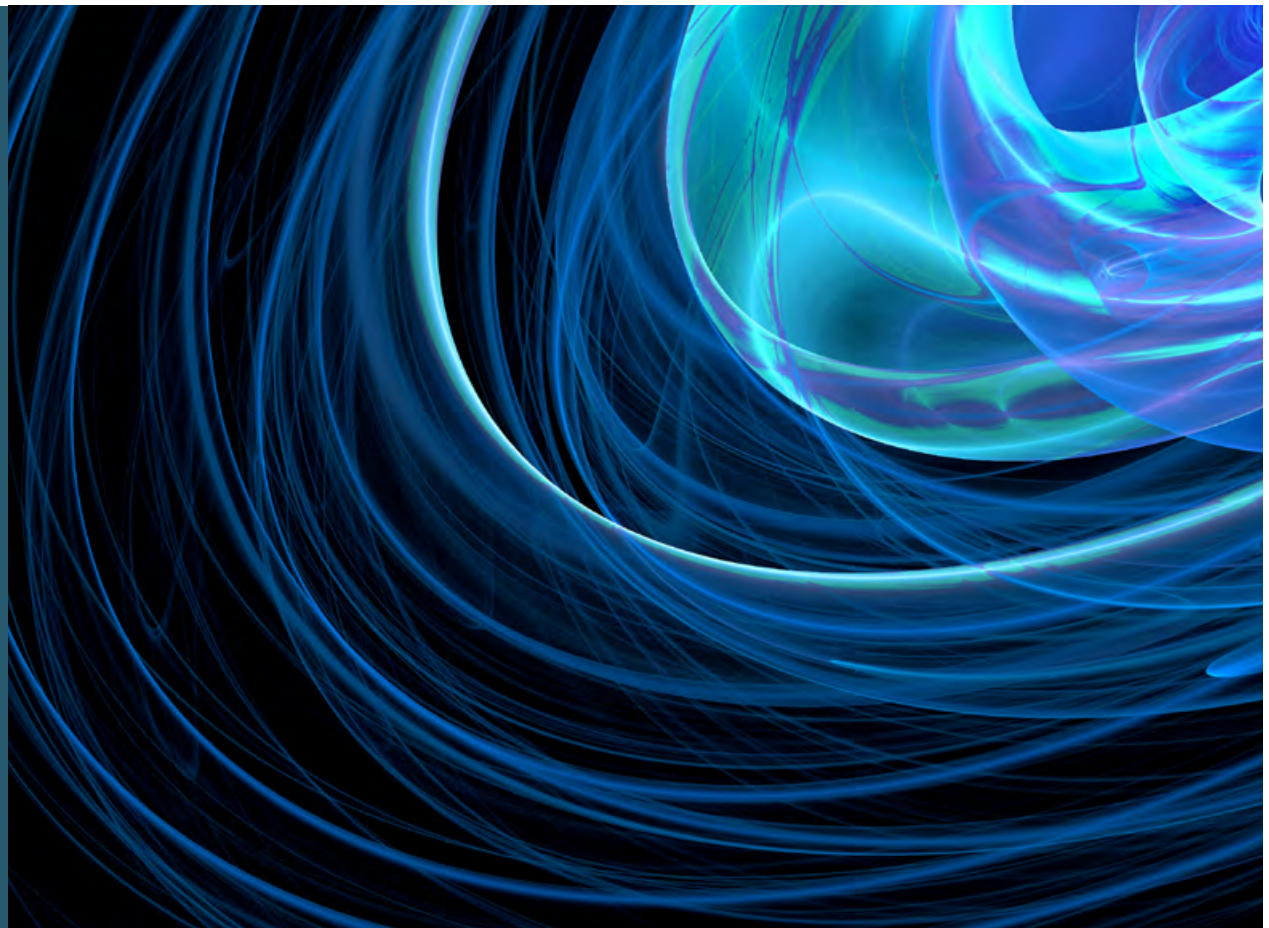
Christian: Clients are driven by compliance timelines. Some are waiting for mandates, others are proactive. But crypto-agility is key to future-proofing. A flexible architecture helps adapt to evolving standards.

Q: What's the impact of larger key sizes in PQC?

Christian: Signature algorithms often have significantly larger key sizes. These must be tested in advance to avoid surprises during migration. This isn't just a technical detail—it affects storage, transmission, and system design. You need to plan for it.

Q: What's the risk if organizations delay PQC adoption?

Michele: Delaying PQC also means missing out on aligning with evolving regulations and standards like DORA and NIST, which are already influencing sectors like finance and telecom. The threat isn't just about "harvest now, decrypt later" where data stolen today could be exposed once quantum computers mature. There's a serious risk of not protecting critical systems in time, or weakening systems through a rushed (and expensive) crisis management migration. This puts the authenticity and availability of information, the availability of business systems, and the control of connected devices at risk too. Readiness will soon become a business differentiator. Organizations that delay may face business continuity challenges and higher costs and reputational damage post-incident.



Q&A with Ben Packman, Chief Strategy Officer at PQShield

Q: Why is the market starting to move on PQC now?

Ben: The urgency stems from NIST's deprecation of RSA and ECC – disallowed by 2035. This reframes PQC as a compliance issue within a five- to 10-year window, not just a distant quantum threat. It helps move the conversation from "when will quantum arrive?" to "how do we prepare now?" – a shift that's critical for enterprise planning.

Q: Has PQC adoption already begun in the real world?

Ben: Yes. Billions of endpoints already use PQC. Chrome, Signal, Apple iOS, and Cloudflare have integrated it. PQShield has contributed to the research, algorithms, and protocols behind many of these implementations, making PQC a present-day reality – not just a future concept.

Q: How do you view the role of QKD versus PQC?

Ben: QKD and PQC solve different problems. QKD is point-to-point and good for detecting interception but lacks signatures and authentication. PQC supports one-to-many and many-to-many communication, making it more practical for enterprise-wide deployment.

Q: How should organizations begin their PQC journey?

Ben: Don't start with crypto inventory. Start by identifying your most critical data with long-term value. Then map the vendors touching that data. Most cryptography sits in the supply chain, only 20% of it maybe is in the direct control of an organization, rest is outside their control.

Q: How do you convince skeptics to act now?

Ben: Frame PQC as a compliance timeline, not a quantum scare. Show the board what's already covered, what's in progress, and where help is needed. That changes the conversation from fear to achievable action.

03 Few organizations are ready for the transition to PQC

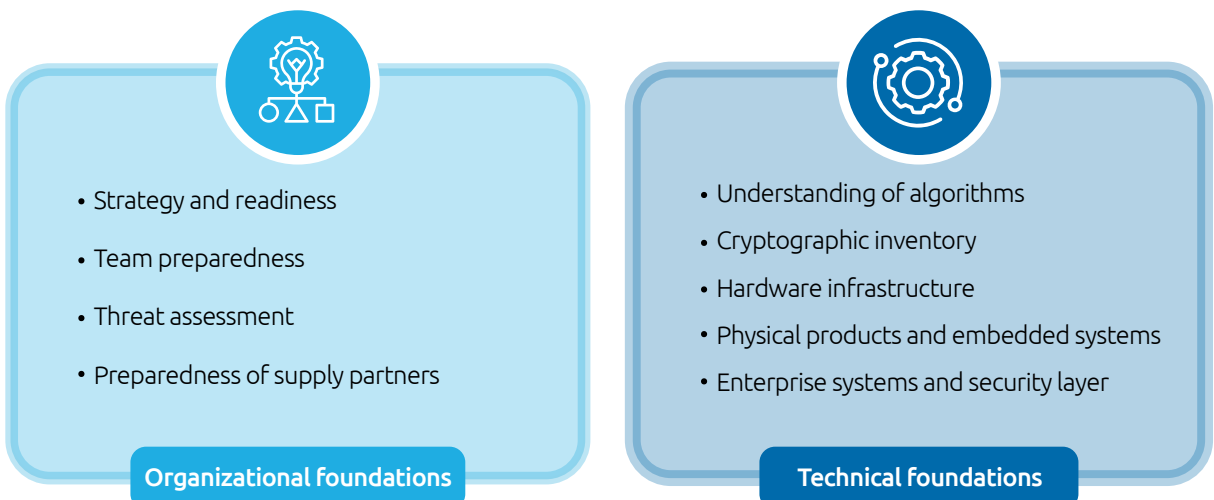
To understand where organizations are on the transition to PQC, we analyzed early adopters' progress on several critical elements.

As figure 12 shows, this analysis groups these elements into two dimensions of PQC readiness: organizational foundations and technical foundations. The organizational foundations help in enabling a smooth transition to a PQC-ready future, while technical behaviors, including infrastructure development, are the necessary tools.

15%

of early adopters are "quantum-safe champions" who lead in both organizational and technical foundations

Figure 12.
Elements needed for transition to PQC



Source: Capgemini Research Institute analysis.

DNA of the quantum-safe champions

Based on these elements of PQC readiness, we identified four different cohorts. Of these:

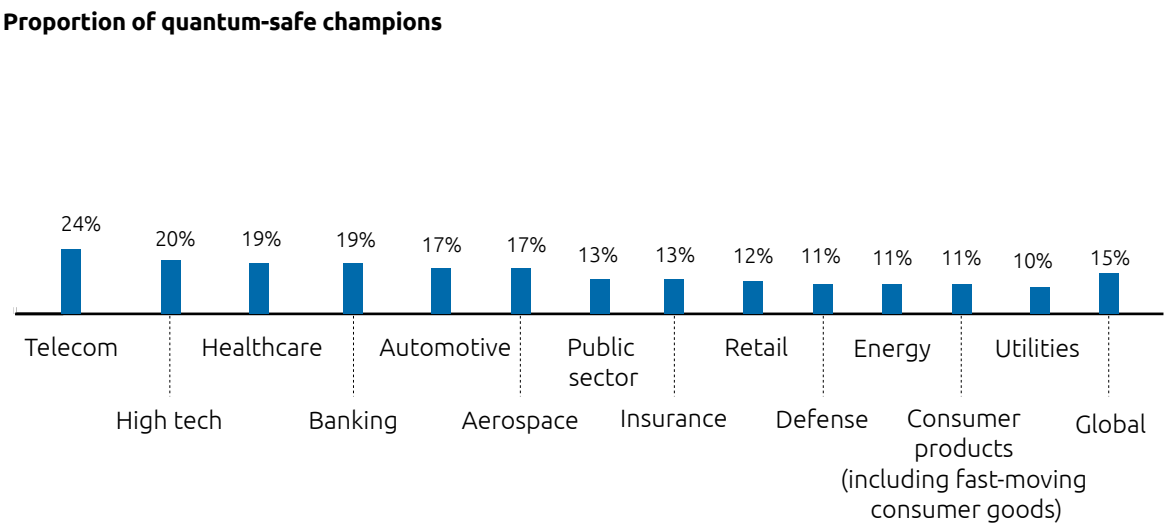
- 15% are quantum-safe champions that lead in both organizational and technical foundations
- 56% fall into the "quantum-safe beginners" category
- "Quantum-safe planners" lack the technical foundations and form 15% of the sample, while "quantum-safe explorers" lack the organizational foundations and constitute 14% of the sample.

We found that among quantum-safe champions:

- 44% believe Q-Day will be in the next five years, compared with just 17% of early adopters
- 23% have budgeted or approved near-term PQC initiatives against 10% of early adopters
- 48% have plans to start transitioning in one to two years, compared with 28% of early adopters.

Quantum-safe champions are allocating a higher percentage of their cybersecurity budget (2.74%) to quantum-safe initiatives, compared to the 2% that the early adopters are allocating. Among the different industries we surveyed, the telecom sector has the highest proportion of the quantum-safe champions, followed by the high tech industry (see figure 13).

Figure 13.
The telecom sector has the highest proportion of quantum-safe champions



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

Among the countries we surveyed, the Netherlands (29%), China (23%), and the United States (21%) top the list of countries with the highest proportion of the quantum-safe champions. Figure 14 explains the differences among each of the cohorts across the various elements of the PQC readiness.

