SecureFi Institute Research Series

The Quantum Security Framework -
Emerging Technology and Infrastructure Security

The Quantum Security Gap

Why Institutions Are Unprepared for the Cryptographic Transition

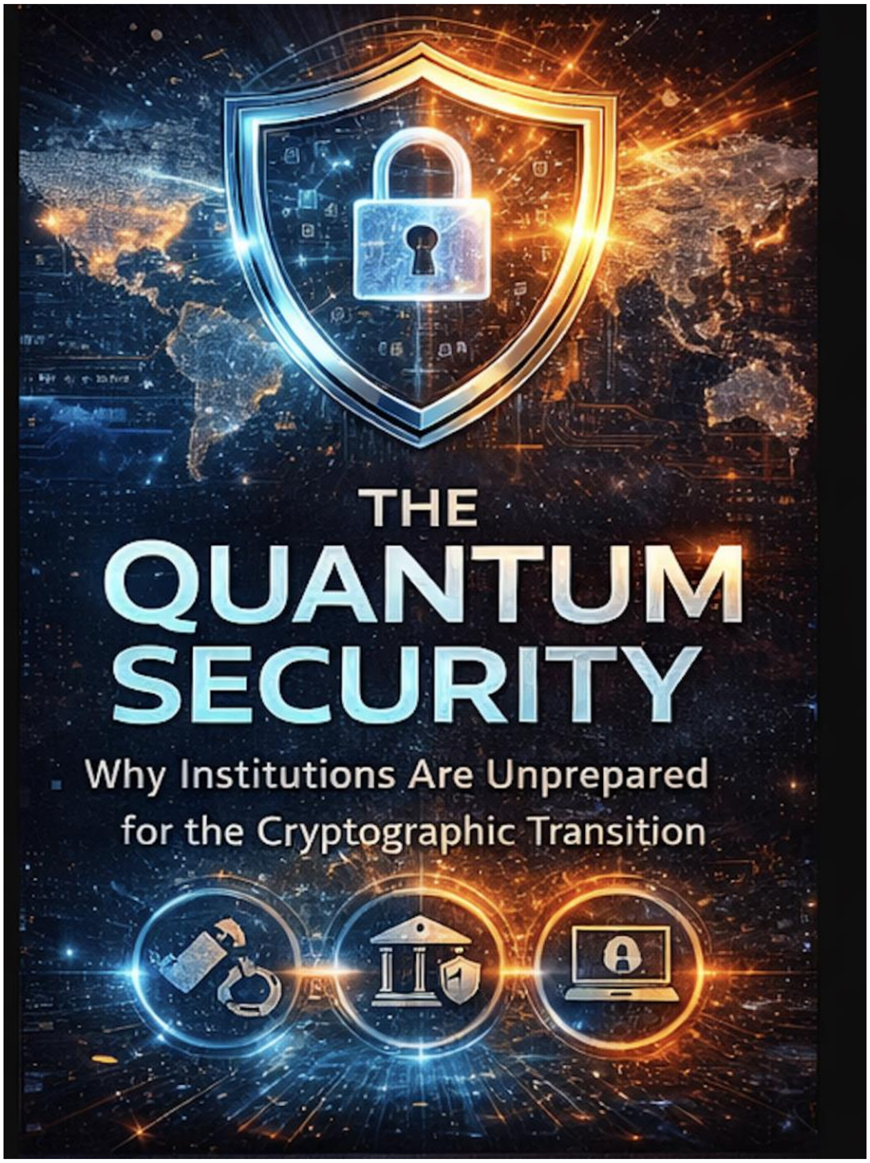
Date: March 2026
SecureFi Institute

SecureFi
Institute
An OnShoreWave Business

The Quantum Security Gap

Why Institutions Are Unprepared for the Cryptographic Transition

SecureFi Institute Research Brief


THE
QUANTUM
SECURITY
Why Institutions Are Unprepared
for the Cryptographic Transition

Executive Summary

Quantum computing has the potential to disrupt widely used cryptographic systems that currently secure digital communications, financial transactions, and critical infrastructure. While research into post-quantum cryptography has accelerated in recent years, most institutions have not yet begun preparing for the transition.

The challenge is not simply the development of new cryptographic algorithms. The greater challenge lies in the scale and complexity of replacing cryptographic systems that are deeply embedded across modern digital infrastructure.

