THOUGHT LEADERSHIP

Quantum Risk Is a Mission Risk

Securing mission infrastructure for the post-quantum era – why infrastructure will play a defining role in mission success

Prepared by Lumen Technologies
July 2026

Table of contents

Executive Summary

Adversaries are no longer waiting for quantum computing capabilities to mature. They are acting now.

Sensitive communications and mission-critical data are already being intercepted and stored with the expectation that future quantum capabilities will enable decryption. This "harvest now, decrypt later" dynamic introduces a time-delayed vulnerability that extends beyond current controls and into the long-term integrity of mission operations.[1]

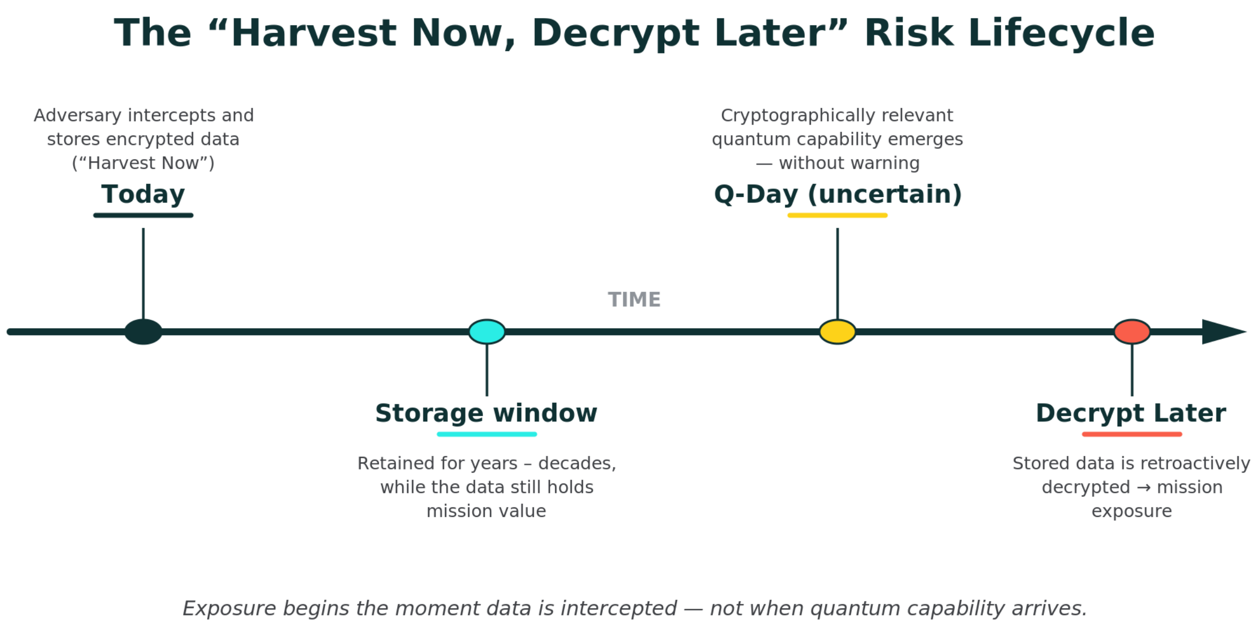

Figure 1. The "harvest now, decrypt later" risk lifecycle: data intercepted today is exposed retroactively once a cryptographically relevant quantum capability emerges.

At the same time, the timeline to quantum-enabled cryptographic disruption remains uncertain. It will not arrive as a clearly defined event, but as a threshold—one that, once crossed, renders widely used encryption methods ineffective without warning.[6]

This creates a structural problem. Most federal and defense networks were not designed to accommodate continuous cryptographic change. They rely on static encryption models and treat cryptography as an overlay rather than a foundational component of infrastructure.

The implications go beyond cybersecurity. When cryptographic assumptions fail, the impact is operational, affecting the reliability of communications, the integrity of data, and the ability to execute mission decisions with confidence.