Figure 14.
Key characteristics of quantum-safe champions vs. other cohorts

Category	Quantum-safe beginners	Quantum-safe planners	Quantum-safe explorers	Quantum-safe champions
Strategy and roadmap	No formal migration plan; PQC seen as long-term issue	Board-approved phased roadmap (functionality/sector) exists; execution is not yet underway	Algorithm-centric pilots dictate direction, but no enterprise roadmap	Enterprise-wide roadmap aligned to NIST timelines; hybrid rollout milestones tracked periodically
Policy and governance	Crypto policy outdated or absent	Policy updated to include PQC clauses; annual review cycle	Technical standards drafted for pilots; enterprise policy gaps remain	Central crypto-governance that enforces policy, audits, and breach simulations
Budgeting and planning	No budget estimation or allocation; reactive spending	Budget scoped; awaiting release of funds	PoC funds available; full-scale business case not secured	Multi-year budgets ring-fenced for migration and hybrid operations
Team capabilities	PQC knowledge limited to a few security engineers; no training	Role-based training program launched; cross-functional committee formed	R&D cryptographers active; broader organization unaware	24 × 7 "Quantum SWAT" hub, internal academy, formal vendor/partner skill pipelines
Threat impact and assessment	No structured business impact analysis or harvest-now, decrypt-later timeline analysis	Business-impact and financial-risk assessments completed for critical systems	Time-to-attack modeling is done for selected pilots only	Dynamic threat model covering all assets, refreshed with intel feeds
Supply chain engagement	Vendors not questioned on PQC; no clauses in requests for proposals (RFPs)	Vendor self-assessments collected; annual follow-ups scheduled	Joint PoCs with select hardware/security vendors	Binding service level agreements (SLAs) include crypto-agility and upgrade timelines; shared migration roadmaps

Figure 14.
Key characteristics of quantum-safe champions vs. other cohorts

Category	Quantum-safe beginners	Quantum-safe planners	Quantum-safe explorers	Quantum-safe champions
Cryptographic inventory	No systematic scans; algorithm usage largely unknown	Full inventory captured; sensitivity-based categorization pending	Granular inventory for pilot domains; enterprise coverage incomplete	Automated, continuous inventory with dependency graph, owner data, and retirement dates.
Algorithm readiness	Unaware of NIST finalists; RSA/ECC dominate	Selection framework drafted; standards awareness high, pilots pending	PoC code in dev/QA for Kyber & SPHINCS+; hybrid schemes explored	Standardized PQC suite live in production; hybrid encryption default, fallback paths validated
Hardware infrastructure readiness	HSMs, routers untested; no upgrade plan	Compatibility studies underway; budget secured	PQC-capable HSMs and switches in lab pilots; performance baselines captured	Production infra PQC-ready, crypto-agile, latency and throughput tuned to SLA targets
Embedded and physical product readiness	Long-life products ignored; no R&D focus	Preliminary impact analysis for flagship products; design guidelines drafted	PQC libraries ported to constrained devices; performance challenges unresolved	PQC boot-chains and secure updates integrated; design rulebooks mandate quantum-safe crypto
Software, network, and storage system readiness	Legacy software unscanned; systems noncompliant	Code-scanning tools procured; priority systems scheduled for remediation	PQC prototypes in pilot network segments; cloud key-rotation tests running	CI/CD enforces PQC compliance gates; storage encryption and auth stacks crypto-agile and scalable
Metrics	No KPIs tracked; success = “no breach”	Initial KPIs (% inventoried, % staff trained) tracked quarterly	Technical KPIs (latency, key-size impact) tracked; org KPIs absent	Balanced PQC scorecard (org + tech) reviewed by exec committee; external audits certify posture

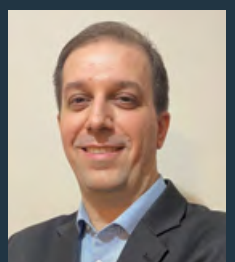
Source: Capgemini Research Institute analysis.

The case for crypto-agility

To prepare for the post-quantum era, organizations must prioritize crypto-agility – the ability to swiftly switch between cryptographic algorithms without disrupting operations. Luciano from Bradesco adds, *"Crypto-agility is a core objective for us. We're designing systems that can adapt to evolving algorithms, especially since NIST may approve more algorithms in the coming years."* This agility ensures resilience against sudden cryptographic failures and supports seamless migration to NIST-approved PQC standards.

Developing crypto-agility involves establishing clear policies, inventorying cryptographic assets, and automating key and certificate management. On March 5, 2025, NIST released the draft cybersecurity white paper (CSWP) "Considerations for Achieving Crypto Agility: Strategies and Practices." This discusses challenges, trade-offs, and approaches to providing operational mechanisms for achieving crypto-agility while maintaining interoperability. [47]

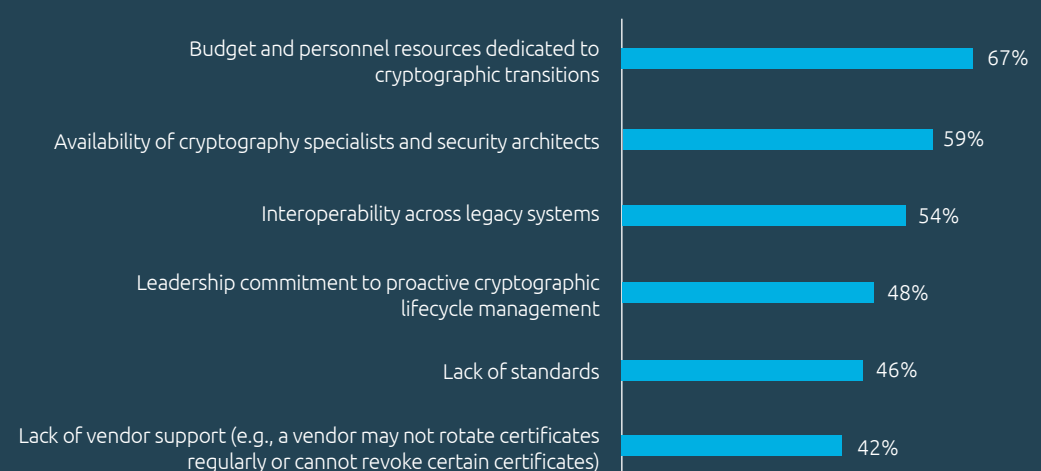
- Just 40% of organizations can respond effectively to the discovery of a critical vulnerability in a widely used cryptographic library (e.g., OpenSSL), while 36% say they can respond to the emergence of credible evidence that quantum computers can break current public-key algorithms.
- Only 35% of executives say their organizations maintain a centralized inventory of all cryptographic keys, algorithms, and certificates in use, and 23% agree that their IT infrastructure is designed to support quick updates or replacements of cryptographic algorithms, when needed.



"Crypto-agility is a core objective for us. We're designing systems that can adapt to evolving algorithms, especially since NIST may approve more algorithms in the coming years."

Luciano Carolino
IT security specialist at Bradesco bank

Figure 15.
"Budget and personnel resources dedicated to cryptographic transitions" is a challenge to organizations in achieving crypto-agility



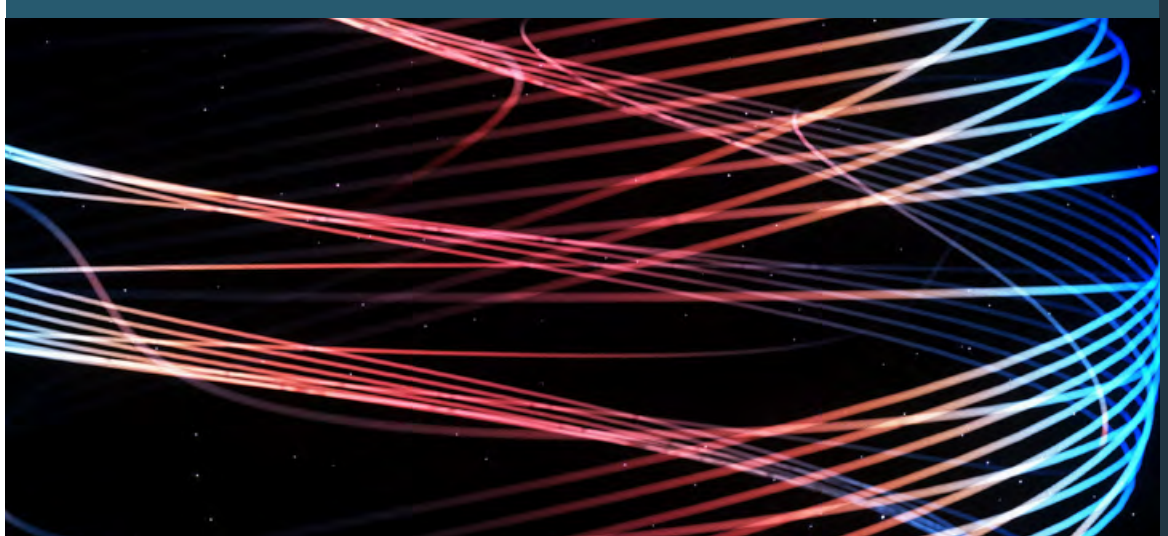
Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 703 early adopters.

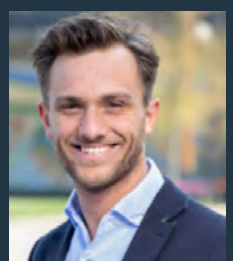
Top challenges to achieving crypto-agility include:

- Some 67% of organizations struggle with allocating sufficient budget and personnel to cryptographic transition. Early quantum readiness steps – like assessments and planning – require minimal investment and no major infrastructure changes. If quantum is truly seen as a threat, budget shouldn't be the excuse. Start now; delay only increases risk and reduces preparedness.
- Another 59% lack the necessary expertise, and face delays in assessing, planning, and executing agile cryptographic strategies.
- Over half (54%) of organizations operate on legacy infrastructure that lacks compatibility with modern cryptographic standards. This creates friction in adopting agile frameworks and increases the complexity of system-wide upgrades.

Highlighting their work on a quantum-secured crypto-agile network, Lori Beer, global Chief Information Officer at JPMorgan Chase said, *"We are investing in quantum security to help ensure our readiness as quantum technologies are maturing. We are preparing a dual remediation strategy that incorporates both post-quantum cryptography and QKD."* [48]

Julian van Velzen, CTIO and head of Capgemini's Quantum Lab, concludes, *"Organizations must be able to adapt, swap, and scale cryptographic algorithms without rewriting their infrastructure. It's the only way to stay resilient against future threats, including quantum, and to ensure long-term digital trust and compliance."*





"Organizations must be able to adapt, swap, and scale cryptographic algorithms without rewriting their infrastructure. It's the only way to stay resilient against future threats, including quantum, and to ensure long-term digital trust and compliance."

Julian van Velzen
CTIO and head of Capgemini's Quantum Lab

67%

of organizations struggle with allocating sufficient budget and personnel to cryptographic transition.

54%

of organizations operate on legacy infrastructure that lacks compatibility with modern cryptographic standards.

"If quantum cryptography is embedded in quality assurance for new programs, we'll be ready for the unknown. That's the best strategy – to be prepared before the change is forced upon us"

Adriano Luiz de Oliveira
Head of cybersecurity, CNP Seguradora, a subsidiary of the CNP Assurances group

Three in 10 organizations are ignoring the quantum threat – and risk falling behind

Despite the implications of advances in quantum computing, three in 10 organizations remain hesitant to adopt quantum-safe solutions. They view quantum threats as distant and prefer to wait for standardized protocols. Budget constraints and the perception of quantum computing as solely a research topic further delay adoption. Despite expected impacts, planning continues at a slow pace.[49] Among the organizations that are currently not working on or not planning to use quantum-safe solutions in the next five years:

- 65% do not see quantum computing as an immediate threat
- 67% prefer to wait for widely accepted standards (e.g., waiting for global adoption of current NIST PQC standards)
- 68% do not currently have the budget to investigate or adopt PQC solutions
- 70%+ say "escalating cybersecurity threats" and "regulatory mandates" will increase urgency to adopt PQC.

However, escalating threats and regulatory pressures may soon shift this cautious stance.

Organization should understand that the PQC shift is monumental and takes time. Starting later means finishing too late. A three-to-five-year year delay could leave your systems exposed and irreparable. Begin now – quantum safety demands urgency, not complacency.

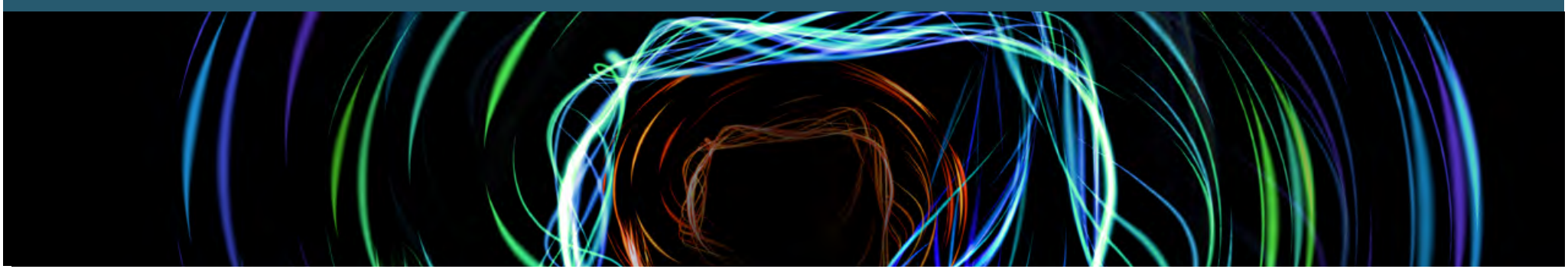


Figure 16.
Organizations want cost-benefit analysis information to understand PQC's importance

Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 297 organizations.

