Persistent
Re(AI)magining™ the World

Facing Post Quantum Wake Up Call

Answering What, Why and When for CIOs, CISOs, CTOs & Digital Leaders

On a quiet Monday morning, a global bank's fraud team spots something unusual. Transactions are being authorized with valid digital signatures from certificates that were revoked years ago. Audit logs show no tampering. The cryptographic controls all appear intact. Yet funds are moving.

The only possibility: Attackers are forging transactions using data they harvested years ago, which they have now decrypted and manipulated using quantum-enabled capabilities.

This is not science fiction. It is a plausible future for any organization whose security and trust are anchored in today's public-key cryptography. Quantum computing is now a strategic disruptor that will reshape how enterprises secure data, design systems and maintain trust.

With the National Institute of Standards and Technology (NIST) finalizing post-quantum cryptographic (PQC) standards and adversaries already harvesting encrypted data for future decryption, the question for technology and security leaders is no longer, "Is quantum coming?" but "Will we be ready when it does?"

For CIOs, CISOs, CDOs, CTOs and senior security practitioners, the next 24–36 months will determine whether they enter the quantum era prepared or exposed.

Not Tomorrow's Threat, Today's Truth

Timelines for a Cryptographically Relevant Quantum Computer (CRQC) remain varied, but consensus is tightening around a 7 - 15 years window. That can sound distant, until one remembers how long it takes to change the cryptographic foundations of a complex enterprise.

> **A compromise a decade from now will be triggered by data theft taking place today.**

In most large organizations, cryptography is everywhere and largely invisible:

- Embedded in application code, APIs, microservices and AI pipelines.
- Baked into network devices, databases, cloud platforms, storage systems and data protection layers.
- Hard-wired into certificates, identity systems, machine identities, workload identities and hardware security modules.
- Powering agentic AI systems, GenAI platforms, model-to-model trust and autonomous machine -to-machine interactions.
- Entangled with third-party platforms, SaaS products and legacy systems that are rarely touched.

The rise of agentic AI, GenAI platforms and machine to machine identities fundamentally amplifies this challenge. Cryptography is no longer just protecting human users and static systems; it now underpins autonomous agents, AI workflows, model APIs, ephemeral workloads and non human identities operating at machine speed. These systems continuously authenticate, encrypt, sign and exchange data — often without clear ownership, visibility or upgrade paths — making post quantum readiness significantly more complex and more urgent.

