SecureFi Institute Research Brief

Why Post-Quantum Cryptography Matters Now

Preparing Leadership and Systems for the Quantum-Safe Transition

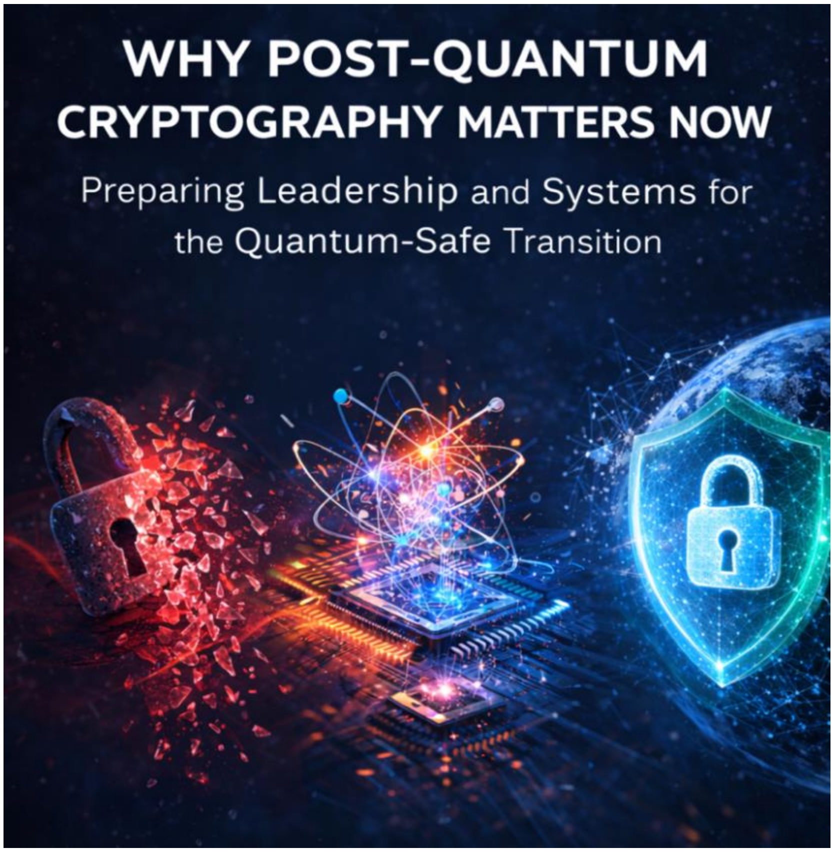
Date: March 2026
SecureFi Institute

SecureFi
Institute
An OnShoreWave Business

Why Post-Quantum Cryptography Matters Now

Preparing Leadership and Systems for the Quantum-Safe Transition

SecureFi Institute Research Brief


WHY POST-QUANTUM
CRYPTOGRAPHY MATTERS NOW
Preparing Leadership and Systems for
the Quantum-Safe Transition

Executive Summary

Post-quantum cryptography is emerging as a strategic cybersecurity priority for governments, critical infrastructure operators, and technology providers. Quantum computing research continues to advance, and widely used public key cryptographic systems such as RSA and elliptic curve cryptography are expected to become vulnerable once sufficiently capable quantum

In August 2024, the National Institute of Standards and Technology released the first finalized post-quantum cryptography standards, marking a significant milestone in the global transition toward post-quantum cryptography. Federal agencies including CISA, NIST, and the Department of Defense have since encouraged organizations to begin inventorying vulnerable cryptographic systems and developing migration plans.

For government agencies, critical infrastructure operators, and commercial enterprises, the challenge is not simply replacing algorithms. The transition will require system inventory, vendor coordination, procurement alignment, and phased migration planning across software, hardware, cloud services, and operational technology.

SecureFi Institute focuses on helping leaders understand this transition from a governance and strategic readiness perspective. As advanced computing environments increasingly converge across cybersecurity, artificial intelligence, high performance computing, and quantum systems, institutional readiness becomes as important as technical capability.

Key Takeaways for Leaders

The transition to post-quantum cryptography represents one of the most significant cybersecurity shifts facing government and industry over the coming decade. While large scale quantum computers capable of breaking current encryption may still be years away, the planning and migration timeline for organizations is already beginning.

Leaders should consider the following priorities.

1. The transition timeline begins before quantum computers arrive

Sensitive data collected today may remain valuable for decades. Adversaries may store encrypted information now and attempt to decrypt it later once quantum capabilities mature. Organizations with long term confidentiality requirements should begin preparing early.

2. Standards are now available

The National Institute of Standards and Technology finalized the first post-quantum cryptography standards in 2024. These standards provide a starting point for organizations to begin integrating quantum resistant algorithms into future systems and procurement decisions.

3. Migration will take years

Cryptography is embedded deeply within enterprise systems, software platforms, cloud services, and operational infrastructure. Identifying where vulnerable algorithms are used and planning upgrades across these environments will take time.

4. This is a leadership issue, not only a technical one

Successful transition will require coordination between cybersecurity teams, executive leadership, procurement offices, and technology vendors. Governance, planning, and risk management will be as important as technical implementation.

5. Early preparation reduces long term risk

Organizations that begin planning now will be better positioned to manage migration deliberately rather than responding under pressure when quantum capable systems eventually emerge.

The question is not whether quantum computing will affect modern cryptography. The question is whether organizations will begin preparing early enough to manage the transition responsibly.

The Issue is No Longer Theoretical

Public key cryptography underpins much of modern digital infrastructure. Encryption protocols used for secure communications, digital signatures, authentication systems, and financial transactions depend heavily on mathematical problems that are difficult for classical computers to solve.

Quantum computing changes this assumption.