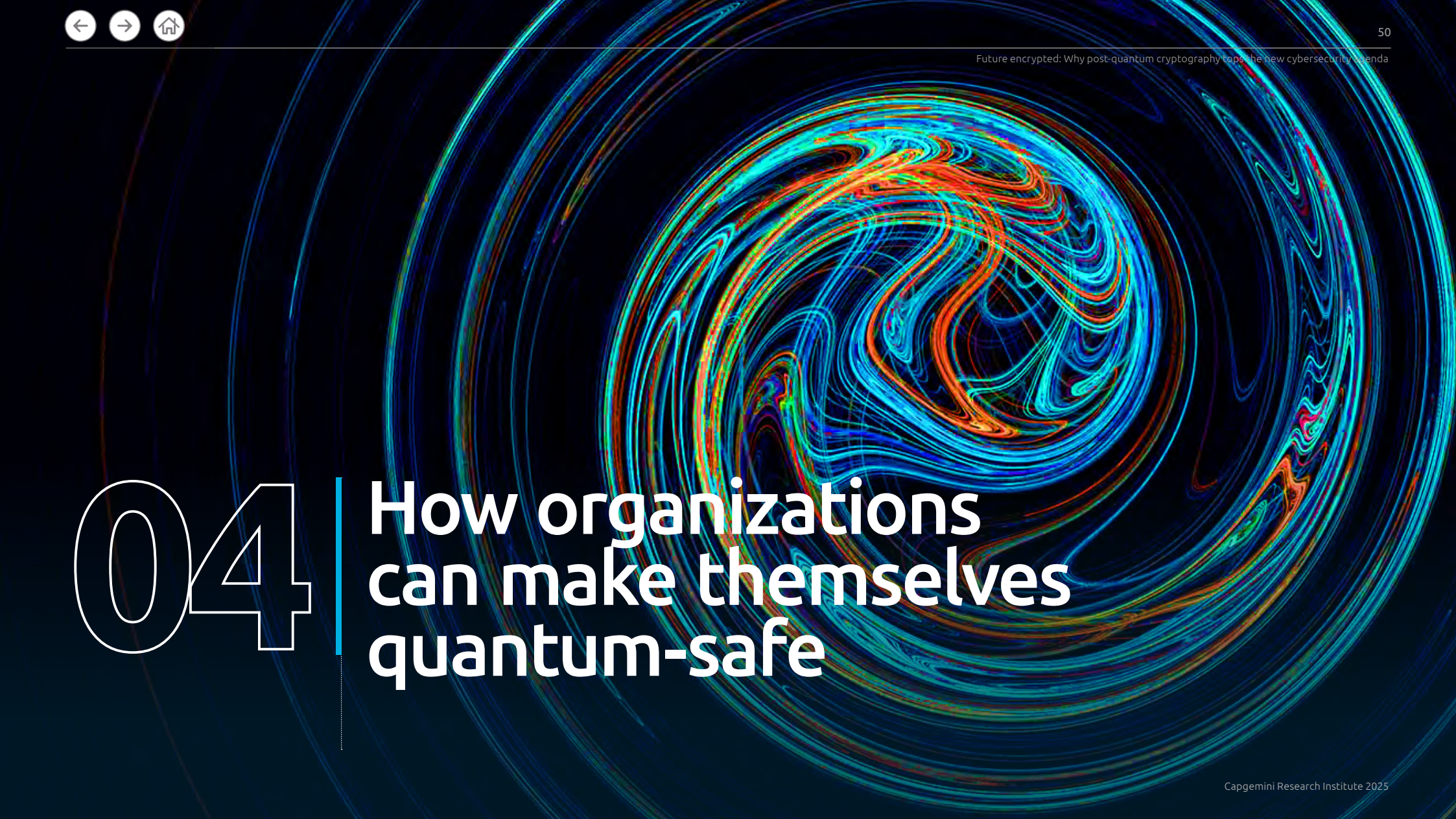
More than half of these organizations say having a cost-benefit analysis, and availability of "technical documentations" and "migration handbooks" would help their organization to understand the importance of PQC (see figure 16).

Many businesses remain unaware or dismissive. Is there an upside here? Even if some enterprises think, there is still time to act; know that the window is narrowing very fast. As quantum computing moves from lab to reality, those who act now will lead tomorrow. The quantum clock is ticking. Global organizations must act now – collaborate, educate, and migrate to post-quantum cryptography. Tech giants, governments, and infrastructure providers must unite to establish post-quantum cryptographic standards, create secure migration pathways, and educate leadership on the stakes involved.

Marjorie Bordes, Group CISO at Capgemini, adds, "If your organization hasn't begun planning for quantum safety, you're already behind. Migration to PQC is complex, cross-functional and time-consuming. Delaying action not only increases risk exposure, but also limits your ability to comply, com-pete and protect sensitive data in the years ahead."

"If your organization hasn't begun planning for quantum safety, you're already behind. Migration to PQC is complex, cross-functional and time-consuming. Delaying action not only increases risk exposure, but also limits your ability to comply, compete and protect sensitive data in the years ahead."

Marjorie Bordes
Group CISO at Capgemini



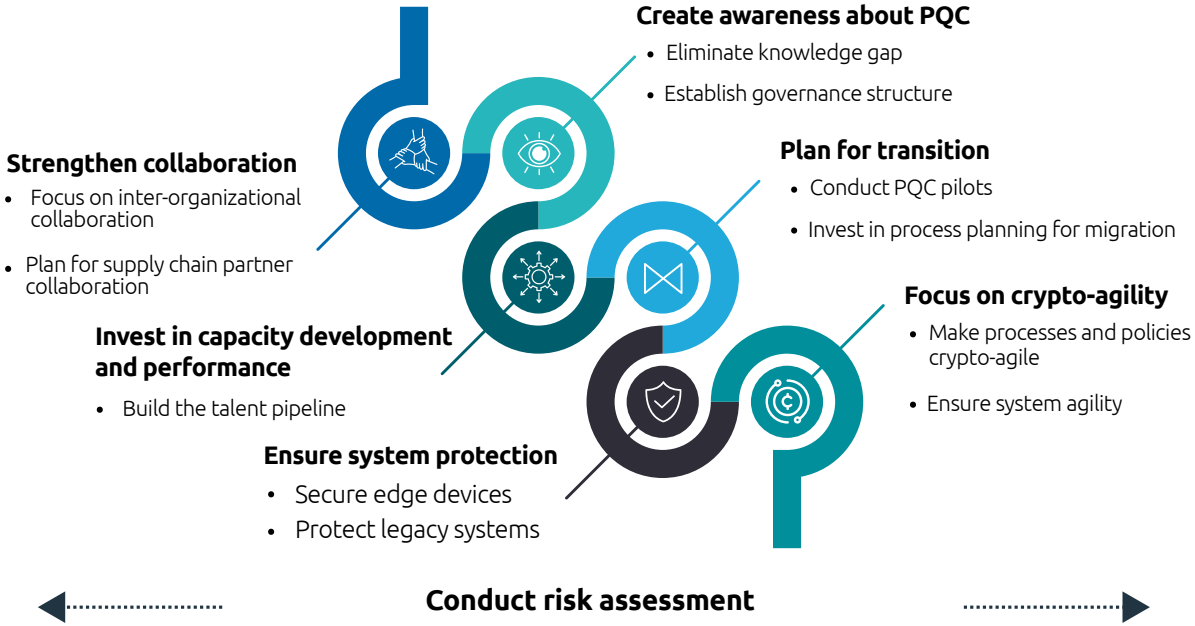
04 How organizations can make themselves quantum-safe

As Q-Day nears, organizations can no longer delay their transitions to a quantum-safe future. Based on our survey, interviews, and experience, we propose the recommendations below for organizations to become quantum-safe.

> **"To supply the substantial computational power required to support quantum-resistant algorithms, industries must invest in next generation hardware and collaborate on developing efficient, scalable encryption methods that can withstand quantum threats, ensuring long-term security without sacrificing performance."[81]**

Kalyan Gottipati
Principal Solution Architect at Citizens Financial Group.

Figure 17.
Key considerations for organizations to be quantum-safe



Source: Capgemini Research Institute analysis.

Conduct quantum risk assessment

A quantum risk assessment is the first critical step in understanding how exposed your organization is to future quantum threats. Especially in sectors like banking, insurance, and utilities, it helps identify where vulnerable cryptographic assets reside – whether in encryption keys, hardware, or certificates. This process not only reveals the scope of potential vulnerabilities but also informs the cost and complexity of transitioning to quantum-safe systems. It's a vital part of the learning curve that enables CISOs to prioritize and plan effectively. Bernd Meurer, Field CTO at BT Group adds, *"Many of our customers have done a high-level assessment of systems and communication interfaces, but a full impact analysis for post-quantum readiness is still in draft in many cases."*

Understand risk assessment methods: Currently, there are two published quantum cryptanalytic risk assessments (QCRAs) with different types of use cases. "A methodology for quantum risk assessment" by the Global Risk Institute sets a timeline for quantum technology development, identifies vulnerable assets, and forecasts when quantum threats might materialize. Meanwhile, the Crypto Agility Risk Assessment Framework (CARAF) assesses how quickly and effectively an organization can transition to new cryptographic solutions in response to emerging threats.[50]

Utilize risk-assessment tools: Several solution providers offer risk-assessment tools to help organizations in developing a robust quantum-safe strategy. These assess quantum computing threats, identify cryptographic weaknesses, prioritize critical assets, provide risk-assessment reporting, conduct attack simulations, and develop a quantum-safe migration plan.

Update cryptographic inventory

A cryptographic inventory is essential for organizations to identify where cryptography is used across software, communications, and hardware devices.

By cataloging cryptographic assets, security teams can pinpoint and replace outdated or weak algorithms, mitigating risks of quantum attacks.[51] *"It's better to start with a high-level inventory and then go deeper. We need to prioritize actions to protect critical systems,"* says the Group Chief Information Security Officer at a telecom company based in the Americas. Organizations can utilize the following approach while evaluating cryptographic inventory for PQC:

Identify cryptographic assets: Identify all systems (both internal and client-facing), applications, gateways, and supporting security components that require cryptographic transition. These include PKI, web servers, authorization frameworks, authentication directories, and protected domain name systems (DNS). Pay special attention to custom systems and software from smaller vendors, as these may have unique cryptographic requirements.[52]

Assessment and evaluation of cryptographic assets: After identifying all assets, it's essential to evaluate their strengths, relevance, and adherence to current security standards.[53]

Documentation and monitoring: Maintain detailed records of all cryptographic assets, including their usage, expiry dates, and any changes made. Continuously monitor and update the inventory to ensure all assets remain secure and compliant with evolving security standards.[54]

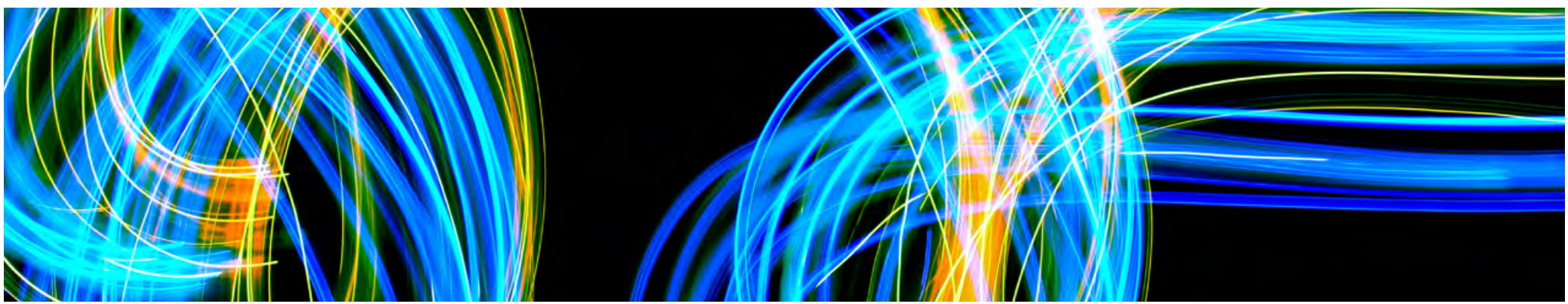
Identify dependencies between cryptographic assets: Identify dependencies between cryptographic assets and decide the migration order based on these dependencies. Retain interoperability until all related assets are migrated. This approach minimizes disruption.[55]

Prioritize based on sensitivity

This approach involves evaluating and prioritizing systems and sensitive data based on their importance and vulnerability to quantum threats. Migrating to PQC is resource-intensive. By prioritizing sensitive assets, organizations can allocate their resources more effectively. Key considerations for sensitivity-based prioritization are:

1. **Data discovery and classification:** Categorize data based on its sensitivity and criticality. For quantum-readiness, organizations should:
   - Establish criteria for different levels of data sensitivity and develop classification standards and policies
   - Use automated tools along with manual reviews, to identify sensitive data across databases, file systems, cloud storage, and endpoints
   - Continuously tag and label data based on sensitivity, maintaining records of classifications and data owners
   - Continuously monitor data sensitivity and cryptographic implementations, scheduling regular audits to ensure accuracy and completeness.[56]
2. **Assess sensitivity and lifespan:** Harvest-now, decrypt-later exploits the gap between data longevity and cryptographic strength. If data lifespan plus migration time exceeds quantum arrival, per Mosca's theorem, compromise becomes inevitable. Assess the sensitivity and lifespan of your organization's information to identify data that may be at risk. This ongoing risk-assessment process will help prioritize elements of transition.[57]

Organizations handling data with long confidentiality spans and those providing critical infrastructure face the most immediate threat.[58] One-time passwords (OTPs), session tokens, real-time sensor data, or temporary chat messages and such like only have ephemeral value. While short-lived data is less exposed to the "harvest-now, decrypt-later" threat, organizations must still ensure that: it's encrypted in transit, not inadvertently logged or stored, and handled with appropriate access controls. By following these steps, organizations can effectively prioritize where PQC migration happens first, ensuring that the most sensitive and critical data is protected.