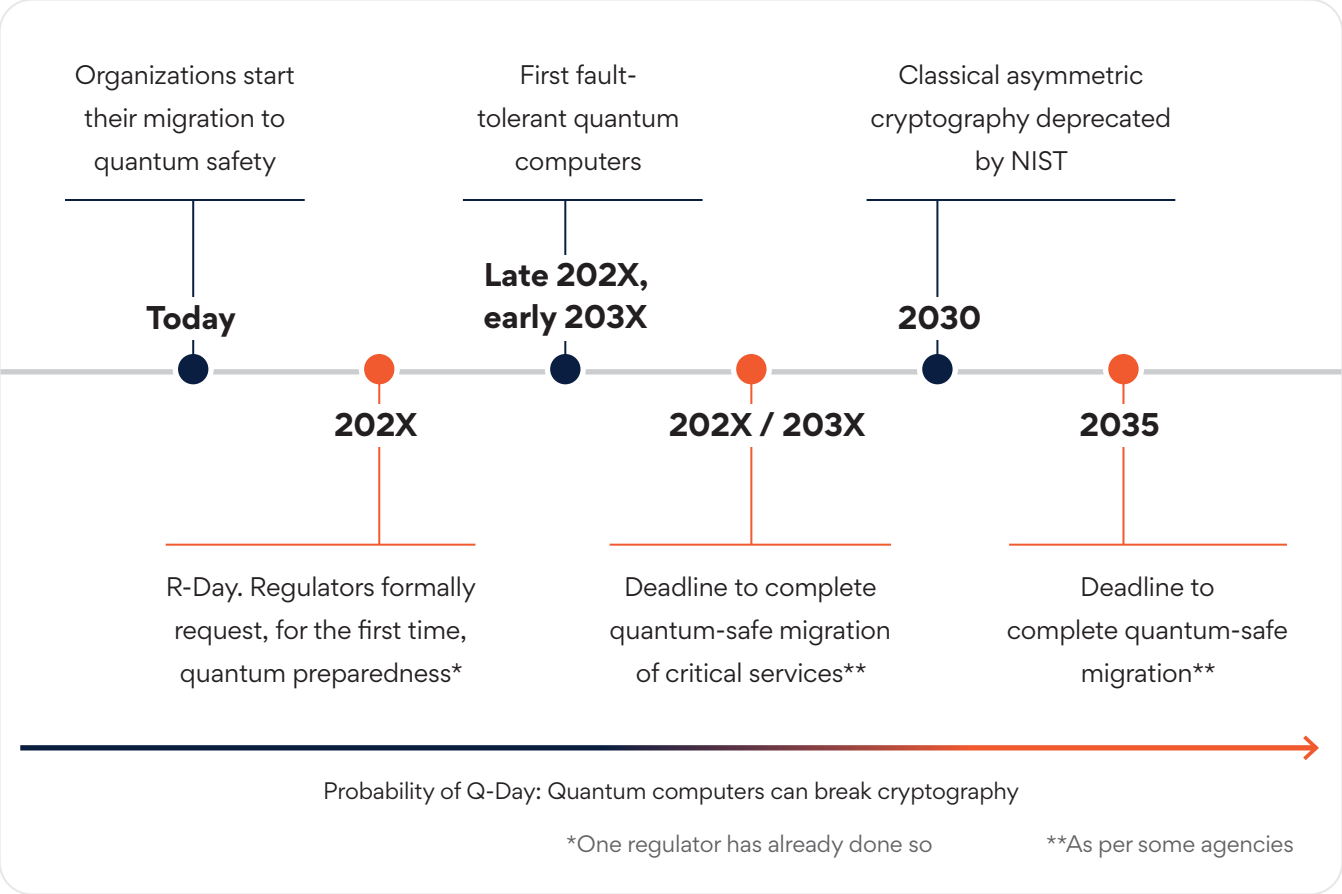


Figure 1: Timeline for the migration to quantum safety, Source: World Economic Forum

Changing these foundations, including algorithms, key lengths, protocols and libraries, can easily span seven to 10 years. Which means:

If data needs to remain confidential for more than 10 years, it is at risk **today**.

If systems have long upgrade cycles, they are at risk **today**.

If vendors are not quantum-ready, enterprises are at risk **today**.

Ticking Bomb: Harvest Now, Decrypt Later

Nation-state actors and sophisticated adversaries are already collecting encrypted data, expecting to decrypt it when quantum capabilities mature. This "harvest now, decrypt later" strategy is especially dangerous for sectors with long-lived, high-value data:

BFSI: Transaction logs, KYC data, payment rails, long-term contractual agreements.

Healthcare: Lifetime patient histories, genomic data, medical device telemetry.

Telecom: Signalling data, network telemetry, customer metadata.

Manufacturing & IP-heavy Industries: R&D archives, design files, patents, industrial control data.

Government & defense: Classified archives, diplomatic cables, military communications.

