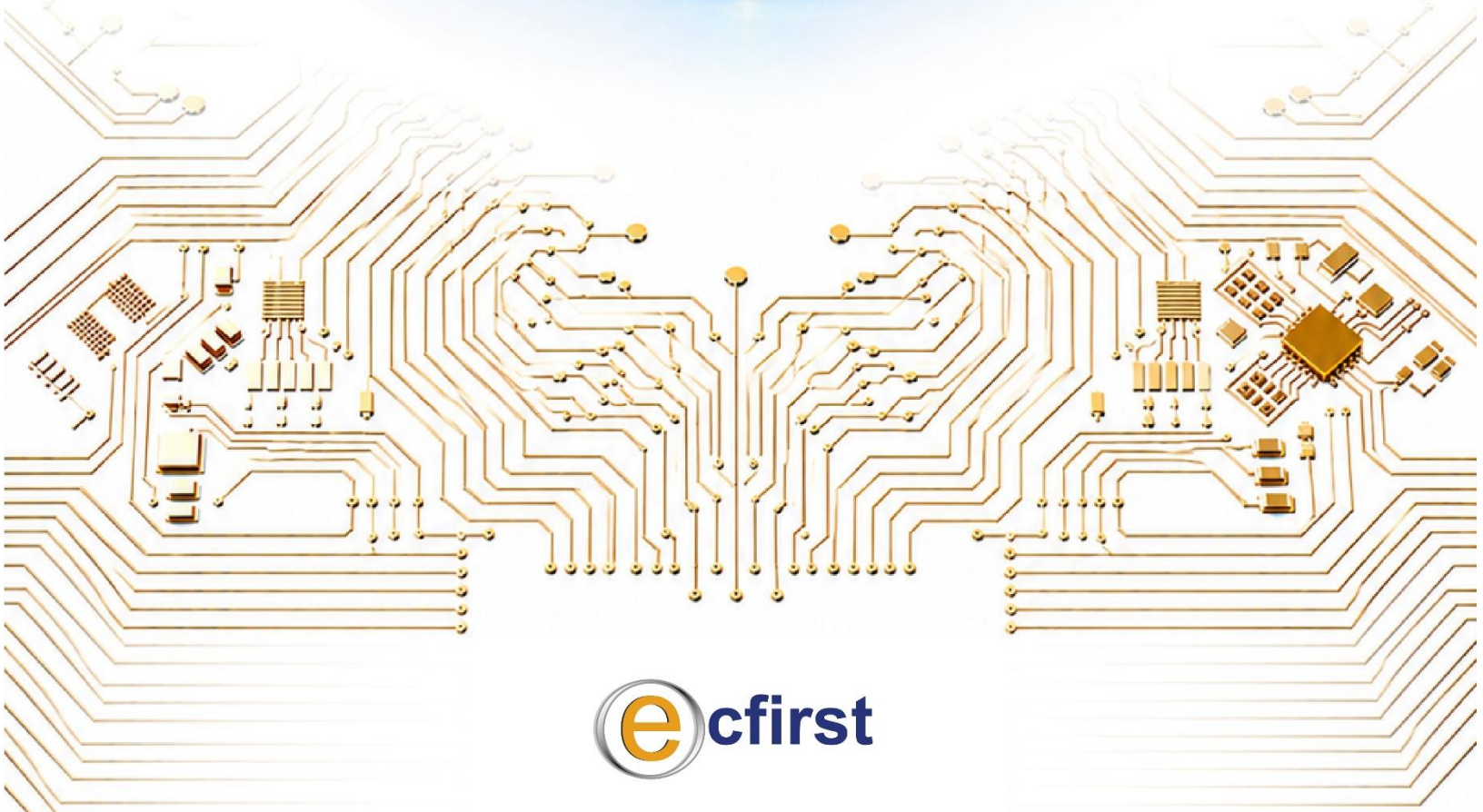
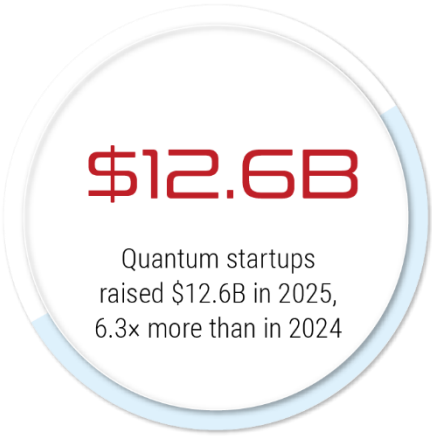
Quantum Cyber Risk



ecfirst

You assess risk for a living. Most findings on your worksheets are fixable in a quarter. Quantum computing is different: a **dated, funded engineering program** that will make the cryptography underneath nearly everything you assess obsolete, on a timeline the industry is now publishing openly

Today's security depends on mathematical loc ordinary computers to pick. Encrypting data with a public key means an attacker woul bers were multiplied together to produce it, a vexing task classically. But quantum comp rns and excel at factoring very large numbers, which is why **RSA, Diffie-Hellman, a** HTTPS, VPNs, code signing, and most digital certificates — are exposed.[1] Symmetric encryption (AES) and password hashing are far more resilient and need only modestly longer keys.