Many organizations lack visibility into where cryptography is used across their systems. Others operate infrastructure with long lifecycles that make rapid transitions difficult. Governance structures, procurement processes, and vendor ecosystems further complicate migration planning.

As a result, a growing gap exists between awareness of the quantum security challenge and the institutional readiness required to address it. Closing this quantum security gap will require coordinated leadership across cybersecurity governance, infrastructure planning, and technology strategy.

This research brief builds on previous SecureFi Institute analyses of post-quantum cryptography, emerging computing infrastructure, and cybersecurity strategy to examine why institutional readiness for quantum security remains limited.

The Growing Awareness of Quantum Risk

Over the past decade, advances in quantum computing research have increased awareness of potential risks to current cryptographic systems. Algorithms such as Shor’s algorithm demonstrate that sufficiently advanced quantum computers could break widely used public key cryptography, including RSA and elliptic curve cryptography.

This possibility has prompted the development of new quantum-resistant cryptographic algorithms designed to withstand attacks from both classical and quantum computers.

Government agencies, research institutions, and technology companies are increasingly evaluating how these new cryptographic approaches can be integrated into existing digital infrastructure.

Despite this growing awareness, most organizations have not yet begun systematic planning for the transition.

The Institutional Readiness Gap

A significant gap exists between understanding the potential impact of quantum computing on cryptography and preparing institutions to address the transition.

In many organizations, awareness of the issue remains limited to specialized technical communities. Executive leadership and governance bodies often view quantum computing as a distant or uncertain challenge rather than an immediate infrastructure planning issue.

As a result, few institutions have developed clear transition strategies or established governance structures to manage the cryptographic changes that will eventually be required.

This gap between awareness and readiness represents one of the most significant challenges in preparing for the future of digital security.

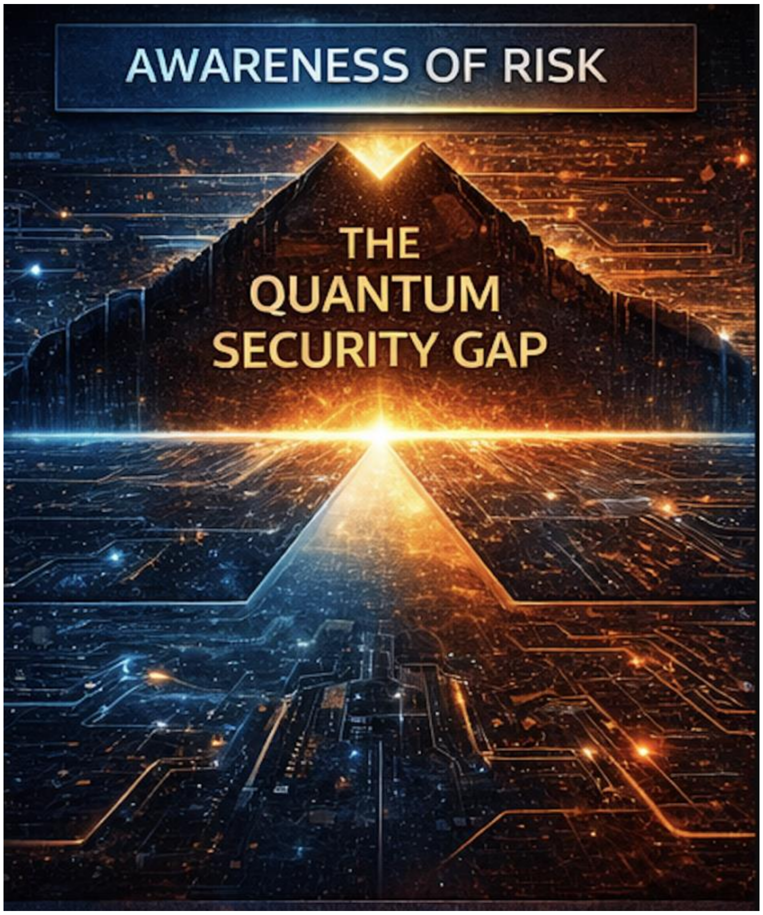


Figure 1. The Quantum Security Gap

Awareness of quantum computing risks to modern cryptographic systems is increasing across research, government, and industry communities. However, many institutions have not yet developed the governance structures, infrastructure inventories, and migration strategies required to transition to quantum-resistant cryptography. This gap between awareness and preparedness represents a growing security challenge.