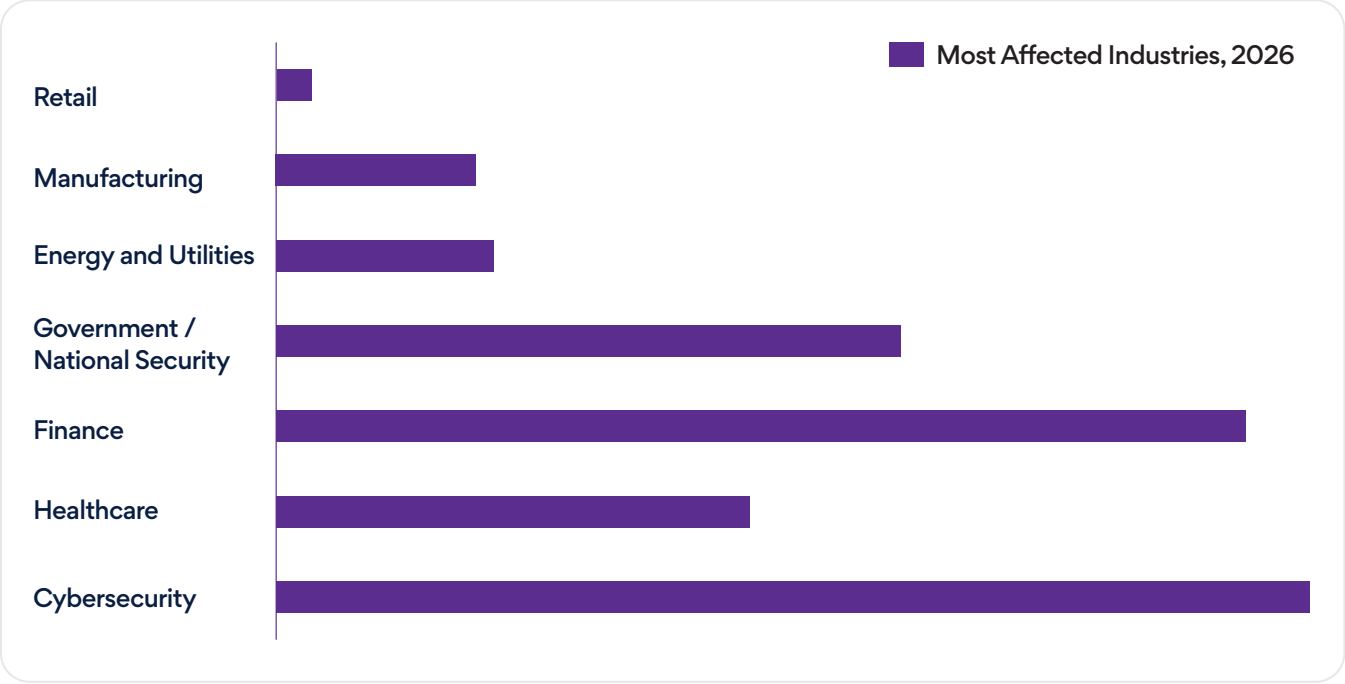


Figure 2: Harvest-Now-Decrypt-Later threat exposure for industries, Source: Fortune Business Insights

Quantum is no longer theoretical. It is a live threat vector that is already interacting with current decisions on data retention, encryption and system design.

Generational Shift: NIST PQC Standards

The finalization of algorithms such as CRYSTALS-Kyber (for key establishment) and CRYSTALS-Dilithium (for digital signatures) by NIST marks the most significant cryptographic shift in four decades. These algorithms are designed to withstand both classical and quantum attacks, but they introduce new performance characteristics, integration challenges and architectural implications.