The challenge is not choosing the right cryptographic approach in isolation. It is ensuring that the infrastructure supporting mission systems can accommodate continuous change in those approaches over time.

Addressing this challenge requires a shift from static architectures to adaptive infrastructure that can evolve as cryptographic requirements change, while helping minimize operational disruption. Organizations that begin this transition early can align modernization with mission priorities and maintain control over change. Those that delay will face compressed timelines, reduced flexibility, and increased operational risk.

> Quantum readiness is no longer a cybersecurity initiative—it is a mission-critical infrastructure requirement. – **Scott Barnett, VP Federal Sales, Lumen**

National Security Context: Why Action Is Required Now

Quantum computing is emerging as a domain of strategic competition, with direct implications for intelligence, cyber operations, and secure communications. Its impact lies not only in new capabilities, but in its potential to invalidate long-standing assumptions about how trust is established in digital systems.

Unlike other technology transitions, risk does not begin when quantum systems are operational. It begins when data is intercepted. Adversaries can collect and store encrypted data today, anticipating future decryption capabilities.

This creates a forward-facing exposure, particularly for federal and defense missions where data must remain secure for years or decades.

At the same time, infrastructure limitations constrain response. Most environments lack visibility into cryptographic dependencies, the ability to adapt at scale, and a clear path to prioritize modernization.[2]

These limitations are not the result of inaction. They reflect how infrastructure was originally designed—to support stability, not continuous transformation. As a result, organizations face a widening gap between the pace of change in the operating environment and the adaptability of existing infrastructure. The challenge is not simply the need for new cryptographic methods. It is the lack of an infrastructure model that can support their ongoing evolution.

That requirement points to a broader shift in how mission infrastructure must now be conceived.

> "The response must be structural: infrastructure that can support cryptographic change without compromising mission continuity."
>
> **– Scott Barnett, VP Federal Sales, Lumen**

The Shift: From Static Architecture to Adaptive Infrastructure

Addressing this challenge requires a fundamental change in how infrastructure is designed and operated.

Historically, networks have been optimized for stability, with changes introduced carefully and infrequently. This model assumes that underlying technologies—such as cryptographic standards—remain viable over extended periods. That assumption no longer holds. NIST finalized the first post-quantum cryptography standards in August 2024, establishing FIPS 203, 204, and 205 as an initial foundation for migration.[3] The algorithms are now defined, which means organizations can begin planning for the infrastructure changes required to support transition.

Infrastructure must now support continuous evolution. Cryptographic capabilities cannot remain fixed; they must be able to change without requiring full system redesign. This introduces a new requirement: **crypto-agility at the infrastructure level**.

Crypto-agility is not simply the ability to swap algorithms. It is the ability to maintain continuous visibility into where cryptography exists, understand its role in mission systems, and introduce changes in a controlled and coordinated manner. To support this, infrastructure must provide continuous visibility into dependencies, integrate cryptographic functions into the network, and enable phased transitions without disruption.

In this model, infrastructure is no longer a passive transport layer. It becomes an active mechanism for maintaining mission continuity as conditions evolve. The next step is to define what that infrastructure framework must contain.

An Infrastructure Framework for Quantum Readiness

A practical path forward requires an architectural framework that supports visibility, adaptation, and scale.

This begins with establishing a clear understanding of current state. Cryptographic dependencies are often distributed across applications, data flows, identity systems, and transport layers. Without visibility into these dependencies, modernization cannot be effectively prioritized. Once visibility is established, infrastructure must support controlled adaptation, enabling cryptographic changes to be introduced incrementally without requiring large-scale replacement.

A functional framework includes four core capabilities:

- **Discovery and inventory** to identify cryptographic exposure
- **Algorithm modernization** to transition critical systems to resilient methods
- **Layered protection** for environments requiring higher assurance
- **Advanced key management** for sensitive, long-lived data

These are not isolated solutions. They form a coordinated system that allows organizations to evolve infrastructure progressively while maintaining continuity. The goal is not to deploy a single enduring solution, but to build infrastructure capable of continuous evolution. That framework becomes meaningful only when it can be translated into a practical path for infrastructure transformation.