What Actually Breaks: Eight Exposure Categories

"Encryption breaks" is too abstract to scope an assessment against. In practice, the failure surfaces in eight distinct ways, and each maps to a different part of an environment.[2]

Exposure	What It Means in Practice
Broken public-key encryption	RSA, Diffie-Hellman, and ECC become breakable — the foundation beneath TLS, VPNs, and key exchange
Harvest-now, decrypt-later	Data stolen today is decrypted once quantum capability matures
Forged digital signatures	Attackers impersonate trusted vendors and sign malicious software as legitimate
Secure boot compromise	Firmware trust checks are bypassed, undermining every control layered above them
Financial transaction risk	Payment authorization and ledger integrity are threatened
Exposed historical backups	Old encrypted archives become readable retroactively
IAM and certificate failure	Certificate-based authentication is spoofed; attackers impersonate identities
Legacy and IoT exposure	Embedded, medical, and building systems that cannot be updated stay vulnerable permanently


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.

"Q-Day": A Window, Not a Date

"Q-Day" is the hypothetical moment quantum computers become powerful enough to break standard-key encryption. There isn't expected to be one fixed date; it is likely to occur over several months or years, according to Scott Aaronson, a computer-science professor at the University of Texas at Austin.[1] Quantum computers exist today but mostly under highly restricted lab conditions, still ill-equipped for everyday practical use. What has changed is that the milestones are now dated and public: **IBM has said it plans to deliver the first quantum computer for real-world applications by 2029**.

2029

IBM's target for a real-world quantum computer

In October 2025, Google's Quantum Echoes algorithm ran ***13,000 times*** faster than the best classical algorithm on one of the world's fastest supercomputers — the first peer-reviewed, verifiable quantum advantage.[14]

Harvest-Now, Decrypt-Later: The Risk That Is Already Here

The single most important point for a client conversation is that this risk does not wait for Q-Day. In a **harvest-now, decrypt-later** (HNDL) attack, adversaries download large sets of encrypted data they cannot crack today and unlock them once quantum algorithms are good enough.[1] The theft has already happened; only the decryption is on a delay.

That's particularly threatening to intellectual property and sensitive government intelligence, which remain valuable long after they are harvested.

— Andrew McLaughlin, Chief Operating Officer, SandboxAQ (WSJ)

84%

of organizations believe encrypted data is already vulnerable to harvest-now, decrypt-later attacks

Physical vs. Logical Qubits

A logical qubit bundles many error-prone physical qubits into one reliable unit, that's what capability really tracks.

The attack runs in five stages: **steal** (traffic or files exfiltrated), **store** (ciphertext held in cold storage, often for years), **wait** (quantum computing matures), **decrypt** (a future machine breaks the key), and **exploit** (the data is read, sold, or used). Only the first stage requires anything of the attacker today, which is what makes the economics so favorable — storage is cheap and intelligence-grade data holds its value.[2]

For any assessment touching data with a multi-year sensitivity window — PHI, PII, IP, legal and M&A records, defense intelligence — **HNDL exposure is a present-tense finding**, regardless of when Q-Day actually lands.

The Fix: Post-Quantum Cryptography

Quantum-safe encryption already exists. The leading approach uses **lattice-based protocols**, which secure data with geometry-based problems that are difficult for both standard and quantum computers to solve.[1] NIST finalized three post-quantum standards on August 13, 2024 — **FIPS 203 (ML-KEM)** for key encapsulation, **FIPS 204 (ML-DSA)** for digital signatures, and **FIPS 205 (SLH-DSA)** as a hash-based backup. A fourth signature standard, **FIPS 206 (FN-DSA, based on FALCON)**, remains in draft, and NIST selected **HQC** in March 2025 as a backup key-encapsulation mechanism built on different math than ML-KEM.[3] Because migration can take years, a **hybrid approach** combining existing and post-quantum cryptography is widely recommended as a bridge during the transition, per Ali El Kaafarani, chief executive of PQShield.[1]

The clock is explicit, and it is now law. The **Quantum Computing Cybersecurity Preparedness Act** (6 USC §1526) requires federal agencies to inventory quantum-vulnerable systems, and a June 2026 executive order sets the dates: federal high-value assets must migrate for **key establishment by December 31, 2030** and **digital signatures by December 31, 2031**, with contractor compliance regulations due by the end of 2030.[6] Separately, NIST IR 8547 deprecates 112-bit-security algorithms such as RSA-2048 beginning in 2030 and disallows them by 2035.[4]

Google researcher Craig Gidney cut the estimated cost of breaking RSA-2048 from 20 million noisy qubits in 2019 to under 1 million in 2025 — a twentyfold drop in six years.[15]

Who Is Already Moving

More than 300 organizations worldwide have now adopted quantum computing, and a third of the largest adopters spend $10 million or more a year on it — quantum readiness is no longer optional for the clients you assess.[12]