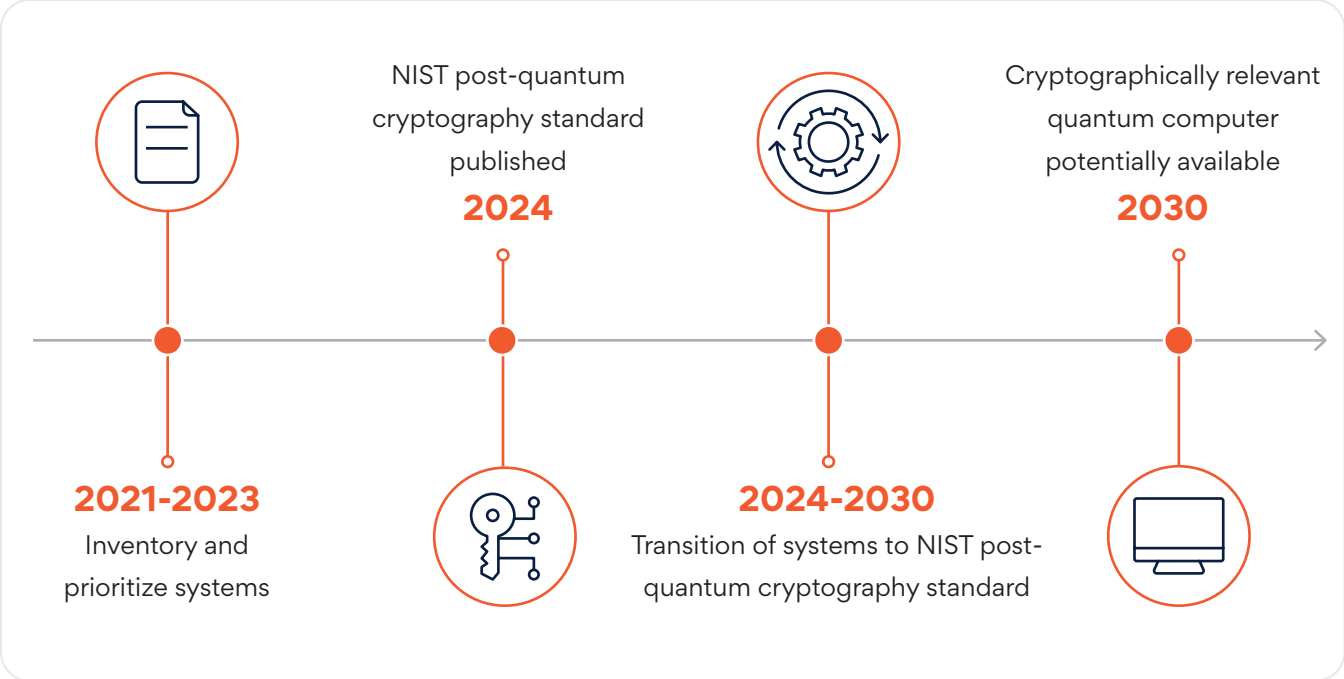


Figure 3: Preparing for Post-Quantum Cryptography, Source: Department of Homeland Security, in partnership with NIST

For **CIOs and CTOs**, this means

- The technology stack must evolve to support PQC-ready protocols and libraries.
- The vendor ecosystem must align with NIST's roadmap and related international standards.
- Architecture must move decisively toward crypto agility, or the ability to swap algorithms without redesigning systems from scratch.

For **CISOs and security leaders**, this means

- Risk models must explicitly incorporate quantum timelines and harvest-now / decrypt-later scenarios.
- Governance frameworks must include PQC migration and crypto lifecycle management.
- Incident response, crisis management and business continuity plans must assume quantum-enabled adversaries.

> **This is not a patch. It is a foundational redesign of how organizations think about trust.**

Regulators are Moving Faster than Enterprises

In the US, the Quantum Computing Cybersecurity Preparedness Act and related OMB memoranda require federal agencies to conduct quantum readiness assessments and plan PQC transitions aligned to NIST standards. In the European Union, the EU Cybersecurity Act and GDPR's security-by-design and state-of-the-art encryption obligations increasingly treat quantum-resilient cryptography as part of appropriate technical measures. India is similarly investing in indigenous PQC research and quantum-safe telecom infrastructure through national programs and guidelines, signalling a global move toward mandated quantum-safe security.

The expectation is clear: Compliance deadlines will not wait for enterprise comfort or vendor readiness. Organizations that delay will face compressed timelines, higher costs and elevated operational risk when regulations converge with real-world quantum capabilities.

Who Owns Quantum Readiness?

One of the most common questions in boardrooms and executive discussions is: “Who should own our quantum readiness program?”

The honest answer is that no single function can own this alone. But someone must lead.

A practical governance structure looks like this:

- **Executive Sponsor**: Typically, the CIO or CISO, is accountable for overall program success and reporting to the board.
- **Co-Leads**: CIO (architecture and platforms), CISO (risk, controls, security), CTO (innovation, engineering), CDO (data strategy and retention).
- **Steering Committee**: Cross-functional group including enterprise architecture, security, risk, legal / compliance, procurement and business unit leaders from high-risk areas (e.g., retail banking, clinical operations, network operations).
- **Program Management Office**: Coordinates crypto inventory, risk assessment, vendor engagement and migration projects; tracks KPIs and regulatory milestones.