The Infrastructure Transformation Journey

Transformation must occur as a controlled progression, not a disruptive event.

The first phase is understanding—establishing visibility into cryptographic dependencies and their role in mission operations. The second phase is prioritization—aligning modernization efforts based on mission criticality and data longevity. The third phase is controlled adaptation, introducing new capabilities alongside existing systems, allowing infrastructure to evolve incrementally. The final phase is operationalization, in which cryptographic evolution becomes part of ongoing operations rather than a periodic transformation effort.

This progression enables organizations to manage change proactively. Instead of responding to external pressures, they align infrastructure evolution with mission priorities and maintain control over execution. The value of that progression becomes clearest when measured in mission terms.

Mission Outcomes

The purpose of infrastructure transformation is not technical alignment. It is mission continuity.

An adaptive infrastructure model enables organizations to sustain operations even as underlying assumptions change.

In practical terms, organizations are better positioned to maintain operational continuity as cryptographic requirements evolve and can help preserve data integrity over extended timelines as standards change.

It also means decision assurance: mission leaders can maintain greater confidence in the accuracy and reliability of the information driving critical decisions. The same adaptability supports operational resilience, helping systems to function effectively in environments where disruption and uncertainty are expected rather than assumed away.

And because change is introduced deliberately, organizations retain a controlled transition—the ability to modernize on their own timelines, aligned with mission priorities rather than external pressure. These outcomes shift the role of infrastructure from providing stability to sustaining operations in dynamic conditions, and they become more concrete when examined through the lens of actual mission environments.

Mission impact – ready vs. not ready

Illustrative, unclassified archetypes – not tied to any specific system, program, or operation.

Mission	If you're quantum-ready	If readiness lags
Commander & C2	The common operating picture can remain reliable through cryptographic change; decisions rest on data whose integrity holds even as standards shift.	Quiet erosion of confidence in the picture – at the moment decisions can't wait – as the cryptography beneath C2 falls behind.
Warfighter at the edge	Cryptography evolves without breaking the comms that fires, ISR, and blue-force tracking depend on, even in denied or degraded conditions.	Data harvested from a forward network today is intercepted now and decrypted later, turning past coordination into an adversary's advantage.
Intelligence Community	Sources, methods, and analytic product can be better protected across the decades those secrets must hold.	Harvest-now-decrypt-later exposes intelligence years after collection – a decades-delayed breach you can't detect today.

Defense Use Cases

Adaptive infrastructure applies across a range of mission environments.

Classified network modernization. Legacy systems can be modernized incrementally, while helping maintain operational continuity while enabling infrastructure to evolve. The alternative is a forced, high-risk cutover under time pressure – the kind mission systems can least afford.

Multi-site mission operations. Distributed environments—spanning headquarters, regional facilities, forward operating environments, and partner sites—can maintain coordination and communication while aligning infrastructure capabilities to mission sensitivity.

High-volume data movement. Data flows can be designed to remain reliable and usable even as underlying cryptographic methods evolve.

Coalition and partner sharing. Interoperability can be supported across organizational boundaries—including other agencies, allied nations, and approved contractors without compromising operational integrity. Without it, the price of interoperability becomes exposure: data shared today that a partner's weaker cryptography could surrender to decryption later.

Hybrid and cloud environments. Infrastructure can help support consistent operation across distributed architectures without disrupting workflows.

Edge and mobility operations. Systems can be designed to remain functional in constrained environments where centralized control is not possible. For the warfighter, that is the difference between trusted comms at the edge and data that quietly becomes tomorrow's targeting intelligence.

Across these use cases, the common requirement is adaptability—ensuring infrastructure that can support mission operations regardless of changing conditions. That operational relevance must then be matched by practical evidence that the transition can be measured, validated, and executed with confidence.

