The Quantum Threat: Future-Proofing Your Archive Security

The cybersecurity landscape faces an unprecedented challenge that demands immediate attention despite seeming years away: quantum computing's ability to break current encryption standards. The median estimate among experts is that within 15 years, a quantum computer will be able to break RSA-2048 in 24 hours, according to the Global Risk Institute's "Quantum Threat Timeline Report 2024." While this timeline may appear distant, the threat is active today through a strategy cybersecurity experts call "harvest now, decrypt later" (HNDL)—where adversaries steal encrypted data now and wait for quantum computers powerful enough to decrypt it. Organizations must act immediately to protect their archives, with optical storage technologies offering unique advantages in mitigating this quantum threat.

The Quantum Computing Threat Landscape

Quantum computers represent a fundamental shift in computational capability. Unlike classical computers that process information as binary bits (zeros and ones), quantum computers use qubits that can exist in multiple states simultaneously through a property called superposition. This enables them to solve certain mathematical problems—including the cryptographic algorithms protecting today's data—exponentially faster than conventional computers.

In August 2024, the U.S. National Institute of Standards and Technology (NIST) finalized its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer. These post-quantum cryptography (PQC) standards—including CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+—represent the culmination of an eight-year global competition to develop quantum-resistant encryption methods. NIST mathematician Dustin Moody, who heads the PQC standardization project, encourages system administrators to start integrating them into their systems immediately, because full integration will take time.

The urgency extends beyond theoretical concerns. Google's announcement of its Willow chip at the end of 2024 represents a significant milestone, promising reduced noise and fewer errors as the number of qubits grows—a necessary step to advance toward advanced quantum computing. While experts debate exact timelines, the progression is

unmistakable. The Global Risk Institute estimated in 2024 that by 2034, there is between a 17% and 34% chance that a cryptographically relevant quantum computer (CRQC) would exist capable of breaking RSA 2048 in 24 hours, with the probability increasing to 79% by 2044.

The Harvest Now, Decrypt Later Threat

The most pressing aspect of the quantum threat is not future decryption capabilities—it's the data being stolen today. Nation-state adversaries and other bad actors are stealing sensitive information now, with the intent to decrypt it later using quantum tools once available, in a tactic known as "harvest now, decrypt later" (HNDL) attacks.

A Deloitte poll finds that a little over half of IT professionals surveyed say their organizations are presently at risk of HNDL attacks, yet fewer than half are presently on top of their analysis of this emerging cyber risk. More concerning, approximately 11% indicated that it would take an actual cyber incident—the point at which it is far too late—before leadership would act on the threat.

The Federal Reserve Board has issued stark warnings about HNDL risks. Their 2025 analysis emphasizes that "harvest now, decrypt later," represents a present, active, and in some circumstances unavoidable data privacy risk posed by future-state quantum computers. Once encrypted data is captured, no future encryption upgrade can retroactively protect it—the data remains vulnerable until quantum computers can decrypt it.

For long-term archives, this creates a particularly acute challenge. Medical records, financial transactions, legal documents, and proprietary research that must be retained for decades face exposure when quantum decryption becomes viable. Organizations implementing archive solutions today must consider not just current encryption standards but the quantum threat to data that will remain archived for 20, 50, or even 100 years.

Post-Quantum Cryptography: The Primary Defense

The cybersecurity community's primary response to the quantum threat centers on post-quantum cryptography. KPMG research in collaboration with Germany's Federal Office for Information Security found that 95 percent of respondents believe quantum computing's relevance and potential impact on today's cryptographic security systems is "very high or

high", yet only 25 percent say the threat is currently being addressed in their risk management strategy.

Deloitte emphasizes that while upgrading cryptography to protect against quantum computers requires a comprehensive effort, given sufficient time, it should be a relatively straightforward operation. Initial steps include establishing governance, understanding cryptographic exposure, prioritizing remediation efforts, and building comprehensive roadmaps for internal updates and vendor compliance.

Major technology companies are already implementing post-quantum encryption. Chrome began adopting NIST-approved post-quantum encryption on desktop in September 2024, while Microsoft updated its core crypto library. However, the transition will take years. The National Security Memorandum 10 (NSM-10) sets a clear deadline for full migration to PQC by 2035, requiring all cryptographic systems used by federal agencies to be quantum-resistant.

How Optical Archive Solutions Mitigate Quantum Threats

While post-quantum cryptography addresses ongoing encryption needs, optical data archive solutions offer unique advantages for long-term data preservation in the quantum era. These benefits stem from fundamental architectural differences between optical storage and traditional magnetic or semiconductor-based systems.

Physical Immutability and Air-Gap Protection:
Optical storage technology writes data to physical media using laser-induced changes in material structure. Once written, the data cannot be altered or encrypted by any software command, including quantum algorithms. This physical immutability provides absolute protection against quantum-enabled tampering or re-encryption attempts. When combined with air-gapped architectures that maintain complete network isolation, optical archives eliminate remote attack vectors entirely—quantum-powered or otherwise.