"Many of our customers have done a high-level assessment of systems and communication interfaces, but a full impact analysis for post-quantum readiness is still in draft in many cases."

Bernd Meurer
Field CTO at BT Group

Create PQC awareness

Dr. Morgan Stern from the NSA Cybersecurity Directorate emphasizes the importance of urgency in PQC transition: *"Hardware has a 10-year lifespan, so action is required now to ensure future interoperability and security."*[59]

Greater dissemination of knowledge could drive urgency in establishing governance structures for the transition to quantum-safe infrastructure.[60] Adding to this, *"Start experimenting with PQC, even if standards and protocols aren't finalized. Understand where performance issues may arise and how they impact your systems,"* says Temi Adebambo, GM and CISO, Microsoft Gaming.

Eliminate knowledge gap

- Provide comprehensive education and training on quantum threats and future technologies
- Increase awareness about quantum threats and the importance of PQC transition by engaging cross-functional teams, including business, IT, legal, risk, compliance and security, in collaborative workshops. Emphasize PQC as a strategic business imperative, not solely a CISO concern. Organizations must recognize PQC as a cross-functional concern that impacts compliance, customer trust, intellectual property, and long-term cyber resilience.
- Bring in skilled resources and experts to work on addressing the challenges associated with quantum-safe infrastructure.
- Learning the state of related regulations: awareness of existing and emerging regulations around PQC and quantum safety is essential. Track updates from NIST, ETSI, or your local security and compliance bodies, etc. Collaborate or participate in industry forums or working groups (e.g., ETSI QSC, IETF PQC).

Establish governance structure

- Establish governance structures with clearly defined roles and responsibilities to oversee the transition to quantum-safe infrastructure.
- Implement governance structures that enhance compliance with industry standards and the latest security practices.
- Mitigate risks associated with outdated or vulnerable algorithms by systematically evaluating and updating cryptographic practices.
- Build resiliency into your framework by continuously assessing and improving cryptographic methods to stay ahead of evolving quantum threats.[61]

"Start experimenting with PQC, even if standards and protocols aren't finalized. Understand where performance issues may arise and how they impact your systems"

Temi Adebambo
GM and CISO, Microsoft Gaming

Plan for transition

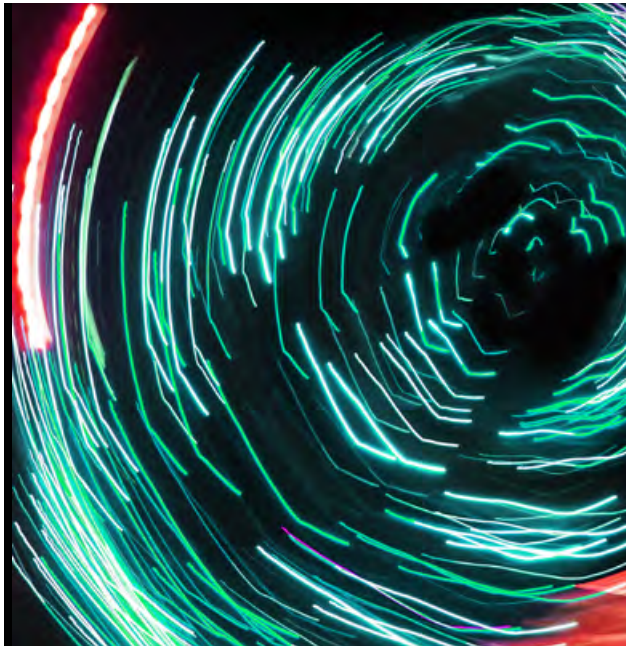
Use hybrid cryptography

Hybrid cryptography is a security strategy that combines public key cryptographic (PKC) algorithms with PQC algorithms to ensure resilience against both classical and quantum threats. Most PKC (public key cryptography) algorithms in use today are expected to be vulnerable to cryptographically relevant quantum computers (CRQC)s). As a part of this hybrid approach, it is also recommended to explore currently emerging tools such as hash-based signature schemes (XMSS, Leighton-Micali (LMS), SPHINCS, and BPQS) which are showing improved performance characteristics.

Hybrid cryptography offers three major advantages:

Enhanced security: Hybrid cryptography provides a robust security framework that protects against both current and future threats. This ensures that, even if post-quantum algorithms are not yet fully reliable, classical algorithms can still offer strong protection.

Gradual implementation: Hybrid cryptographic systems allow organizations gradually to implement quantum-resistant methods as migrating to PQC "might" impact TLS, email, PKI, X.509, code signing, and S/MIME. Gradual adoption reduces disruption, builds resilience, and positions your organization ahead in post-quantum security readiness. This seamless transition helps maintain security and operational continuity while adapting to new cryptographic standards.



Backward compatibility: Hybrid models ensure that older systems and protocols remain compatible with new quantum-resistant algorithms. This is crucial for maintaining the integrity and functionality of legacy systems while upgrading to more secure cryptographic methods.

Google developed a quantum-resilient FIDO2 security key, which enhances digital authentication by combining traditional public-key cryptography with NIST's approved post-quantum algorithm called Dilithium. This hybrid approach aims to future-proof security keys against quantum computing threats while maintaining compatibility with current systems.[62]

Conduct PQC pilots

PQC pilots ensure a smooth transition to quantum-safe infrastructure. These pilots help organizations assess the effectiveness and practicality of PQC solutions before full-scale deployment. Below are the key steps to follow:

- Conduct controlled trials to ensure performance, security, and compatibility concerns are adequately addressed. They should work closely with vendors, conduct internal assessments, and refine migration strategies based on real-world results.[63]

- Beginning with pilot projects that implement PQC in noncritical systems can help organizations to understand the practical implications and challenges. Gradually extending the implementation to critical systems once initial hurdles are overcome allows for a smoother transition.[64]
- Conduct testing, including penetration testing and cryptanalysis to validate security.[65]

Authority-sponsored pilot initiatives:

- Funded by the EU, a team of 12 distinct but highly experienced organizations formed the PQ-REACT consortium to address the challenges of PQC. One of the pilots focuses on applying quantum-resistant cryptography to smart grid deployments. It aims to secure firmware updates for deployed meters, ensuring they are protected against quantum threats.[66]

- Q-PrEP, funded by the European Commission, supports the shift to post-quantum cryptography (PQC) in public administrations. It raises awareness of quantum threats, builds a cross-sector PQC network, fosters collaboration, aligns understanding of quantum risks, and delivers a unified roadmap for quantum-safe IT across the European public sector. Capgemini Engineering also plays a key role in this pilot.[67]

Private pilot initiatives: Sectigo, in collaboration with Crypto4A, has launched Sectigo PQC Labs, a PQC sandbox backed by an HSM that meets NIST's full PQC standards. The platform enables organizations to test, validate, and transition to quantum-resistant cryptography in a secure environment.[68]

Timothy Bates, former Lenovo CTO and Cybersecurity Professor of Practice at the University of Michigan, emphasizes the significance of pilots: *"It's better to face small, controlled failures now than catastrophic breaches later. Push for investments in quantum technologies and talent pipelines. These will be the linchpins of your organization's survival in a post-quantum world."*[69]

As enterprises begin exploring post-quantum cryptography (PQC) rollouts or proofs of concept (PoCs), a growing ecosystem of tools is making implementation more accessible and practical:

Open Quantum Safe (OQS): A leading open-source project, OQS provides the liboqs C library, which integrates quantum-safe algorithms into existing protocols. It supports NIST finalist algorithms and is designed for experimentation and integration.

Hybrid TLS stacks: Projects like BoringSSL + liboqs and OpenSSL + liboqs enable hybrid key exchanges – combining classical and quantum-safe algorithms – allowing gradual migration without sacrificing current security.

These tools support secure messaging to VPNs and cloud services. Adrian Neal, Global lead for PQC at Capgemini, adds, *"PQC pilots aren't just technical tests– they're strategic exercises in inventory, discovery, interoperability, and cross-team coordination. Success depends on more than algorithm selection; it requires aligning cryptographic upgrades with real-world systems, policies, and partners. Piloting early helps organizations build the muscle memory needed for enterprise-wide quantum readiness."*

"It's better to face small, controlled failures now than catastrophic breaches later. Push for investments in quantum technologies and talent pipelines. These will be the linchpins of your organization's survival in a post-quantum world."[69]

Timothy Bates
Former Lenovo CTO and Cybersecurity Professor of Practice at the University of Michigan

“PQC pilots aren’t just technical tests– they’re strategic exercises in inventory, discovery, interoperability, and cross-team coordination. Success depends on more than algorithm selection; it requires aligning cryptographic upgrades with real-world systems, policies, and partners. Piloting early helps organizations build the muscle memory needed for enterprise-wide quantum readiness.”

Adrian Neal
Global lead for PQC at Capgemini

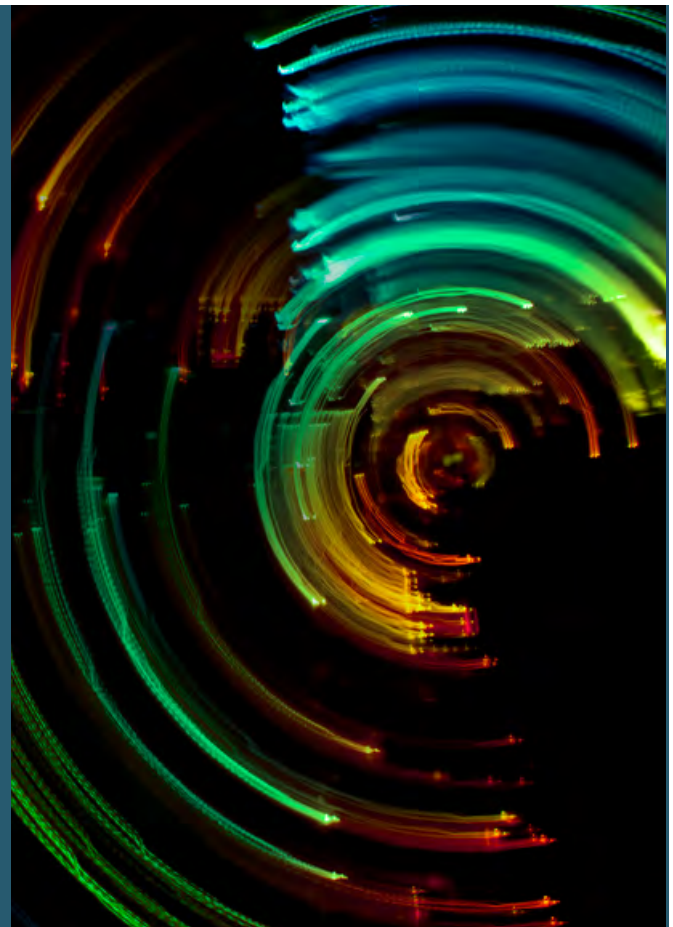
Capgemini and Standard Chartered – Quantum preparedness pilot

Introduction: Capgemini and Standard Chartered partnered to explore the integration of post-quantum cryptography (PQC) into financial systems through a focused proof-of-concept (POC).