Algorithms such as Shor's algorithm theoretically allow a sufficiently powerful quantum computer to factor large numbers and solve discrete logarithm problems far more efficiently than classical computers. These capabilities could compromise widely used encryption methods including RSA and elliptic curve cryptography.

While practical quantum computers capable of breaking current encryption are still under development, the global security community recognizes that the transition to post-quantum cryptography must begin well before such systems arrive.

The Harvest Now, Decrypt Later Risk

One of the most important drivers behind early adoption of post-quantum cryptography is the concept known as harvest now, decrypt later.

Adversaries may collect encrypted data today with the expectation that it can be decrypted in the future when quantum computing capabilities improve. This creates risk for information that must remain confidential for long periods of time.

Examples include

National security data
Intellectual property
Financial and banking records
Health and medical data
Critical infrastructure systems
Government communications

For organizations that rely on long-term confidentiality, the timeline for action is not determined by when quantum computers arrive. It is determined by how long sensitive information must remain secure.

What Changed Recently

Several developments have moved the conversation about post-quantum cryptography from research into implementation planning.

In 2024, the National Institute of Standards and Technology finalized the first set of post-quantum cryptography standards, including CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium for digital signatures**.** These standards provide a foundation for organizations to begin integrating post-quantum cryptography into future systems.

NIST also selected SPHINCS+ as an additional digital signature standard and continues to evaluate additional algorithms as part of the broader PQC transition.

Federal agencies have begun encouraging organizations to prepare for migration. The Cybersecurity and Infrastructure Security Agency has issued guidance urging agencies and infrastructure operators to identify vulnerable cryptographic systems and develop transition plans.

The Department of Defense has similarly emphasized the importance of preparing for post-quantum cryptographic migration across defense, intelligence, and national security environments.

In addition to agency guidance, the United States government has identified quantum computing and post-quantum cryptography as strategic national priorities. Federal initiatives such as the National Quantum Initiative and recent national cybersecurity strategies emphasize the importance of preparing government and critical infrastructure systems for the long-term security implications of advanced computing technologies. These initiatives reinforce the expectation that organizations should begin preparing for cryptographic transition well before quantum systems capable of breaking current encryption become operational.

Together, these developments signal that the transition to post-quantum cryptography has entered an early implementation phase.

The Migration Challenge

Replacing cryptographic algorithms across modern digital infrastructure is complex. Encryption technologies are embedded deeply within software applications, operating systems, network protocols, hardware devices, and cloud services.

In many cases, organizations do not have complete visibility into where cryptography is implemented across their environments.

Migration planning typically requires several steps

Identifying where public key cryptography is used
Determining which systems depend on vulnerable algorithms
Prioritizing systems based on mission impact and data sensitivity

Engaging vendors regarding post-quantum readiness
Planning phased upgrades across infrastructure and applications

For large organizations, the transition may take many years to complete.

Why This Matters for Government and Commercial Markets

Government agencies face unique challenges related to national security, classified systems, and long-term technology platforms. Systems deployed today may remain operational for decades, increasing the importance of early planning.

Commercial organizations face different pressures including regulatory compliance, supply chain dependencies, customer trust, and operational continuity.

Industries likely to experience early pressure include

Financial services
Healthcare and medical technology
Telecommunications
Energy and critical infrastructure
Defense and aerospace
Cloud and technology providers

In both government and commercial environments, leadership awareness is essential. The transition to post-quantum cryptography (PQC) is not purely technical. It involves governance, procurement, risk management, and long-term technology planning.

Leadership Readiness

The transition to post-quantum cryptography will require collaboration between technical teams, executive leadership, policymakers, and industry partners.

Organizations that begin planning early will be better positioned to

Reduce long-term security risk
Avoid rushed migration under future pressure
Coordinate vendor roadmaps and procurement decisions
Strengthen institutional resilience
Maintain trust in digital infrastructure

Leadership awareness therefore becomes a critical component of successful transition.

Conclusion

The transition to post-quantum cryptography represents one of the most significant cybersecurity shifts of the coming decade. While the timeline for cryptographically relevant quantum computers remains uncertain, the direction of travel is clear.

Standards are emerging. Federal guidance is expanding. Industry awareness is growing.

Organizations that begin preparing today will be better positioned to manage the transition responsibly and maintain long-term security in a rapidly evolving technological environment.

SecureFi Institute supports government and institutional leaders in understanding emerging technologies and preparing for the governance, security, and operational challenges they introduce.

References

National Institute of Standards and Technology (NIST)
Post-Quantum Cryptography Standardization Project

Cybersecurity and Infrastructure Security Agency (CISA)
Quantum Readiness and Post-Quantum Cryptography Migration Guidance

Department of Defense Chief Information Officer
Preparing for Migration to Post-Quantum Cryptography

NIST National Cybersecurity Center of Excellence
Migration to Post-Quantum Cryptography Project

National Quantum Initiative Act (United States)

About SecureFi Institute

SecureFi Institute focuses on leadership awareness and governance readiness across emerging computing technologies, including artificial intelligence, cybersecurity, high performance computing, and quantum systems.

The Institute works to help government and institutional leaders understand the security and strategic implications of these technologies before they become deeply embedded in critical infrastructure.

SecureFi Institute Research Brief No. 007

Why Post-Quantum Cryptography Matters Now

March 2026

Figures and Analytical Models

All figures, diagrams, and analytical models presented in this research brief were developed by SecureFi Institute as part of its research on emerging computing architectures and cybersecurity implications.

Research Disclaimer

This research brief is provided for informational and educational purposes and reflects analysis from SecureFi Institute on emerging computing technologies and cybersecurity trends. The views expressed are intended to support awareness and discussion of technology and infrastructure challenges and do not represent official policy positions.