Harvest Now, Decrypt Later

Understanding the Emerging Quantum Risk and What Organizations Must Do Now

Executive Summary

Quantum computing is often framed as a future disruption.

However, one of the most significant risks associated with it is already in motion.

Organizations, adversaries, and nation-states are collecting encrypted data today with the expectation that it can be decrypted in the future. This model, commonly referred to as “harvest now, decrypt later,” shifts the focus of security from present protection to long-term resilience.

The risk is not when quantum capabilities fully mature.
The risk is the data being generated, transmitted, and stored today.

Most organizations lack visibility into where cryptography is used, how keys are managed, and which data must remain secure over time. This creates a gap between current practices and future exposure.

Addressing this challenge requires early awareness, improved visibility, and a phased transition toward more resilient cryptographic approaches.

The Reality of the Threat

The “harvest now, decrypt later” model is straightforward.

Data is encrypted using current cryptographic methods and transmitted or stored within systems. That encrypted data can be intercepted, copied, and retained.

As computational capabilities evolve, particularly with the advancement of quantum computing, that stored data may become accessible.

This model changes how risk must be evaluated.

Encryption protects data today, but it does not guarantee long-term protection.

The threat is not theoretical. It is based on current data collection practices and the long-term value of information.

How Data Is Exposed Today

Encryption is widely used across modern systems, but it is not a single control.

It exists across multiple layers, including:

- Data in transit across networks
- Data stored in databases, files, and backup systems
- Identity and authentication systems using certificates and keys
- Applications and APIs exchanging data
- Cloud and hybrid environments

Each of these layers introduces potential exposure points.

Data in transit can be intercepted at network or endpoint levels.
Data at rest, particularly in archives and backups, can be stored for long periods of time.
Identity systems rely on cryptographic trust that may not hold indefinitely.

At the center of all of this is key management.

The strength of encryption depends not only on algorithms, but on how keys are generated, stored, and controlled. Weaknesses in key management can undermine otherwise strong systems.

What Data Is Most at Risk

Not all data carries equal risk.

The primary concern is data that retains value over time.

This includes:

- National security and defense information
- Critical infrastructure data
- Intellectual property and research
- Identity and personal data
- Financial and transactional records

This “long-life data” is particularly vulnerable because its value persists.

If collected today and decrypted in the future, it can reveal sensitive information, capabilities, and relationships.

Organizations must shift from thinking about data protection in the present to protecting data across its entire lifecycle.

Why Current Cryptography Will Not Hold

Modern cryptographic systems are built on assumptions about computational difficulty.

Asymmetric cryptography, including widely used methods such as RSA and elliptic curve cryptography, depends on problems that are difficult for classical computers to solve.

Quantum computing introduces new approaches that challenge these assumptions.

While current systems remain secure against today’s threats, they are not designed to withstand future computational models.

This does not mean immediate failure.

It means that long-term protection cannot rely solely on existing methods.

Where Organizations Are Most Exposed

Exposure is broader and more distributed than most organizations realize.

Key areas include:

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

In many cases, organizations assume that encrypted data is secure.

However, stored encrypted data may still be vulnerable over time.

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

The Visibility and Control Challenge

One of the most significant barriers to addressing this risk is lack of visibility.

Organizations often do not have:

- 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 across teams.

Tooling provides incomplete visibility.

This creates a situation where organizations cannot fully assess their exposure.

The issue is not weak encryption.

It is lack of visibility and control.

The Transition Challenge

Post-quantum cryptography is emerging as a solution.

New algorithms are being developed and standardized to resist quantum-based attacks.

However, the transition is complex.

Post-quantum cryptography is not a simple replacement.

It introduces:

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

The transition will impact communication protocols, identity systems, applications, and infrastructure.

It will require coordination across teams and alignment with evolving standards.

This is a multi-year effort.

What Organizations Should Do Now

Organizations do not need to solve this immediately.

But they do need to start.

Key steps include:

1. Build awareness and align leadership
2. Identify long-life and high-value data
3. Improve visibility into data, encryption, and key management
4. Assess exposure across systems and environments
5. Begin planning for transition and crypto-agility
6. Engage with vendors and partners on readiness

This approach allows organizations to move from awareness to action in a structured way.

Conclusion

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

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

Organizations that treat this as a future problem risk falling behind.

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

SecureFi Institute Research Executive Brief 011

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.