Background: The POC aimed to evaluate the performance of NIST-standardized PQC algorithms – ML-DSA, SLH-DSA, and Falcon – against RSA within Standard Chartered's payment APIs. A custom JWT (JSON Web Token) library was developed to generate and verify tokens using these algorithms. Benchmarks were conducted in both Capgemini's test environments and Standard Chartered's production-grade infrastructure.

Findings: ML-DSA emerged as the top performer, significantly outperforming RSA in both signature and verification throughput. Falcon also showed strong results, particularly in parsing operations due to its smaller signature size. SLH-DSA lagged in performance and is recommended only as a fallback. The study revealed that while PQC algorithms increase token size, their verification efficiency can offset parsing delays. However, performance dropped when public keys were loaded from disk rather than memory, highlighting the need for architectural optimizations. The POC also emphasized that PQC integration is not plug-and-play – it requires infrastructure readiness, hybrid cryptographic strategies, and ongoing performance tuning.

Conclusion: This POC marks a foundational step in Standard Chartered's quantum-safe journey. It validates the feasibility of PQC in real-world financial applications and underscores the importance of early adoption. Capgemini's Quantum Lab Agility Factory will continue to support this transition, ensuring cryptographic agility and resilience in the face of emerging quantum threats.



Invest in process planning for migration

Effective migration requires meticulous planning and execution. To ensure a smooth transition, we recommend the following points:

- Appoint a migration manager with thorough organizational understanding and access to all departments to guide the migration process.
- Allocate sufficient budget to ensure adequate resources for migration.
- Manage downtime by planning for moments when services and parts of the organization need to be isolated and shut down, minimizing impact on continuity.
- Decide whether each cryptographic asset should be replaced, redesigned, or retired based on its importance, risk, and available resources.
- Isolate data/systems to protect against store-now-decrypt-later attacks and during migration when traditional protection isn't feasible. Consider the impact on functionality and availability.[70]

Focus on crypto-agility

Crypto-agility describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures, to achieve resiliency without interrupting the flow of a running system. Gregory Webb of AppViewX states: *"A big challenge will be upgrading systems to the new NIST standard PQC encryption algorithms, which requires careful planning and coordination. This can be addressed by implementing crypto-agility, so systems can quickly switch between algorithms, and developing transition plans that prioritize critical systems to ensure security and compliance."*[71]

Elements of crypto-agile systems: Use of modern cryptography and maintaining accurate crypto-inventory are two integral pillars to crypto-agile systems. The third pillar is engineering in the ability to make encryption changes quickly and efficiently.[72] Christian Schmitz, Managing Director, evolutionQ, adds, *"Clients are influenced by compliance regulations and the maturity of different quantum safe technologies. We recommend integrating different quantum safe technologies into one solution for better resilience and crypto agility."* The Key Management Handbook[73] from ISPG advises (an example for a crypto-agile system) as below:

- Rotate encryption keys annually, including TLS certificates and database encryption keys.
- Maintain a documented process for key rotation, whether manual or automated.
- Aim to complete key and certificate rotations in minutes to minimize response time in case of key compromise.
- Design software to allow library updates without changing the code, assuming backward compatibility.
- Provide key lengths via configuration files, rather than hard-coding them.

Making crypto-agile processes and policies: Organizational policies should mandate technical and procedural measures for cryptographic agility, especially for new systems. Consider multiple algorithms or parameter sets to facilitate migration to new cryptographic standards.

Include cryptographic agility in procurement processes for new software and hardware components and ensure components can be updated appropriately. Prefer hardware that supports different algorithms or is easily updatable. As a part of change management, identify responsible parties for cryptography changes and ensure synchronized updates across the organization.[74]

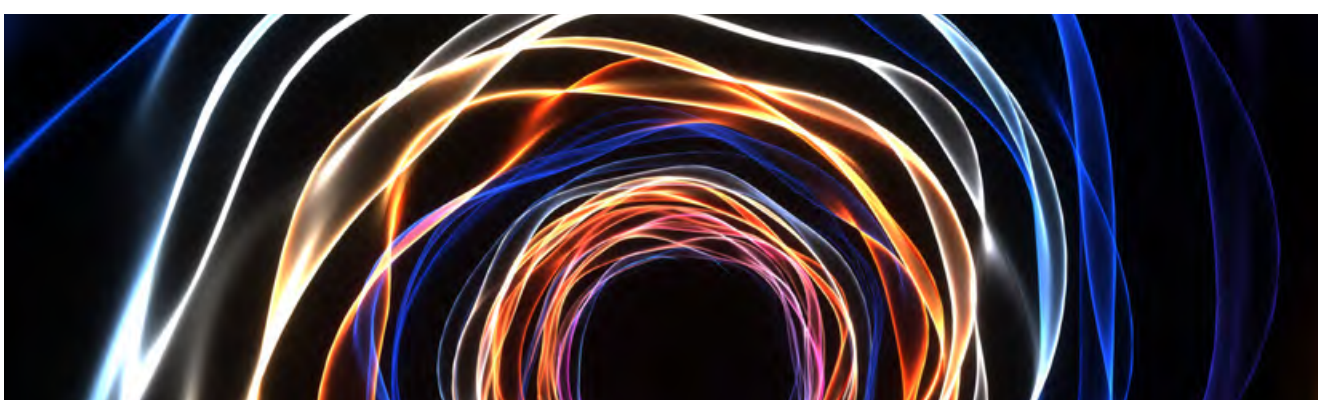
Forms of crypto-agility: Forms of crypto-agility that are relevant to most organizations are migration agility, compliance agility, implementation agility, and platform agility. Organizations should consider these in formulating their crypto-agility strategies.

Ensure system agility: Here, "system agility" refers to the ability of an organization's systems to quickly and efficiently adapt to changes, particularly in the context of evolving

technologies, and system and security requirements. Organizations should aim to achieve system agility through the following steps:

- **Design systems for flexibility:** Facilitate the adoption of cryptographic algorithms with minimal changes by designing systems that are adaptable and modular.
- **Upgrade technological infrastructure:** Ensure that your infrastructure supports new cryptographic standards, providing quantum-safe encryption for customer data, both in transit and at rest.
- **Collaborate with vendors and third parties:** Work closely with software vendors, service providers, and third parties to ensure their products and services support your transition through updated and compatible solutions.[75]

Crypto-agility must become an organizational reflex – embedded across all business functions, not just security teams. Unlike legacy cryptography that endured decades, agility demands continuous feedback and cultural integration to adapt swiftly to evolving threats and cryptographic advancements.



Ensure system protection

Secure edge devices

Connected sensors, routers, and gateways offer potential entry points for hackers. It is imperative to protect edge devices with elements that are optimized to run quantum-resistant algorithms and can withstand a quantum computer attack.[76]

Use embedded secure element: Secure element (SE) is a chip that is protected by design from unauthorized access and used to run a limited set of applications, as well as store confidential and cryptographic data.[77]

Embedded SE integrates hardware functions into a single design and provides a solution to ease the transition of the internet of things (IoT) to PQC. This is critical to ensure the security of interconnected systems in the IoT frame and is designed to withstand attacks and protect sensitive data. SE encompasses several cryptography functions, such as PQC encapsulation and decapsulation, key derivation, key storage, and key generation. SE enhances the speed and security of critical cryptographic primitives.[78] Secure-IC, a cybersecurity solution provider, has integrated PQC solutions into an integrated secure element that provides security features to address all the leading threats against embedded systems.[79]

Solution providers offer integration of PQC with edge devices such as sensors, routers, network devices, smart cards, etc., and is the key to protection against quantum threat.

Protect legacy systems

As quantum computing continues to advance, securing legacy systems against quantum threats becomes increasingly important. Here are some strategies to protect these systems:

Other alternative approaches: When more resource-intensive algorithms are used, legacy systems might not support the necessary hardware acceleration to maintain performance. In cases where direct upgrades are not feasible, organizations may need to consider alternative approaches, such as:

- Deploying middleware that can interface between legacy systems and newer standards.
- Isolating and segmenting critical legacy systems that cannot be upgraded, while using quantum-safe encryption in other parts to mitigate overall risk.
- Planning a phased migration to newer systems or platforms.[80] For instance, gradually retire IoT devices that do not support PQC or other security measures to strengthen the long-term enterprise cyber resilience.

Invest in capacity development and performance

Migrating to PQC will necessitate upgrading existing systems to meet new cryptographic standards. *"To supply the substantial computational power required to support quantum-resistant algorithms, industries must invest in next-generation hardware and collaborate on developing efficient, scalable encryption methods that can withstand quantum threats, ensuring long-term security without sacrificing performance,"* states Kalyan Gottipati, Principal Solution Architect at Citizens Financial Group.[81]

Capacity development is broadly required in three major areas:

Computational capacity: Quantum-safe cryptographic standards offer robust security against quantum threats, but they come with trade-offs in performance, making it essential to quantify these impacts now to guide efficient, scalable, and secure quantum-safe implementations. Here are some key considerations:

- **Increased computational resources:** These new standards require more computational resources compared with traditional algorithms such as RSA, leading to reduced performance.
- **High-performance environments:** The performance impact is particularly significant in environments where rapid encryption, decryption, and signing processes are essential, such as in real-time financial transactions or high-frequency trading systems.
- **Hardware acceleration:** To mitigate the performance impact, specialized hardware, such as field-programmable gate arrays (FPGAs) or dedicated cryptographic processors, can offload the computational burden while maintaining performance levels.

However, this introduces additional complexity, especially in virtualized environments where such hardware is not typically available or easily integrated.[82]

Bandwidth capacity: Compared with legacy public-key cryptosystems, PQC algorithms can take more time to encrypt and decrypt messages. The larger key sizes of PQC algorithms occupy more storage space, memory, and network bandwidth. Organizations must evaluate and upgrade current network infrastructure as required.[83]

Apart from this, efficient data transmission is an important goal. Cisco and its subsidiary Outshift are working on developing quantum encryption and scalable quantum networks to ensure secure and efficient data transmission.

This collaboration focuses on building advanced quantum switches and networking protocols to enable efficient interconnectivity between quantum computers, which is crucial to scaling quantum computing and enhancing security.[84]

Storage capacity: PQC algorithms come with significantly larger key sizes compared with traditional cryptographic algorithms. Consequently, PQC certificates will require more storage space. During the transition phase, it is essential to maintain both hybrid and traditional cryptographic systems, which will further increase storage requirements. Therefore, it is crucial to evaluate your existing storage solutions and plan for expansions to accommodate the increased data volume. Additionally, ensure that your data backup and recovery systems can accommodate the larger volumes efficiently to avoid any data loss or recovery issues.[85]

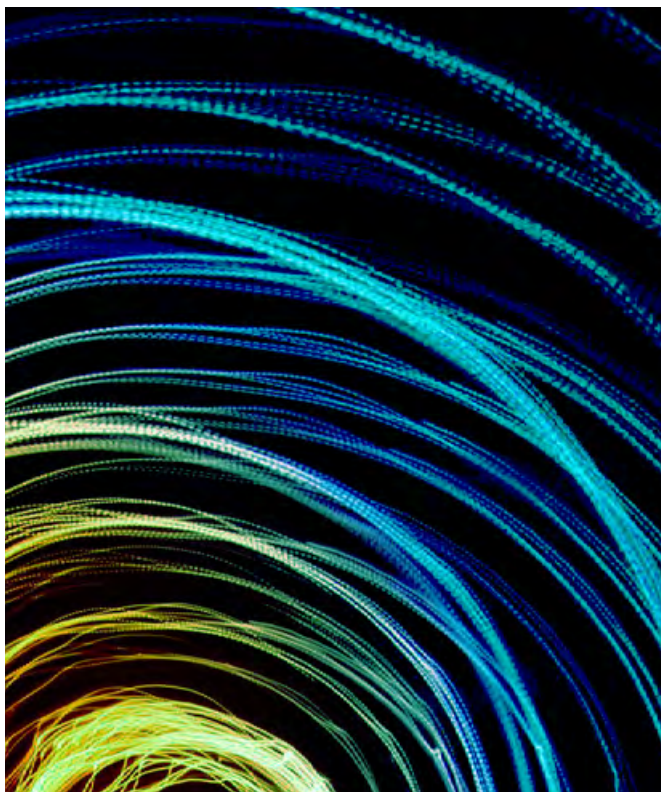
"Clients are influenced by compliance regulations and the maturity of different quantum safe technologies. We recommend integrating different quantum safe technologies into one solution for better resilience and crypto-agility."

