Harvest Now, Decrypt Later

Understanding the Emerging Quantum Risk and What Organizations Must Do Now

Released in recognition of World Quantum Day, April 14, 2026

Executive Summary

Quantum computing is often framed as a future disruption.

This framing is incomplete.

One of the most significant risks associated with quantum computing is already in motion.

Sensitive data is being collected, stored, and preserved today with the expectation that it can be decrypted in the future. This model, referred to as **Harvest Now, Decrypt Later**, is defined as the collection of encrypted data today with the intent to decrypt it when future computational capability allows.

This is not a future breach scenario.

It is a delayed breach model.

Data that appears secure today may be exposed years from now without any new intrusion event.

Encryption protects content. It does not prevent the collection, storage, or future decryption of that content.

Most organizations cannot clearly answer a critical question:

Where are we exposed over time?

The gap is not in encryption technology alone. It is in visibility, ownership, and leadership readiness.

Organizations that begin addressing this now can reduce long-term exposure and position themselves for a secure transition. Those that delay risk carrying forward vulnerabilities that cannot be undone.

The Shift: From Real-Time Breach to Delayed Exposure

Traditional cybersecurity models focus on immediate threats.

Attackers breach systems, extract data, and exploit it in the present.

The **Harvest Now, Decrypt Later** model changes this paradigm.

Data does not need to be decrypted today to create risk.

It only needs to be collected and retained.

As computational capabilities evolve, previously protected data may become accessible.

This creates a new form of exposure:

Risk that is created in the present and realized in the future.

This shift requires organizations to move beyond real-time defense and begin managing long-term data exposure across the full lifecycle of information.

What Is Actually Happening Today

Across modern digital environments, data is constantly in motion.

It moves between users, applications, services, and infrastructure. It is encrypted, transmitted, stored, replicated, and backed up across distributed systems.

During this process, data may be intercepted, captured, and retained in encrypted form.

Nation-state actors and sophisticated adversaries operate with long time horizons. The collection of encrypted data is not opportunistic. It is strategic.

The urgency is not theoretical.

The U.S. government has already established direction on this issue, with transition timelines extending into the early 2030s. At the same time, industry leaders have signaled that meaningful quantum impact could emerge earlier, with some projections pointing to the end of the decade. This compresses the practical readiness window for organizations, requiring meaningful preparation well before the end of the decade.

Encryption protects confidentiality in the present. It does not prevent accumulation.

A Real-World Anchor: The Nature of Long-Life Data

The implications of long-term data exposure are not abstract.

In 2015, more than 21 million federal background investigation records were exfiltrated. These records included biometric data, financial history, foreign contacts, and detailed personal information.

This type of data does not lose value over time.

It becomes more valuable.

This is the nature of long-life data exposure.

If similar data is collected today in encrypted form, the risk is not whether it is accessed now.

The risk is whether it becomes accessible later.

What Data Is Most at Risk

Not all data carries equal long-term risk.

The most significant exposure lies in long-life data, including:

- National security and defense information
- Critical infrastructure systems and operational data

- Intellectual property and research
- Identity and personal data
- Financial and transactional records

The defining characteristic is persistence of value.

If collected today and decrypted in the future, this data can reveal capabilities, relationships, and decisions that remain relevant over time.

Organizations must begin classifying data based on how long it must remain protected, not just how sensitive it is today.

Why Current Cryptography Will Not Hold Over Time

Modern cryptographic systems are built on assumptions about computational difficulty.

Widely used methods such as RSA and elliptic curve cryptography depend on problems that are difficult for classical computers to solve.

Quantum computing introduces new computational approaches that challenge these assumptions.

While current systems remain secure against today's threats, they were not designed for future computational models.

This does not imply immediate failure.

It does mean that long-term protection cannot rely solely on existing approaches.

The timeline for practical quantum impact remains uncertain.

The exposure window does not.

Where Organizations Are Most Exposed

Exposure is broader and more distributed than most organizations realize.

High-risk areas include:

- Long-term data stores such as archives and backups
- Legacy systems that are difficult to modernize
- Third-party and supply chain environments
- Machine-to-machine communications and APIs
- Endpoints and edge systems
- Hybrid and multi-cloud infrastructure

Encrypted data is often assumed to be secure.

In reality, stored encrypted data may represent future exposure.

The challenge is compounded by limited visibility into where data resides, how it is protected, and who owns it.

The Visibility and Control Challenge

The most significant barrier to addressing this risk is not cryptography itself.

It is lack of visibility and control.

Organizations often lack:

- A complete inventory of cryptographic usage
- Clear ownership of data and encryption systems
- Insight into key management practices
- Visibility into dependencies across systems

Encryption is embedded across distributed environments.

Ownership is fragmented.

Tooling is incomplete.

This creates a condition where organizations cannot fully assess or manage their exposure.

The Transition Challenge

Post-quantum cryptography is no longer theoretical.

In 2024, NIST finalized the first post-quantum cryptography standards, FIPS 203, 204, and 205, providing tested, government-endorsed algorithms for organizations to begin adopting.

However, the transition is not a simple replacement.

It introduces:

- Larger key sizes
- Different performance characteristics
- Integration challenges across systems

This transition will impact identity systems, communications, applications, and infrastructure.

It will require coordination across technology, security, and leadership teams.

This is a multi-year effort.

This is not a technology upgrade.

It is a leadership and risk management challenge.

A Leadership Framework for Action

To move from awareness to readiness, organizations must approach this challenge systematically.

THREAT → IMPACT → GAP → RESPONSE → LEADERSHIP

- Threat: Understand how quantum computing changes risk
- Impact: Identify which data and systems are affected over time
- Gap: Assess visibility, ownership, and preparedness
- Response: Define actions across technology and governance
- Leadership: Align decision makers to execute

This provides a repeatable structure for managing long-term risk.

What Organizations Should Do Now

Organizations do not need to solve this immediately.

They do need to start.

Key actions include:

1. Commission a cryptographic inventory, a complete assessment of what encryption is in use, where it runs, and who owns it
2. Identify and classify long-life and high-value data
3. Assess exposure across systems, environments, and dependencies
4. Evaluate key management practices and control gaps
5. Begin planning for cryptographic agility, the ability to update cryptographic algorithms without rebuilding entire systems
6. Engage vendors and partners on post-quantum readiness

Early action reduces long-term risk and enables controlled transition.

Conclusion

The risk associated with quantum computing is not limited to the future.

It is already shaping how data is collected, stored, and exposed today.

Organizations that treat this as a future problem risk carrying forward vulnerabilities that cannot be undone.

Those that begin now can reduce exposure, strengthen resilience, and position themselves for the next phase of secure infrastructure.

The question is no longer whether quantum computing will impact security.

The question is whether organizations are prepared for the exposure that already exists.

SecureFi Institute's Certified in Quantum-Aware Cyber Risk program provides the framework organizations need to move from awareness to readiness. Learn more at securefi.com.

SecureFi Institute Research Executive Brief 011

Released in recognition of World Quantum Day, April 14, 2026

Harvest Now, Decrypt Later

Understanding the Emerging Quantum Risk and What Organizations Must Do Now

SecureFi Institute

SecureFi Institute focuses on the convergence of cyber, artificial intelligence, high-performance computing, and quantum technologies and their impact on secure infrastructure.

Through research, executive briefings, and training, the Institute helps organizations move from awareness to readiness.

For additional insights and research, visit securefi.com

Research. Awareness. Preparedness.

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.