Elimination of Ongoing Encryption Dependencies:
Traditional archive systems that rely on encrypted data storage face the quantum dilemma: data encrypted with today's algorithms will be vulnerable when quantum computers mature. Optical archives can store data in unencrypted or minimally encrypted formats on physically isolated media, eliminating future decryption vulnerabilities. The physical and administrative access controls protecting the media provide security without relying on encryption algorithms that quantum computers might compromise.

Long-Term Data Integrity Without Re-Encryption:
Optical media maintains data integrity for 50-100 years without active intervention or periodic re-encryption. This longevity means organizations can archive data today with confidence that it remains protected throughout its retention period without requiring quantum-resistant encryption upgrades. The physical stability of optical storage eliminates the migration and re-encryption cycles that create quantum vulnerability windows in traditional archives.

Reduced Attack Surface:
Optical archives operate with minimal network connectivity and limited software dependencies compared to traditional storage systems. This reduced attack surface makes them inherently resistant to sophisticated attacks, including those leveraging quantum computing capabilities. The technology's simplicity—data written to physical media and stored offline—provides security through isolation rather than algorithmic complexity.

Compliance and Legal Discovery Benefits:
For organizations in regulated industries, optical archives provide verifiable immutability that satisfies compliance requirements while mitigating quantum risks. Legal discovery and audit processes can proceed with confidence that archived data has not been altered, encrypted, or compromised—regardless of advances in quantum computing capabilities.

Complementary Mitigation Strategies

Organizations should implement comprehensive approaches combining multiple quantum threat mitigation strategies:

Quantum Key Distribution (QKD):
QKD uses quantum mechanical properties to detect eavesdropping attempts, providing theoretically unbreakable encryption for data transmission. While implementation remains expensive and technically challenging, advances in QKD-on-a-chip technology and satellite communications are improving viability for critical applications.

Hybrid Cryptographic Approaches:
Combining traditional encryption with post-quantum algorithms provides layered security during the transition period. This approach maintains backward compatibility while adding quantum resistance, enabling gradual migration without leaving systems exposed.

Cryptographic Agility:
Implementing systems capable of rapidly switching between cryptographic algorithms

enables organizations to respond quickly as quantum threats evolve. This flexibility proves particularly valuable given uncertainty about quantum computing timelines and potential breakthroughs.

Data Classification and Prioritization:
Not all data requires the same level of quantum-resistant protection. Organizations should identify information with long-term sensitivity requirements and prioritize quantum-safe solutions for those data sets. Archives containing personally identifiable information, trade secrets, and classified material warrant immediate attention.

Implementation Roadmap

Organizations should begin quantum threat mitigation immediately through structured approaches:

Assessment Phase (Months 1-3):
Inventory all systems using encryption, identify data with long retention requirements, evaluate quantum vulnerability exposure, and establish governance frameworks for quantum readiness initiatives.

Planning Phase (Months 4-6):
Develop comprehensive migration roadmaps, select appropriate post-quantum algorithms, identify systems suitable for optical archive migration, and establish vendor requirements for quantum-resistant solutions.

Implementation Phase (Months 7-24):
Begin phased migration starting with highest-risk data, implement optical archives for long-term retention requirements, upgrade encryption systems to post-quantum standards, and conduct regular testing and validation.

Ongoing Operations (Year 2+):
Maintain cryptographic agility, monitor quantum computing developments, update strategies as threats evolve, and ensure vendor compliance with quantum-resistant standards.

Conclusion

The quantum threat to encryption is not theoretical—it is active today through harvest now, decrypt later attacks targeting data that will remain sensitive for years or decades.

Organizations cannot afford to delay quantum readiness initiatives until quantum computers become operational; by then, years of harvested data will face immediate exposure.

Optical data archive solutions provide unique advantages for mitigating quantum threats to long-term data preservation. Their physical immutability, air-gapped isolation, and elimination of encryption dependencies offer protection that remains effective regardless of quantum computing advances. When combined with post-quantum cryptography for active systems, hybrid encryption approaches, and cryptographic agility, optical archives form critical components of comprehensive quantum threat mitigation strategies.

The organizations that act now to implement quantum-resistant archive solutions—particularly optical technologies offering inherent protection against quantum threats—will be best positioned to weather the coming quantum revolution while maintaining the security and integrity of their most sensitive long-term data assets.

Sources Cited:

- National Institute of Standards and Technology (NIST): Post-Quantum Cryptography Standards, August 2024
- Global Risk Institute: Quantum Threat Timeline Report 2024
- KPMG: Quantum Computing and Cybersecurity Research, 2024
- Deloitte: Quantum Computing and Cybersecurity Insights, 2024
- Federal Reserve Board: "Harvest Now Decrypt Later" Analysis, 2025
- Dark Reading: Quantum Computing Advances in 2024
- SecurityWeek: Cyber Insights on Quantum Threats
- Cisco Newsroom: Post-Quantum Cryptography Standards