Christian Schmitz
Managing Director, evolutionQ GmbH

Build the talent pipeline

Create a strong talent pipeline for PQC and ensure quantum safety. Here organizations should adopt a multi-pronged strategy:

- **Upskill the existing workforce:** Launch internal training initiatives to reskill cybersecurity and engineering teams in PQC fundamentals and implementation strategies. Develop specialized programs focused on quantum security, including lattice-based and code-based cryptography, and NIST PQC standards. Offer certifications and hands-on labs to deepen expertise.
- **Attract and retain diverse talent:** Recruit from interdisciplinary fields – mathematics, computer science, quantum physics – and create clear career paths to retain top talent in a competitive market.
- **Collaborate with academia:** Partner with universities to co-develop PQC curricula, sponsor research, and offer internships to nurture early-stage talent.
- **Foster cross-disciplinary collaboration:** Encourage collaboration between internal teams and external experts to bridge knowledge gaps and drive innovation in quantum security.



Strengthen collaboration

Focus on inter-organizational collaboration

To navigate the challenges posed by quantum computing, it is crucial to engage in various forms of inter-organizational collaborations for interoperability and regulations, technical facilities, and standardization.

Collaboration for interoperability and regulations: Join global efforts to ensure smooth transitions without disrupting operations (i.e., to promote interoperability). The Post-Quantum Cryptography Coalition includes over 125 participating cyber researchers from industry and academia, working together to compare and define PQC standards. They created a reference for international PQC requirements and are identifying alignment and misalignment areas, which could pose challenges for international vendor compliance and interoperability.[86]

Technical collaborations: Engage in or follow collaborative efforts in the technical aspects of PQC migration. The PQC Alliance (PQCA) addresses cryptographic security challenges posed by quantum computing by producing high-assurance software implementations of standardized algorithms. PQCA supports the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping. Notably, PQCA

has launched the Open Quantum Safe project, one of the world's leading open-source software projects devoted to PQC. PQCA will also host the new PQ Code Package project, which aims to build high-assurance, production-ready software implementations of forthcoming PQC standards.[87]

Collaboration for standardization: Work with organizations such as NIST to develop and adopt PQC standards. Actively participate in the standardization process (if possible) and keep up with developments. These efforts ensure robust security measures against future quantum computing threats. The Migration to PQC Building Block Consortium, coordinated by the National Cybersecurity Center of Excellence (NCCoE) at NIST, includes several key industry players such as AWS, Microsoft, Cisco, Thales, Samsung, etc.[88 89]

Plan for supply chain partner collaboration

In recent years, there has been a significant increase in attacks aimed at supply chains, including those targeting outdated encryption products. *"We depend on thousands of suppliers, and not all can afford to invest in post-quantum security. For strategic ones, we must share responsibility and help them reach a good security level,"* says Julio Padilha from Volkswagen & Audi, South America.

Your own assets can be compromised if your contractors and vendors do not take adequate steps.

To ensure your organization is well-prepared for PQC, consider the following steps:

- Discuss vendors' PQC plans to determine whether your organization will need to acquire new hardware or software.
- Incorporate PQC clauses into contracts with suppliers to ensure everyone involved takes the necessary steps to protect your systems.
- Maintain regular communication with your software and hardware vendors to understand the timing of their PQC implementation.
- Ensure that your vendor is using standardized, validated cryptography, for instance by insisting on Federal Information Processing Standards (FIPS) accreditation.[90 91]

Thales has established a PQC Partner Ecosystem to facilitate and accelerate quantum-safe migrations. Thales, together with Quantinuum, helps organizations test and prepare for PQC, incorporating HSMs and QRNG technology.[92]

"We depend on thousands of suppliers, and not all can afford to invest in post-quantum security. For strategic ones, we must share responsibility and help them reach a good security level"

Julio Padilha
From Volkswagen & Audi,
South America

"We are not going to know when a cryptographically relevant quantum computer arrives – no one's issuing a press release. We'll either be ready or we won't."

Ben Packman
Chief Strategy Officer at PQShield

Conclusion

Quantum computing is advancing in increments, each of which brings us closer to the breaking point of public key cryptosystems. Our research shows that forward-thinking organizations are acting. Nevertheless, readiness remains elusive, with just about 10% of the overall research sample (and 16% of early adopters) combining strong organizational foundations with deep technical capabilities. Hesitation to implement the transition to a post-quantum future can be costly. Regulators in the US, UK, and EU have issued guidance encouraging migration, while major cloud and network providers have taken steps to embed post-quantum ciphers. State agencies could be more proactive than organizations in preparing for the PQC era, investing heavily to secure critical national infrastructure, considering the critical nature of data sensitivity and volume of the data to be protected and impacted in case of a threat. Organizations that delay this transition will face retrofit costs, probable penalties, and a loss of customer trust once the first quantum-enabled breach makes headlines.

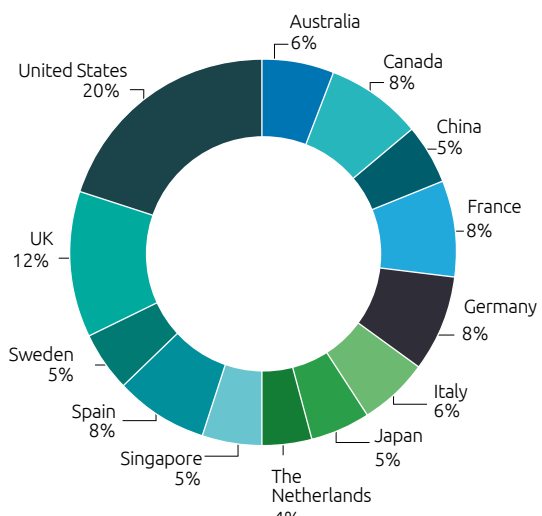
But for organizations that are willing to act, the path to transition is available. Organizations can begin by mapping cryptographic assets and prioritizing them based on business criticality, before launching focused PQC pilots to arrive at a phased-migration roadmap. Embed crypto-agility across all layers of the organization and technical implementations, while fortifying edge and legacy systems against quantum-enabled attacks. Support the transition with skilled teams while working with suppliers to ensure compliance with quantum-safe SLAs. Keep the momentum through enterprise-wide awareness and a governance structure that keeps quantum security to the fore.

Quantum safety is not a discretionary spend but a strategic enabler, which can convert a looming risk into a competitive advantage. The organizations that recognize this fact early will best insulate themselves against the ravages of Q-Day.

Research methodology

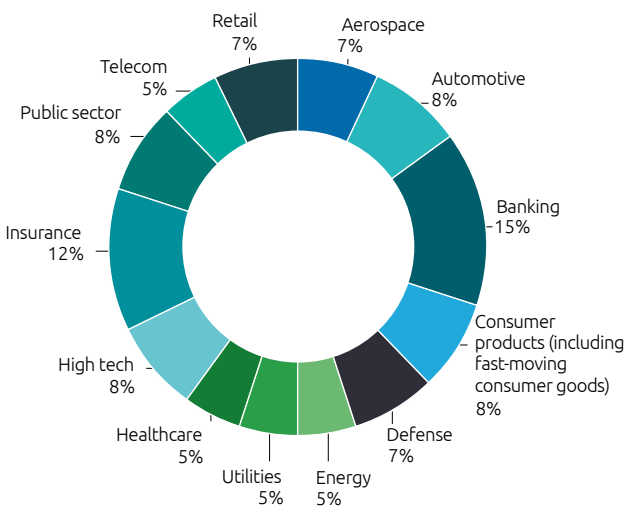
We conducted a survey of 1,000 organizations with annual revenues of at least $1 billion across 13 sectors and 13 countries in Asia–Pacific, Europe, and North America. We carried out the global survey in April–May 2025. Around 70% of this sample, which we refer to as "early adopters" in this report, are either working on or planning to work on quantum-safe solutions in the next five years. We provide the distribution of these respondents and their organizations below.

Organizations by country



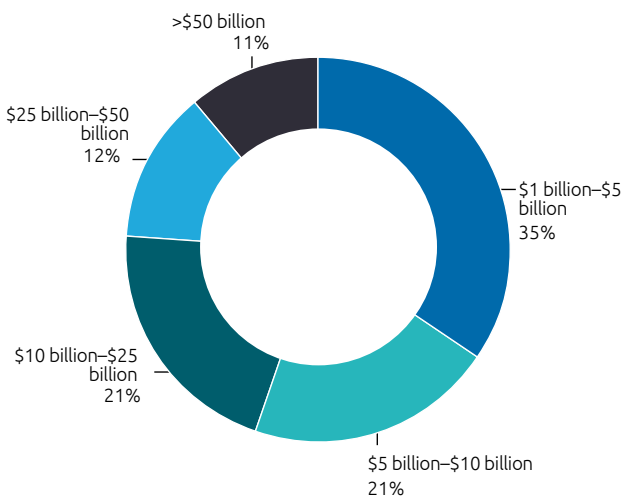
Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 1,000 organizations.

Organizations by sector



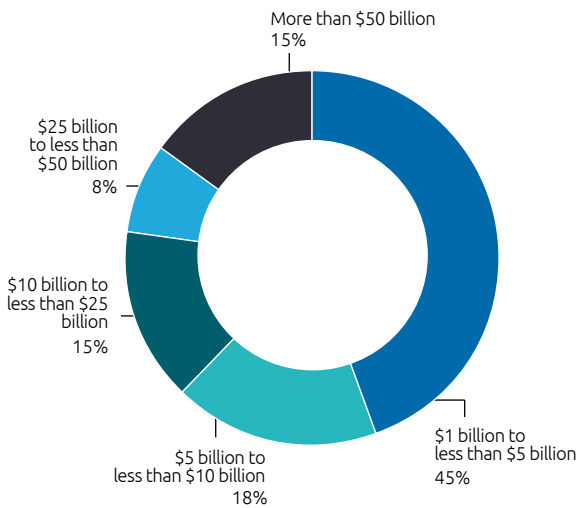
Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 1,000 organizations.

Organizations by annual revenue



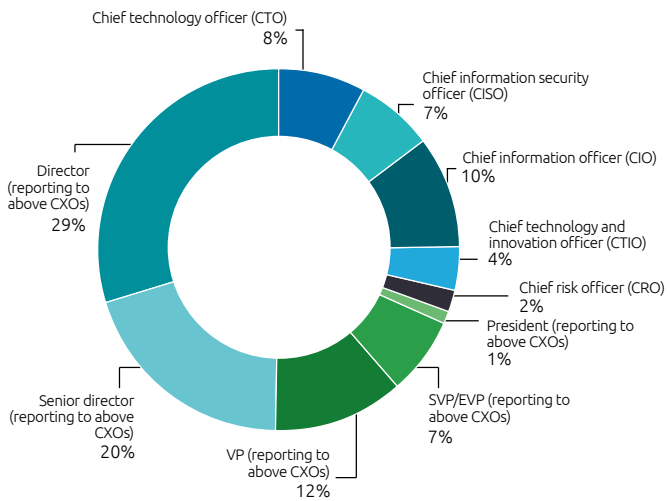
Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 920 organizations excluding public sector.

Public sector organizations by annual budgets



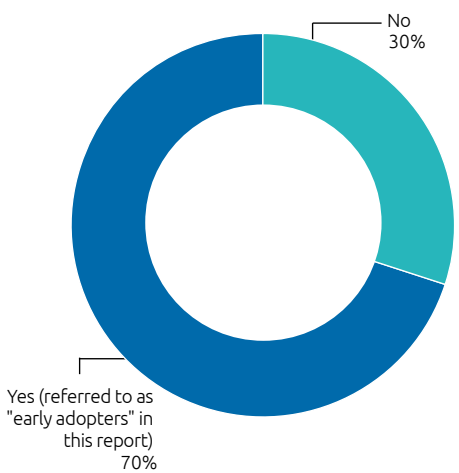
Source: Capgemini Research Institute, PQC survey, April–May 2025, N= 80 public-sector organizations.

Respondents by title/designation



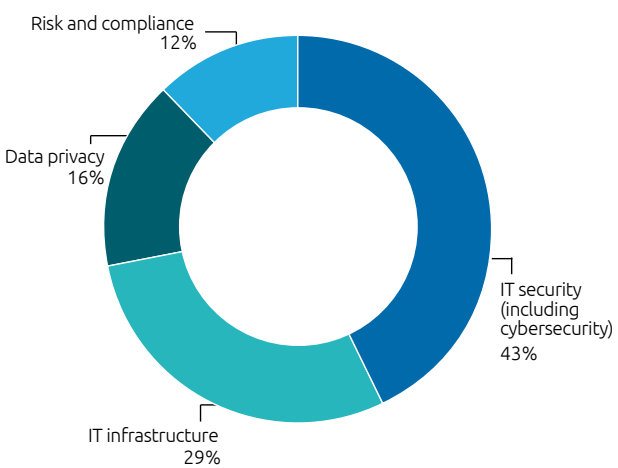
Source: Capgemini Research Institute, PQC survey, April–May 2025, N = 1,000 organizations.