Why Cryptographic Transitions Are Difficult

Replacing cryptographic systems across large organizations is inherently complex. Cryptography is not confined to a single application or technology platform. Instead, it forms the foundation of many digital systems and services.

Examples include:

- identity and authentication systems
- encrypted communications and TLS protocols
- software signing and firmware validation
- cloud infrastructure and secure APIs
- industrial control systems and embedded devices

These cryptographic dependencies are often distributed across infrastructure that has evolved over many years. In many cases, organizations do not maintain a complete inventory of where cryptographic functions are used.

Without this visibility, planning for migration becomes significantly more difficult.

Figure 2. Cryptographic Dependencies Across Digital Infrastructure

Cryptographic systems support many core components of modern digital infrastructure, including identity systems, cloud platforms, software signing, industrial control systems, and communications networks. Because cryptography is deeply embedded across these domains, transitioning to quantum-resistant security requires coordinated changes across multiple technology environments.

Infrastructure Lifecycles

Another challenge is the long operational lifecycle of many infrastructure systems.

Digital infrastructure supporting critical services often remains in operation for many years or even decades. Examples include energy systems, transportation networks, satellite communications, and industrial control environments.

Systems deployed today may continue operating long after quantum computing capabilities reach maturity. If these systems rely on cryptographic algorithms that become vulnerable to quantum attacks, replacing them may require substantial redesign or infrastructure upgrades.

Planning for cryptographic transitions must therefore account for these long infrastructure lifecycles.

Governance and Procurement Barriers

Institutional processes can also slow the pace of security transitions.

Technology decisions often involve multiple governance layers, including procurement requirements, vendor contracts, regulatory compliance, and budget planning cycles. Updating cryptographic systems may require coordination across numerous stakeholders and technology vendors.

In many cases, organizations depend on software platforms, hardware devices, and cloud services developed by external providers. Migration to quantum-resistant cryptography will therefore require vendor support and industry-wide adoption of new standards.

These governance and procurement factors can significantly influence the speed at which organizations are able to adapt their security infrastructure.

Strategic Implications

The quantum security gap carries several important strategic implications.

First, sensitive data protected by current cryptographic systems may be vulnerable to long-term exposure. If adversaries collect encrypted communications today and store them for future decryption, organizations could face significant data security risks.

Second, critical infrastructure systems that rely on long-lived hardware and software platforms may be difficult to upgrade quickly once quantum computing capabilities mature.

Third, countries and institutions that begin preparing earlier may gain strategic advantages in securing their digital infrastructure and protecting technological innovation.

Recognizing these risks highlights the importance of proactive planning.

Leadership Challenge

Preparing for the transition to quantum-resistant cryptography requires leadership awareness across both technical and governance domains.

Cybersecurity leaders, enterprise architects, infrastructure teams, and procurement organizations must work together to evaluate where cryptography is used and how future transitions can be managed.

Leadership engagement is essential because the transition will involve decisions related to infrastructure investment, technology procurement, and long-term risk management.

Without clear leadership ownership, preparation efforts may remain fragmented or delayed.

Looking Ahead

The transition to post-quantum cryptography will likely unfold gradually over the coming decade as standards mature and organizations begin integrating new cryptographic algorithms into their systems.

Closing the quantum security gap will require institutions to move beyond awareness and begin developing practical transition strategies.

Organizations that build visibility into their cryptographic dependencies, incorporate quantum-resistant security planning into infrastructure lifecycles, and coordinate across governance structures will be better positioned to manage the coming transition.

Ultimately, quantum security readiness represents a long-term infrastructure challenge rather than a short-term technical upgrade.

Key Takeaways

- A growing gap exists between awareness of quantum security risks and institutional readiness to address them.
- Cryptographic systems are deeply embedded across digital infrastructure.
- Long infrastructure lifecycles complicate rapid security transitions.
- Governance and procurement processes influence the pace of cryptographic migration.
- Closing the quantum security gap will require leadership awareness and coordinated planning.

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. 006

The Quantum Security Gap

Why Institutions Are Unprepared for the Cryptographic Transition

March 2026

SecureFi
Institute
An OnShoreWave Business

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.