Infographic

Quantum Computing Cyber Risk

ecfirst

Q-Day

The period when quantum computers can break standard encryption: a window, not a date

THE WALL STREET JOURNAL.

Why Quantum Computing Is a Threat to Cybersecurity

The math behind standard encryption will be no match for quantum computers, forcing organizations to rethink cybersecurity.

Quantum Cyber Resilience

- **Lattice-Based Cryptography:** Designed to resist attacks from both classical and quantum computers.
- **Hybrid Approach:** Combines classical and Post-Quantum Cryptography (PQC) to support a secure transition during migration.
- **Hamming Quasi-Cyclic (HQC):** A code-based Key Encapsulation Mechanism (KEM) selected by NIST as an additional backup algorithm.

Quantum Readiness

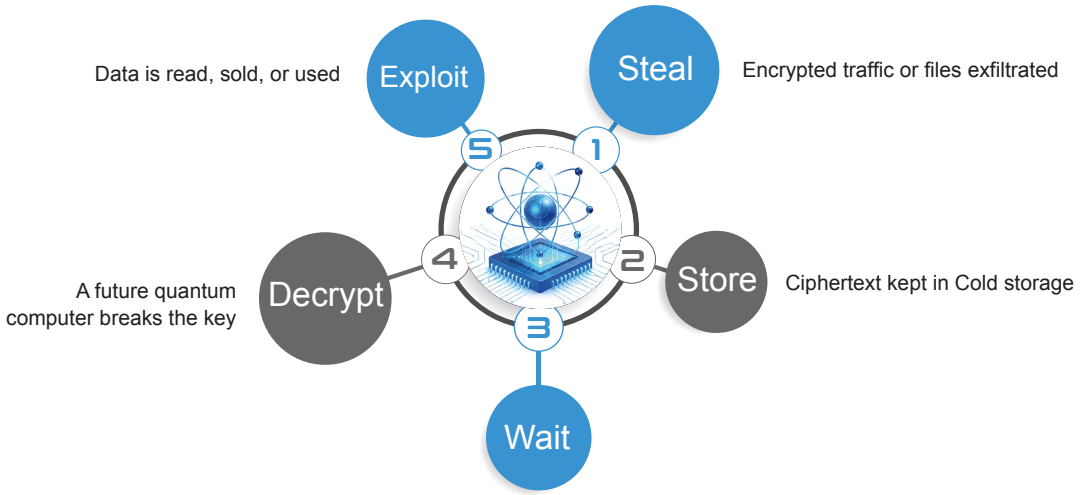
- Build a quantum-readiness roadmap.
- Inventory all cryptographic assets across apps, hardware, and vendors.
- Prioritize high-risk data and systems.
- Engage vendors on PQC plans early.
- Pilot hybrid cryptography before rollout.
- Build crypto-agility for future swaps.

Quantum Threat

- Quantum computers solve certain math problems far faster than classical ones.
- Shor's algorithm can factor large numbers, breaking RSA, Diffie-Hellman, and ECC.
- Broken cryptography could enable fake digital signatures and undermine trust.

Harvest-Now, Decrypt-Later

- Attackers steal encrypted data now, hoping to decrypt it later.
- Long-lived data - IP, health records, government intel — is most exposed.



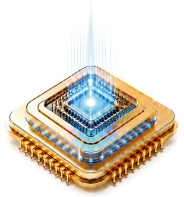
Quantum computing matures over years

Data Intercepted or stolen now can remain a liability for years before it is ever decrypted.

Global AI Cyber Defense Thought Leader

Infographic

Quantum Computing Cyber Risk



ecfirst

Key Timeline

2029
IBM targets commercial fault-tolerant quantum systems; Google, Microsoft, Cloudflare target full PQC migration

2030
Federal high-value assets migrated for **key establishment**; contractor PQC regulations issued; NIST begins deprecating RSA-2048

2031
Federal high-value assets migrated for **digital signatures**

2035
NIST target for full phase-out of legacy public-key algorithms

Source Quantum Computing Cybersecurity Preparedness Act (6 USC §1526); Executive Order "Securing the Nation Against Advanced Cryptographic Attacks," June 22, 2026.

NIST Quantum Standards

Standard	Algorithm	Purpose
FIPS 203	ML-KEM (CRYSTALS-Kyber)	Key encapsulation / encryption
FIPS 204	ML-DSA (CRYSTALS-Dilithium)	Digital signatures
FIPS 205	SLH-DSA (SPHINCS+)	Backup hash-based signatures
FIPS 206 (Draft)	FN-DSA (FALCON)	Compact signatures for constrained devices

Acronyms

CISA Cybersecurity & Infrastructure Security Agency

ECC Elliptic Curve Cryptography

FN-DSA NTRU-Lattice Signatures (FALCON, draft FIPS 206)

HQC Hamming Quasi-Cyclic backup KEM

HNDL Harvest-Now, Decrypt-Later

HSM Hardware Security Module

IAM Identity and Access Management

KEM Key Encapsulation Mechanism

ML-DSA Module-Lattice Signatures (Dilithium)

ML-KEM Module-Lattice KEM (Kyber)

PQC Post-Quantum Cryptography

Q-Day Day quantum computers break standard encryption

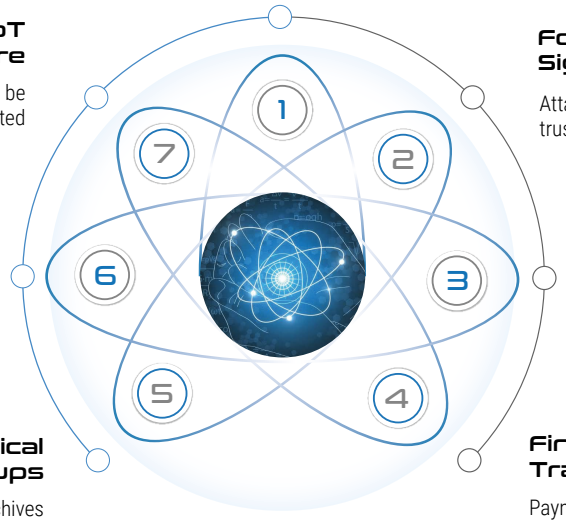
RSA Rivest Shamir Adleman

SLH-DSA Stateless Hash-Based Signatures (SPHINCS+)

91% of security pros lack a formal quantum roadmap.

Harvest-Now Decrypt-Later

Stolen data decrypted once quantum matures



Legacy IoT Exposure
Old devices can't be updated

Forged Digital Signatures
Attackers impersonate trusted vendors/software

IAM/Certificate Failure
Attackers impersonate identities

Secure Boot Compromise
Firmware trust checks bypassed

Exposed Historical Backups
Old encrypted archives become readable

Financial Transaction Risk
Payment and ledger integrity threatened

Global AI Cyber Defense Thought Leader