Organizations who are currently working or having a plan for quantum-safe solutions in next five years



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

Respondents by function (split for non-CXO executives)



Source: Capgemini Research Institute, PQC survey, April–May 2025, N= 700 executives who report to CXOs shown above.

To supplement the survey findings, we also conducted in-depth discussions with 16 executives, both from global organizations considering and exploring quantum safety solutions to withstand future cybersecurity quantum threats, and technology vendors who offer PQC solutions.

The study findings reflect the views of the respondents to our online questionnaire for this research and are intended to provide directional guidance. Please contact one of the Capgemini experts listed at the end of the report to discuss specific implications.

References

1. Capgemini Research Institute, “Quantum technologies: How to prepare your organization for a quantum advantage now,” 2022.
2. 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.
3. Forbes, “16 billion Apple, Facebook, Google and other passwords leaked,” June 2025.
4. NIST, “NIST releases first 3 finalized post-quantum encryption standards,” August 13, 2024.
5. NIST, "Transitioning the use of cryptographic algorithms and key lengths,” March 2019.
6. European commission, “EU reinforces its cybersecurity with post-quantum cryptography,” June 23, 2025.
7. AWS, "Customer compliance and security during the post-quantum cryptographic migration,” October 2024.
8. Cloudflare, “Post-quantum between Cloudflare and origin servers,” May 2025. The Cloudflare Blog, “Post-quantum crypto should be free, so we’re including it for free, forever,” March 2023.
9. Apple Security Research, “iMessage with PQ3: The new state of the art in quantum-secure messaging at scale,” February 2024.
10. CyberInsider, “Microsoft rolls out post-quantum cryptography support for Windows Insiders,” May 21, 2025.
11. OpenSSL Corporation "OpenSSL 3.5 Final Release - features: Support for PQC algorithms (ML-KEM, ML-DSA and SLH-DSA)," April 2025.
12. arXiv, "How to factor 2048 bit RSA integers with less than a million noisy qubits," June 2025.
13. Microsoft, “Microsoft’s Majorana 1 chip carves new path for quantum computing,” February 2025.
14. The Quantum Insider, “China Introduces 504-Qubit superconducting chip,” December 2024.
15. Forbes, “China’s Zuchongzhi-3 reshapes quantum race,” March 2025.
16. Capgemini Research Institute, “New defenses, new threats: What AI and Gen AI bring to cybersecurity,” November 2024.
17. Calcalistech, “Quantum computers will be capable of breaking encryption within hours, potentially exposing all the information currently protected on networks,” January 2025.
18. Huawei, “Huawei has been exploring ways to improve internet security, and one such solution is quantum encryption,” March 2025.
19. The Quantum Insider, “BTQ Technologies announces collaboration with South Korea’s future quantum convergence forum and QUINSA,” December 2024.
20. NCSC, “The U.K. National Cyber Security Centre (NCSC) presented a strategic roadmap for key sectors and organizations as they transition to post-quantum cryptography (PQC) to safeguard against future quantum computing threats,” March 2025.
21. TechTarget, “Explore the impact of quantum computing on cryptography,” April 2025.
22. Infosecurity, “Telecoms provider Vodafone is trialing new quantum-safe technology, designed to protect smartphone users from future quantum-enabled attacks while browsing the internet," March 2025.

23. Forbes, “This global cryptographic transition presents an opportunity for healthcare leaders to upgrade their systems to next-gen cryptography,” March 2025.
24. National Cyber Security Centre – UK, "Timelines for migration to post-quantum cryptography," March 2025.
25. Computer Security Resource Center, “NIST - Post-Quantum Cryptography,” August 2024.
26. NSA, “Quantum Key Distribution (QKD) and Quantum Cryptography (QC),” accessed May 2025.
27. TechTarget, “Homomorphic encryption,” August 24, 2022.
28. IDQ, “Quantum Cyber Security,” accessed May 2025.
29. Crypto4A, “Why should modern HSMs always be Quantum-safe and Crypto-agile?” accessed May 2025.
30. Bidenwhitehouse.archives.gov, "Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260," July 2024.
31. The Quantum Insider, "Report reveals growing interest, investments in quantum security market," November 2024.
32. NIST, “NIST Selects HQC as fifth algorithm for post-quantum encryption,” March 2025.
33. Quantum Computing Report, "Vodafone and IBM have announced a collaboration to integrate IBM Quantum Safe technology into Vodafone Secure Net, the company’s all-in-one digital security service," March 2025.
34. Gov.UK, "£121 million boost for quantum technology set to tackle fraud, prevent money laundering and drive growth," April 2025.
35. NCSC, “New guidance from the NCSC outlines a three-phase timeline for organisations to transition to quantum-resistant encryption methods by 2035,” March 2025.
36. NIST – US, “Transition to Post-Quantum Cryptography Standards,” November 2024.
37. CISA, "Quantum-readiness: Migration to post-quantum cryptography," August 2023.
38. Whitehouse.Gov, "Sustaining select efforts to strengthen the nation’s cybersecurity and amending executive order 13694 and executive order 14144," June 2025.
39. ETSI, "A repeatable framework for quantum-safe migrations," April 2024.
40. GSMA, “Post Quantum Cryptography – Guidelines for Telecom Use Cases,” February 2024.
41. ENISA, "Post-Quantum Cryptography: Current state and quantum mitigation," May 2021.
42. Reed Smith, "CSA to roll out quantum security guidelines from 2025," December 2024.
43. Computer Weekly, "Challenges of deploying PQC globally," August 2024.
44. Government Technology Agency – Government of Singapore, "Transitioning Government to PQ," September 2024.
45. Cisco-Outshift, "The quantum threat: Addressing challenges in post-quantum cryptography," March 2025.
46. TechTarget, "How to prepare for a secure post-quantum future," August 2024.
47. Computer Security Resource Center – NIST, "NIST Crypto Agility Workshop," March 2025.
48. JPMorgan Chase, “JPMorgan Chase establishes quantum-secured crypto-agile network,” May 08, 2024.

49. The Quantum Insider, "Organizational quantum readiness remains low," April 2025.
50. GSMA, "Guidelines for quantum risk management for Telco V1.0," September 23, 2023.
51. QryptoCyber, "Importance of cryptographic inventory to quantum threats," May 1, 2024.
52. Government of Canada, Canadian Centre for Cyber Security, "Preparing your organization for the quantum threat to cryptography," (n.d.). Retrieved March 25, 2025, from https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017.
53. QryptoCyber, "Understanding cryptographic inventory: A cornerstone of quantum-ready security," June 15, 2024.
54. Ibid.
55. TNO, "The PQC Migration Handbook – Guideline for migrating to Post-Quantum Cryptography, revised and extended second edition," December 2024.
56. PostQuantum, "Ready for Quantum: Practical steps for cybersecurity teams," November 1, 2021.
57. Government of Canada, Canadian Centre for Cyber Security, "Preparing your organization for the quantum threat to cryptography," (n.d.). Retrieved March 25, 2025, from https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017.
58. PQShield, "The PQC migration handbook: a comprehensive resource," December 18, 2024.
59. PKI Consortium, "Key takeaways of the PQC conference in Austin," January 30, 2025.
60. Forbes, "Quantum-safe infrastructure: Tough challenges (and expert solutions)," January 24, 2025.
61. Center for Cybersecurity Policy, "PQC: Lead the way or fall behind," July 8, 2024.
62. IEEE Spectrum, "Google Develops Quantum-Safe Security Keys," August 2023.
63. Cloudsecurityalliance.org, "NISTIR 8547: From PQC Standards to Real-World Implementations," March 20, 2025.
64. PostQuantum, "Post-Quantum Cryptography PQC Challenges," June 1, 2023.
65. Halock.com, "Primer on Post-Quantum Cryptography (PQC)," (n.d.). Retrieved on March 28, 2025, from https://www.halock.com/primer-on-post-quantum-cryptography-pqc/#_ftn10
66. PQ-React, "PQC for Smart Grid applications," (n.d.). Retrieved on March 25, 2025, from https://pqreact.eu/pilots/
67. qprep.eu, "Q-PrEP-aring Public Institutions in and by the EU," from https://qprep.eu/project/.
68. GQI, Quantum Computing Report, "Sectigo and Crypto4A Launch PQC Labs for Testing Post-Quantum Cryptographic Solutions," February 8, 2025.
69. InformationWeek, "How to overcome the quantum threat," February 27, 2025.
70. TNO, "The PQC Migration Handbook – Guideline for migrating to Post-Quantum Cryptography, revised and extended second edition," December 2024.
71. Forbes, "Quantum-safe infrastructure: Tough challenges (and expert solutions)," January 24, 2025.
72. Security.cms.gov, "Three elements of cryptographic agility," blog post, April 17, 2024.

73. Security.cms.gov, “CMS Key Management Handbook,” October 14, 2022.
74. TNO, “The PQC Migration Handbook.”
75. FS-ISAC, “Building cryptographic agility in the financial sector,” October 2024.
76. SealSq, “Be prepared for the quantum threat,” (n.d.). Retrieved on March 27, 2025, from https://www.sealsq.com/resources/best-practices
77. Kaspersky IT Encyclopedia, “Secure Element,” (n.d.). Retrieved on April 1, 2025, from https://encyclopedia.kaspersky.com/glossary/secure-element/
78. Qubiq, “PQC Implementation on IoT: Challenges and solutions,” August 1, 2024.
79. Secure-ic.com, Post-Quantum Cryptography, (n.d.). Retrieved on March 27, 2025 , from https://www.secure-ic.com/applications/challenges/post-quantum-cryptography/
80. Capgemini, “New quantum-safe cryptographic standards: Future-proofing financial security in the quantum age,” September 4, 2024.
81. PKI Consortium, “Key Takeaways of the PQC Conference in Austin,” January 30, 2025.
82. Capgemini, “New quantum-safe cryptographic standards: Future-proofing financial security in the quantum age,” September 4, 2024.
83. Quantropi, “3 Weaknesses of Post-quantum Cryptography the World Can’t Afford to Ignore,” (n.d.). Retrieved on March 28, 2025, from https://www.quantropi.com/3-weaknesses-of-post-quantum-cryptography/
84. Outshift.cisco.com, “Building a secure future with quantum encryption and scalable quantum networks,” February 7, 2025.
85. AppViewX, “8 Essential Considerations for Post-Quantum Cryptography Migration,” August 1, 2024.
86. Mitre, “Post-quantum Cryptography Coalition publishes comparison of international PQC standards,” September 5, 2024.
87. The Linux Foundation, “Post-Quantum Cryptography Alliance Launches to Advance Post-Quantum Cryptography,” February 6, 2024.
88. SealSq, “Be prepared for the quantum threat,” (n.d.)., Retrieved on March 27, 2025, from https://www.sealsq.com/resources/best-practices
89. Csrc.nist.gov, “The NCCOE migration to post-quantum cryptography” presentation, December 1, 2022.
90. Government of Canada, Canadian Centre for Cyber Security, “Preparing your organization for the quantum threat to cryptography”, (n.d.). Retrieved March 25, 2025, from https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017.
91. Center for Cybersecurity Policy, “PQC: Lead the way or fall behind,” July 8, 2024.
92. Thales, “Thales PQC partner ecosystem facilitates and accelerates quantum-safe migrations,” blog, August 15, 2024.

Authors

Meet the experts

Pascal Brier
Group Chief Innovation Officer and member of the Group Executive Committee, Capgemini
pascal.brier@capgemini.com

Pascal Brier is the Group Chief Innovation Officer and member of the Group Executive Committee at Capgemini, a role he has held since 2021 after a long career in leadership positions at Microsoft, AT&T and NCR. In his current position, Pascal oversees Technology, Innovation and Ventures for the Group worldwide. His efforts center on tracking, analyzing, and implementing more than 1,000 emerging technologies annually. Under his guidance, the company constantly strives to be at the forefront of technological innovation, making significant impacts on the world of business and wider society.

Karine Brunet
CEO, Cloud and Infrastructure Services and member of Group Executive Committee, Capgemini
karine.brunet@capgemini.com

Karine was previously Capgemini's COO of Cloud Infrastructure Services since 2019. Before Capgemini, Karine was Vodafone's Technology Services Director, and she also held senior roles at Steria, Alcatel, and NCR. Karine has a strong track record of managing large transformation and infrastructure businesses. She holds three master's degrees in Marketing and European Management, Economic Sciences, and European Economics.