Proof Points and Validation

Infrastructure transformation must be validated through practical execution.

The first step is establishing baseline, moving from assumptions to measurable understanding of cryptographic exposure.

The next step is validating change within active environments. Targeted implementations demonstrate that new capabilities can coexist with legacy systems without disrupting operations. From there,

Capabilities can be scaled across environments, creating a repeatable model for infrastructure evolution. Federal direction reinforces the same conclusion. NIST's post-quantum cryptography standards, the NSA's CNSA 2.0 transition guidance, the 2022 Quantum Computing Cybersecurity Preparedness Act, and the National Strategy on Quantum-Resilient Cryptography all signal that existing cryptographic models will not remain sufficient indefinitely.[3] For national security systems, CNSA 2.0 directs completion of the transition to quantum-resistant algorithms by 2033.[4] The mandate is increasingly clear; what organizations can still control is how deliberately they prepare, validate, and execute the transition.

Thought Leadership: Infrastructure Will Define Mission Success

Every major shift in computing has ultimately redefined infrastructure—not immediately, and not always visibly at first, but inevitably. Network architectures evolve when underlying assumptions change, whether those assumptions relate to scale, performance, or trust. Quantum computing represents one of those shifts. Quantum computing does not simply introduce new capabilities, it changes the assumptions on which digital systems depend. The response cannot be limited to selecting new cryptographic methods. It must address the infrastructure that supports them.

Organizations that treat quantum readiness as a discrete upgrade will face increasing complexity and constrained options. Each change will become more difficult to implement without disruption. Those that address the challenge at the infrastructure level create a different trajectory: they enable continuous evolution, allowing systems to adapt without compromising mission operations. This is the difference between reacting to disruption and absorbing it.

This represents a redefinition of reliability. Infrastructure will determine whether organizations can manage this transition—on their own terms, aligned to mission priorities. The question is no longer whether infrastructure will evolve, but whether that evolution will be deliberate or imposed. The future of cryptography will be defined by the infrastructure that enables it to change.

Moving Forward

The transition to quantum-resilient infrastructure begins with understanding. Organizations must establish a clear view of their current environment—where cryptographic dependencies exist and how they support mission systems. From that foundation, they can define a path forward by prioritizing based on mission impact, introducing change incrementally, and maintaining operational continuity.

The advantage available today is time. Acting early allows transformation to occur under controlled conditions; delaying reduces flexibility and increases the likelihood of disruption.

This is not simply a technical consideration. It is an infrastructure leadership responsibility. Decisions made now will determine whether mission environments remain viable as conditions evolve. The objective is not to predict the future, but to ensure infrastructure is prepared to operate within it.

> " The agencies that treat quantum readiness as an infrastructure decision today are the ones that will still hold decision advantage when the threshold is crossed."
>
> – **Scott Barnett, VP Federal Sales, Lumen**

References

1. CSO Online. *Reap Now, Decrypt Later: The Cybersecurity Challenge in the Quantum Age.*

2. ISACA. *Organizations Lack a Quantum Computing Roadmap, ISACA Finds.*

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

4. National Security Agency (NSA). *Commercial National Security Algorithm Suite (CNSA 2.0).*

5. Global Risk Institute & Evolution Q. *Quantum Threat Timeline Report.*

6. U.S. Office of the National Cyber Director. *National Strategy on Quantum-Resilient Cryptography.*

About Lumen

This paper reflects the Lumen perspective on preparing mission infrastructure for the post-quantum era. Lumen works with federal and defense organizations to build adaptive, quantum-ready networks that evolve with the threat—without disrupting the mission.

Why Lumen?

Lumen operates one of the North America's most deeply connected networks—engineered to carry mission-critical traffic for government and defense customers, and to help agencies modernize cryptographic infrastructure without disrupting the mission.

866-352-0291 I lumen.com I info@lumen.com