Clarity on roles is essential:

- **CIO / CTO**: Drive crypto-agile architectures, platform modernization and roadmap integration.
- **CISO**: Owns quantum risk assessment, control requirements and alignment with security frameworks.
- **CDO**: Revisits data classification, retention and minimization in a quantum-threat context.
- **Procurement & Vendor Management**: Embed PQC and crypto agility requirements into contracts and RFPs.
- **Risk & Compliance**: Map PQC readiness to regulatory expectations and enterprise risk appetite.

Crypto Inventory: First Strategic Milestone

Most organizations cannot answer a basic question: Where exactly do we use cryptography today?

Yet this is the starting point for any serious quantum readiness journey. Cryptography is not confined to a single layer of the stack — it is deeply embedded across the digital enterprise, including:

- Business applications, microservices and APIs that secure transactions and data flows.
- Databases, data lakes and backup systems protecting data at rest and in motion.
- Network infrastructure, VPNs and secure connectivity layers.
- Identity, access and privilege management platforms.
- Digital certificates, key management and PKI ecosystems.
- Hardware Security Modules (HSMs), secure enclaves and trusted execution environments.
- Third-party software, SaaS platforms, cloud services and managed service providers.

A quantum impact in any one of these layers can undermine trust across the entire ecosystem.

A crypto inventory is far more than a technical exercise. It is a strategic asset inventory that informs:

Risk management
What data and systems are most exposed to quantum threats?

Architecture
Which components require redesign vs. configuration changes?

Procurement
Where are you dependent on vendors who are not quantum-ready?

Compliance
How will you demonstrate due diligence to regulators and auditors?

> **For CIOs and CDOs, this becomes a data governance and architecture priority. For CISOs, it becomes a foundational control. For CTOs, it is a driver for modernization and simplification.**

Crypto Agility: Designing for Next Change

One of the most important design principles for the quantum era is crypto agility. Practically, this means:

Abstracting cryptography	behind well-defined services or libraries, rather than hard-coding algorithms inside business logic
Centralizing key and policy management	so algorithms and key sizes can be changed via configuration and policy, not code changes
Avoiding tight coupling	between applications and specific cryptographic primitives, protocols or vendors
Building hybrid modes	(classical + PQC) into design where feasible, to support gradual, low-risk transitions.

Crypto agility is not just a technical convenience; it is an insurance policy against future cryptanalytic breakthroughs, quantum or otherwise. What not to do:

Hard-code specific algorithms (e.g., RSA-2048, ECDSA) in application code.

Scatter cryptographic implementations across teams & repositories without standards.

Assume cloud provider or vendor will solve crypto agility on the organization's behalf.

Rethinking Data Classification and Retention

Quantum readiness is a data lifecycle issue as much as it is a cryptography issue. Traditional classification focuses on sensitivity (public, internal, confidential, highly confidential). Quantum-aware classification adds dimensions such as:

Longevity	How long must this data remain confidential or trustworthy?
Impact of future exposure	What happens if this data is decrypted in 10–20 years?

In practice, that means:

Re-evaluating retention policies for high-sensitivity, long-lived data (e.g., reducing unnecessary long-term storage where legally permissible).

Tokenizing or pseudonymizing sensitive data where possible, especially in analytics and test environments.

Segmenting and segregating crown-jewel datasets with stronger protections and earlier PQC adoption.

This is where CDOs and data governance councils must work closely with CISOs and architects.

Organizational Challenges Bigger than Technical Ones

The hardest part of any security shift is rarely the technology itself. It is the organization's ability to adapt. Overcoming these requires clear executive sponsorship, cross-functional governance and a narrative that connects PQC to business resilience and trust, not just to security hygiene. With PQC, expect challenges such as:

Performance overhead from new algorithms impacting latency-sensitive systems

Skills shortages in modern cryptography, secure engineering and crypto agility

Vendor readiness gaps where critical suppliers lag behind NIST timelines

Cultural resistance because cryptography has historically been "invisible" and outside business conversations

Interoperability issues with legacy systems and protocols that were never designed for PQC

Role of Vendors and Partners

No enterprise can migrate to PQC on its own. Success depends heavily on vendors and partners, but that does not mean everything is at their mercy.