Marco Pereira
Executive Vice President, Global Head Cybersecurity, Cloud and Infrastructure Services, Capgemini
marco.pereira@capgemini.com

Marco previously served as Chief Product and Strategy Officer at Trustwave, and Global Head of Strategy, Operations, and Product Management for Cybersecurity at DXC. Earlier in his career, he also held senior roles at HP, Wipro, and NTT Data. Marco holds a bachelor's and a master's degree in Information Systems and Computer Engineering, an MBA, and several leading industry cybersecurity certifications, including CISSP, CCSP, CISM, CISA, and ISO 27001 Lead Auditor.

Julian van Velzen
CTIO and Head of Quantum Lab, Capgemini
julian.van.velzen@capgemini.com

Julian van Velzen is the head of Capgemini's Quantum Lab, a global network of quantum experts, partners, and facilities. He leads efforts to transform R&D through the integration of AI, high-performance computing, and quantum technologies. His work also focuses on preparing organizations for a quantum future and adopt post-quantum cryptography. He has a background in condensed matter physics and is a member of Capgemini's CTIO community.

Authors

Meet the experts

Joshua Welle
Vice President – Global Head of Cybersecurity Portfolio
joshua.welle@capgemini.com

Joshua is a seasoned cybersecurity and national security expert with over 20 years of management consulting and operational experience. A trusted advisor to CIOs and CISOs, Joshua delivers high-impact cybersecurity programs and is a recognized thought leader, writing on cybersecurity topics, digital strategy, and leadership. Joshua is a member of the Council on Foreign Relations and the Truman National Security Project. A retired Navy Commander, he is a graduate of the U.S. Naval Academy and holds advanced degrees from the Harvard Kennedy School and the University of Maryland.

Adrian Neal
Senior Director, Global lead for PQC, Capgemini
adrian.neal@capgemini.com

Adrian, an Oxford master's graduate and two-time NATO Defence Innovation Challenge winner, is a globally recognized expert in cybersecurity and cryptography. Over 40 years, he has held roles across banking, insurance, financial markets, energy, pharma, IT, aviation, and telecoms in eight countries on three continents. He primarily advises governments, defense firms, and multinational companies on post-quantum readiness and also counsels central banks on the social and economic risks of Central Bank Digital Currencies (CBDCs), especially regarding future post-quantum cryptographic instability.

Geert van der Linden
Executive Vice President, Cybersecurity, Capgemini
geert.vander.linden@capgemini.com

Geert has served as the CISO for Cloud Infrastructure Services since 2021. He was the head of the global cybersecurity practice until 2024, where he was instrumental in developing the portfolio. He joined Capgemini in 2008, initially managing the application outsourcing practice in the Netherlands, before becoming the CIO of the Infrastructure Strategic Business Unit (SBU) in 2012. Early in his career, Geert also worked with the Dutch government. He holds degrees in Informatics, Business Informatics, and Organization, and is a qualified Chartered Accountant and Chartered IT Auditor.

Jerome DESBONNET
CTIO, Cybersecurity and Chief cybersecurity architect for Cloud and Infrastructure Services, Capgemini
jerome.desbonnet@capgemini.com

Prior to his current role, Jerome served as the Head of Security Solutions and Operations at Euroclear from 2018 to 2021. He also held the position of Global Cybersecurity CTO at Capgemini and SOGETI. His background includes roles as a security CTO for various organizations, project lead, and engineer, specializing in consulting, security engineering, architecture, identity and access management (IAM), privileged access management (PAM), Security Operations Center (SOC) management, threat intelligence, and threat hunting.

Authors

Meet the Capgemini Research Institute

Jerome Buvat
Head of the Capgemini Research Institute
jerome.buvat@capgemini.com

Jerome is the head of the Capgemini Research Institute. He works closely with industry leaders and academics to help organizations understand the business impact of emerging technologies.

Ramya Krishna Puttur
Associate Director, Capgemini Research Institute
ramya.puttur@capgemini.com

Ramya has over thirteen years of experience in consulting and digital transformation and is an Indian Institute of Technology alumnus with gold medals at both post-graduation and under-graduation levels. She has co-authored numerous publications for the Capgemini Research Institute on the impact of digital technologies across industries and developed proprietary tools for assessing clients' data and digital maturity.

Siva Chidambaram Sathyanandan
Manager, Capgemini Research Institute
siva.chidambaram-s@capgemini.com

Siva is a seasoned manager carrying experience collaborating with industry leaders to drive modern tech-enabled solutions driven by data. He specializes in strategic research, advisory, and improving business operations through business intelligence and thought leadership that aids in staying ahead amongst dynamic landscapes.

The authors would like to thank the following people for their contributions to the research:

Bob Schwartz
EVP, Applied Innovation Exchange, Global Director

Babu Mauze
EVP and Head of Cloud Infrastructure, Capgemini Financial Services

Kei Kumar
Senior Director

Leonardo Silva Carissimi
Director, Cybersecurity - operations

Jean-Marie Lapeyre
EVP & Chief Technology and Innovation Officer - Global Automotive Industry

Andreas Sjostrom
VP and Director of San Francisco Applied Innovation Exchange

Nicolas TICHTINSKY
Security Director

Craig Hilton
Cybersecurity Architect

Arnaud Balssa
EVP, Global Business Technology leader

Marjorie Bordes
VP, Group Chief Information Security Officer, Group Cybersecurity

Ashish Bhasin
Senior Director

Daniel Going
Enterprise Architect

Sudhir Pai
EVP, Chief Technology & Innovation Officer, Financial Services

Alex Bulat
VP Strategy & Transformation Consultant

Subrahmanyam KVJ
Senior Director, Capgemini Research Institute

Daniel Schoeman
Security Architect

Vincent E Foreman
Managing Delivery Architect

Hendrik Meer
Engagement Manager

Vincent Godiner
Chief of Staff to the CIO

Chetan Yadav
Associate Consultant

Ferdy Riphagen
Cybersecurity Architect - Group Cybersecurity

Clément BRAUNER
Managing Consultant

Billy Macleod
Test Analyst

Siebe Spee
Intern, Quantum Lab

Christian Knopf
Cybersecurity Defence Advisor

Henk Vermeulen
Managing Consultant

Sanket Dahake
Manager

Magnus Gerisch
Cybersecurity Business & Technology Advisor

Chris Petronis
Senior Security Consultant

Abhiruchi Masurkar
Senior Consultant

The authors would like to thank all the industry executives who participated in this research. They would also like to thank Tricia Stinton, Esther Buck, Vijayalakshmi K, Punam Chavan, Aparajita Paul, Suparna Banerjee and Manish Saha for their contributions to the research.

Why partner with Capgemini?

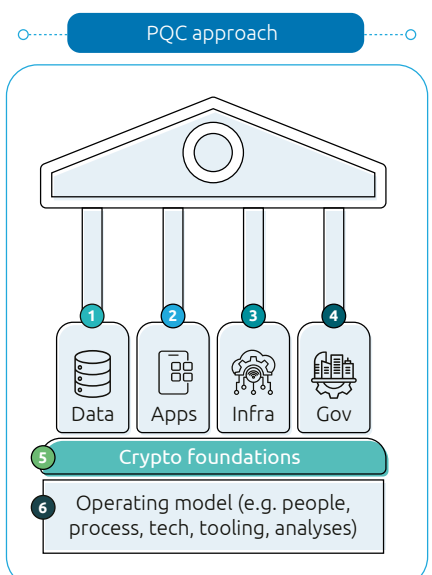
Quantum computing is fast approaching a critical inflection point—threatening to render today's encryption methods obsolete. For organizations entrusted with sensitive data, intellectual property, and digital trust, the risk is no longer theoretical. It's imminent. Capgemini's Post-Quantum Cybersecurity (PQC) services are engineered to help forward-thinking enterprises stay ahead of this disruption. We combine deep cryptographic expertise, industry-specific insights, and a globally proven methodology to help clients:

- Identify and assess vulnerabilities across cryptographic assets
- Enable crypto-agility to adapt to evolving standards
- Implement quantum-safe architectures that scale
- Ensure compliance with emerging regulations

Our end-to-end approach is designed for speed, resilience, and compliance—empowering clients in finance, healthcare, government, and other sectors to future-proof their digital infrastructure.

Capgemini's PQC framework

A future-ready model built on six strategic building blocks —designed to accelerate secure transformation while minimizing disruption.



Building blocks	Description
1 Data security	**Mapping data flows:** Identify and classify data at rest/in transit to align with PQC risk levels.
2 Applications	**Tracking application cryptography:** Identify cryptographic dependencies in critical apps to prioritize migration and ensure operational continuity.
3 Infrastructure	**Managing cryptographic infrastructure:** Evaluate and modernize cryptographic infrastructure (HSMs, PKI, networks) for PQC compatibility.
4 Governance	**Validating governance models :** Assess key management, PKI processes, and compliance readiness to establish strong crypto governance.
5 **Crypto foundations**	Catalog crypto service providers (libraries, entropy sources, HSMs) to assess readiness and reduce dependency risks.
6 **Operating model**	Establish a repeatable model for discovery, risk assessment, and migration planning across people, process, and tech.

The quantum future is closer than you think. If you're exploring how to adapt your cybersecurity strategy for the post-quantum era, we're here to help.
Follow us on LinkedIn: Capgemini Cybersecurity

For more information, please contact:

Global

Marco Pereira
EVP, Global Head of Cybersecurity, Cloud Infrastructure Services (CIS)
marco.pereira@capgemini.com

Julian van Velzen
CTIO and Head of Capgemini's Quantum Lab
julian.van.velzen@capgemini.com

Joshua Welle
Vice President – Global Head of Cybersecurity Portfolio
joshua.welle@capgemini.com

Adrian Neal
Senior Director and Global Offer Lead, PQC, CIS
adrian.neal@capgemini.com

Regional

APAC
Keith Betts
Senior Director, Cybersecurity
keith.betts@capgemini.com

Germany
Adivitya Mahajan
Cloud and platforms security specialist
adivitya.mahajan@capgemini.com

Brazil
Leonardo Silva Carissimi
Director, Cybersecurity operations
leonardo.carissimi@capgemini.com

North America
Cedric Thevenet
Head of Cyber Sales & Solutioning
cedric.thevenet@capgemini.com

UK
Doug Davidson
Cybersecurity Business Solutions Architect
doug.davidson@capgemini.com

France
Abdembi Miraoui
Co-Head of Cloud, Endpoint & Infrastructure Security
abdembi.miraoui@capgemini.com

Spain
Andrews De Benito Orbañanos
Engagement Manager
andres.de-benito-orbananos@capgemini.com

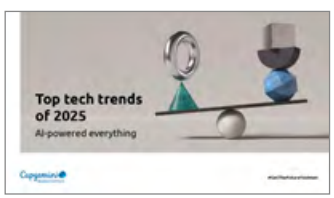
The Netherlands
Julian van Velzen
CTIO and Head of Capgemini's Quantum Lab
julian.van.velzen@capgemini.com

More Capgemini Research Institute publications

Quantum technologies: How to prepare your organization for a quantum advantage now

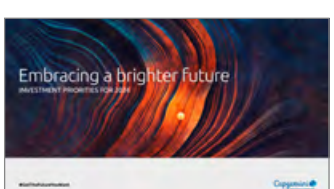
New defenses, new threats: What AI and Gen AI bring to cybersecurity

Conversations for Tomorrow #9: Generative AI



Top Tech Trends of 2025: AI-powered everything

Navigating uncertainty with confidence: Investment priorities for 2025



Embracing a brighter future: Investment priorities for 2024

Gen AI in software

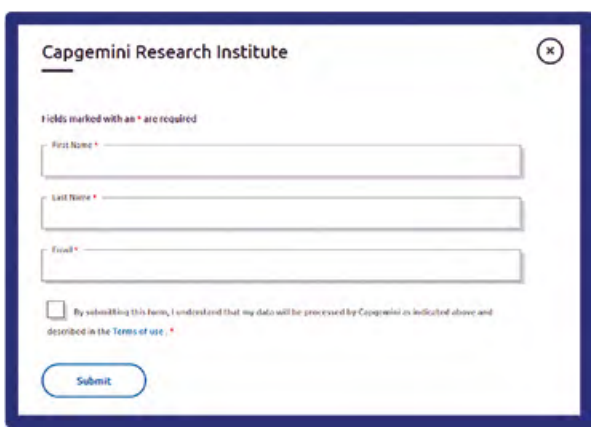
A world in balance 2024: Accelerating sustainability amidst geopolitical changes

Generative AI in organizations 2024

The resurgence of manufacturing: Reindustrialization strategies in Europe and the US 2025

Subscribe to latest research from the Capgemini Research Institute

Receive copies of our reports by scanning the QR code or visiting
https://www.capgemini.com/capgemini-research-institute-subscription/



Notes

Notes

Notes

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Get the Future You Want | **www.capgemini.com**