Leaders should demand from key suppliers:

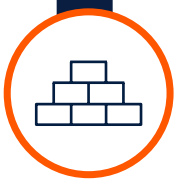
- PQC-ready product roadmaps aligned with NIST and relevant regional standards.
- Hybrid classical + PQC support to enable gradual, low-risk transition.
- Transparent timelines and migration guides for their products and services.
- Interoperability testing results and participation in relevant industry working groups.
- Contractual commitments on PQC adoption, support windows and security disclosures.

Critical questions to ask vendors:

- Where do your products rely on public-key cryptography today?
- What is your roadmap for PQC support and how does it align with NIST standards?
- How will you support hybrid deployments (classical + PQC)?
- What performance and interoperability testing have you conducted?
- How will you notify us of cryptographic vulnerabilities and migration requirements?

Realistic 10-Year Roadmap

Quantum readiness is a marathon, not a sprint. A realistic roadmap spans roughly a decade:



Years 1–3

Foundation

- Establish governance and executive sponsorship.
- Conduct a crypto inventory across applications, infrastructure and vendors.
- Classify cryptographic use cases by data sensitivity, longevity and business criticality.
- Run quantum risk assessments for high-value, long-lived data and critical systems.
- Conduct vendor assessments focused on PQC roadmaps and crypto agility.
- Launch pilot PQC deployments and proofs of concept in non-critical environments.
- Design crypto-agile architectures and reference patterns.

Years 4–6

Transition

- Roll out hybrid classical + PQC solutions in prioritized domains.
- Implement PQC-ready key management and PKI infrastructures.
- Upgrade network and application stacks to support PQC-capable libraries and protocols.
- Coordinate vendor ecosystem alignment; adjust contracts and SLAs.
- Integrate PQC milestones into broader programs (cloud, zero trust, digital identity).

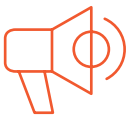
Years 7–10

Maturity

- Achieve full PQC adoption for critical systems and long-lived data.
- Decommission vulnerable algorithms and legacy crypto implementations.
- Embed continuous crypto governance and monitoring.
- Integrate with quantum-safe communication channels and evolving standards.
- Periodically reassess posture as quantum capabilities and standards evolve.

First 90 Days: What Leaders Should Do Now

Here is a pragmatic 90-day action plan:



Days 1–30

Awareness and Ownership

- **Brief the board and executive team**: Provide a concise overview of quantum risk, PQC standards and what it means for the organization's data and systems.
- **Appoint an executive sponsor**: In partnership with the CIO or CISO, establish a cross-functional quantum readiness working group.
- **Identify crown-jewel data and systems**: Long-lived, high-value data; payments and transaction systems; regulatory reporting; critical infrastructure.

Days 31–60

Discovery and Assessment

- **Launch a scoped crypto inventory** of critical systems and key data flows.
- **Engage 5–10 strategic vendors** to understand their PQC roadmaps and gaps.
- **Integrate quantum risk** into existing enterprise risk registers and security roadmaps.

Days 61–90

Strategy and Pilot

- **Define your quantum readiness strategy and principles**: Crypto agility, data longevity, vendor requirements.
- **Select 1–2 pilot projects**: For example, a non-critical internal application or a segment of your PKI infrastructure to test PQC integration.
- **Establish KPIs / KRIs** for quantum readiness, such as:
  a. Percentage of critical systems covered by crypto inventory.
  b. Number of strategic vendors with credible PQC roadmaps.
  c. Progress against a defined multi-year migration plan.

By the end of 90 days, you are not "quantum-safe" — but you have turned an abstract future risk into a concrete, governed program with momentum.

Board-Talk: Framing Quantum Risk and Readiness

Boards do not need a deep dive into lattice-based cryptography. They need clarity on business impact, regulatory expectations and readiness. Convey to the board:

Quantum risk is real and time-bound
The threat horizon aligns with typical technology refresh cycles, making inaction risky.

Data is already being harvested
Long-lived, high-value data stolen today can be decrypted in the future.

Regulators are moving
There is a clear direction of travel toward mandatory assessments and migration.

There is a credible plan
Governance, inventory, vendor strategy and phased migration steps are defined.

Useful metrics for board reporting:

- Coverage of crypto inventory across critical systems.
- Proportion of strategic vendors with documented PQC plans.
- Percentage of high-value, long-lived data protected with quantum-resilient or hybrid controls.
- Progress against the 3-, 5- and 10-year roadmap milestones.

Connecting PQC to Cloud, Zero Trust and AI

Quantum readiness does not live in isolation. It intersects with other major initiatives:

Cloud Migration

As applications move to the cloud, embed crypto agility and PQC-ready architectures into landing zones and reference designs.

Zero Trust

Strong identity, continuous verification and micro- segmentation all depend on trustworthy cryptography, making PQC part of a robust zero-trust posture.

AI and Data Analytics

As AI models train on sensitive data, ensure that data pipelines, storage and model artifacts are protected with cryptography that can withstand future quantum attacks.

> **Treat PQC not as a separate project but as a critical thread running through your larger transformation fabric.**

What "Good" Looks Like for CIOs, CISOs, CTOs and Security Leaders

A quantum-ready enterprise exhibits:

Visibility: Comprehensive crypto inventory across critical systems and vendors.

Agility: Architectural patterns and platforms that allow algorithm changes without major redesign.

Momentum: Measurable, quarter-by-quarter progress along a clearly articulated roadmap.

Governance: PQC and crypto lifecycle management embedded into architecture, procurement, risk and compliance processes.

Resilience: Hybrid cryptography deployed for high-value, long-lived data and critical services.

The message is straightforward

The future is quantum **The risk is real** **The window to prepare is open — but narrowing**

The time to act is now.

Take the next step — Talk to Persistent about your post-quantum readiness journey.

The organizations that act now will be the ones that protect trust, reduce future disruption and move into the quantum era with confidence. The ones that wait may face compressed timelines, higher costs, vendor dependencies and unnecessary exposure.

Author Details

About Dilip Panjwani

Dilip is a seasoned cybersecurity leader with over two decades of experience serving as CISO across major BFSI institutions, fintech organizations and global IT enterprises.

Across these roles, he has been responsible for securing high-value financial systems, regulatory-driven environments and large-scale digital transformation programs. His work spans enterprise security architecture, threat management, data protection, cloud security and building cyber resilience for organizations operating in some of the most demanding risk landscapes.

Today, Dilip leads the cybersecurity practice and delivery function at Persistent Systems, where he partners with CIOs, CISOs, CTOs and digital leaders to elevate their cybersecurity maturity, strengthen governance and build future-ready security programs. His unique blend of practitioner depth and advisory experience gives him a 360-degree view of the challenges enterprises face as they navigate emerging threats like cyber risk management, quantum risk, AI-driven attacks and regulatory complexity.

Dilip is a trusted voice in the cybersecurity community and a leader who continues to shape how organizations think about security, resilience and digital trust.

Start Your Quantum Readiness Conversation.

Contact Us

About Persistent

Persistent Systems (BSE: 533179 and NSE: PERSISTENT) is a global services and solutions company delivering AI-led, platform driven Digital Engineering and Enterprise Modernization to businesses across industries. With over 26,500 employees located in 18 countries, the Company is committed to innovation and client success. Persistent offers a comprehensive suite of services, including software engineering, product development, data and analytics, CX transformation, cloud computing, and intelligent automation. The Company is part of the MSCI India Index and is included in key indices of the National Stock Exchange of India, including the Nifty Midcap 50, Nifty IT, and Nifty MidCap Liquid 15, as well as several on the BSE such as the S&P BSE 100 and S&P BSE SENSEX Next 50. Persistent is also a constituent of the Dow Jones Sustainability World Index. The Company has achieved carbon neutrality, reinforcing its commitment to sustainability and responsible business practices. Persistent has also been named one of America's Greatest Workplaces for Inclusion & Diversity 2025 by Newsweek and Plant A Insights Group. As a participant of the United Nations Global Compact, the Company is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as take actions that advance societal goals. With 468% growth in brand value since 2020, Persistent is the fastest-growing IT services brand in 'Brand Finance India 100' 2025 Report.

USA
Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Fax: +1 (408) 451 9177
Email: info@persistent.com

India
Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 0000
Fax: +91 (20) 6703 0008

Persistent
Re(AI)magining the World

www.persistent.com