Organization	Post-Quantum Status
Google, Cloudflare, Microsoft	Aim to use quantum-resistant encryption across all products, services, and core infrastructure by 2029
Signal, Apple iMessage	Already using post-quantum end-to-end encryption
WhatsApp, Messenger (Meta)	In the process of deploying post-quantum features
Keeper Security, 1Password	Have adopted quantum-resistant algorithms
Financial institutions, central banks, card networks	Adopting post-quantum protocols to protect sensitive data

Global quantum investment reached $12.6 billion in 2025 — more than six times the roughly $2 billion raised in 2024.[1,2,12] A 2025 Global Risk Institute survey of experts now rates a code-breaking quantum computer "quite possible" (28–49%) within 10 years and "likely" (51–70%) within 15.[13]

Yet a Trusted Computing Group survey of 1,500 security professionals across the U.S. and Europe found **91% have no formal roadmap** to protect against quantum threats, and 81% believe their crypto libraries and hardware security modules are unprepared for migration.[1,5] That gap between awareness and action is where an assessor adds the most value.

Spotlight: Why IBM Is the Company to Watch

IBM holds a position no other company does: it is simultaneously the most transparent builder of the hardware that creates this threat and a co-author of the standards that neutralize it. IBM Research cryptographers in Zurich co-developed **CRYSTALS-Kyber and CRYSTALS-Dilithium**, the basis for NIST's ML-KEM and ML-DSA standards.[7] On hardware, IBM's Nighthawk processor (120 qubits, 218 tunable couplers) shipped in late 2025, and its Loon module demonstrated the components for fault tolerance — including error-correction decoding under 480 nanoseconds — a full year ahead of schedule. IBM targets verified quantum advantage by the end of 2026 and its fault-tolerant **Quantum Starling** system by 2029.[8,9]

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

Starling
Fault-tolerant, 2029

IBM's first fault-tolerant machine, 200 logical qubits running 100 million gates.

91%

of security pros have no formal quantum roadmap

IBM is the only company positioned to rapidly invent and scale quantum software, hardware, fabrication, and error correction.

— Jay Gambetta, Director of IBM Research

IBM also ships the most complete migration toolkit on the market — **Guardium Cryptography Manager** for cryptographic asset discovery, **Quantum Safe Explorer** for source-code scanning, and **Quantum Safe Remediator** for hybrid, crypto-agile remediation — plus quantum-safe capability already built into IBM z16, Power10, and IBM Cloud.[10] For an assessor, that dual position is a practical gift: one company's public roadmap tracks both the threat and the fix.

IBM's quantum processors run below 15 millikelvin, over 180x colder than deep space

A separate DigiCert survey of 1,001 security leaders found 84% believe some of their encrypted data is already exposed to harvest-now, decrypt-later attacks, and while 87% are working on post-quantum cryptography, only 7% have deployed it across most of their certificates.[16]

What This Means for Your Assessments

CISA, the NSA, and NIST jointly direct organizations of every size to build a quantum-readiness roadmap, complete a cryptographic inventory, and engage vendors on post-quantum plans now rather than at the last minute.[11] Translated into fieldwork:

$1.3-2.7T

Potential economic value of quantum technology by 2035

- **Add a cryptographic asset inventory** to standard fieldwork — algorithms, key lengths, and protocols across applications, firmware, certificates, VPNs, HSMs, and backup/archive systems. Most clients genuinely do not have one, making this the highest-leverage finding available.
- **Ask directly about roadmap, ownership, and budget.** With 91% of organizations lacking a formal plan, the 2029–2030 vendor and federal milestones give you a defensible benchmark to measure a client against.
- **Prioritize by data longevity.** Flag long-lived PHI, PII, IP, and government or defense data as HNDL-exposed today — not at some future Q-Day.
- **Pilot hybrid cryptography and build crypto-agility** before full rollout, so systems stay protected during migration and future algorithm swaps are routine rather than disruptive.
- **Use vendor commitments as third-party risk checkpoints.** IBM's, Microsoft's, Google's, and Cloudflare's public 2029 targets are a fair, sourced bar to hold a client's own vendors and cloud providers to.
- **Make quantum readiness a standing risk-register item.** This is a multi-year migration; your value compounds if you are the one tracking it release over release.

What to tell people who ask about their personal data

The transition will largely happen behind the scenes, handled by governments, technology providers, and security vendors. Three practical points: **don't fret over passwords** — attackers want automated mass attacks, not individual logins; **keep software updated** so devices and password managers pick up post-quantum upgrades automatically; and **stay informed** — tools such as the PQSpy browser extension flag sites already using post-quantum encryption.[1]

<1M Qubits

Estimated cost to break RSA-2048, down from 20 million in 2019

Dec 31, 2030

Federal deadline for post-quantum cryptography key establishment in high-value systems

300+ Organizations

Have adopted quantum computing worldwide, a third of large adopters spend **$10M+ a year**

Glossary

Terms used above, in plain language.

Term	Plain Meaning
AES	The standard method for scrambling stored data. Largely quantum-resistant.
CBOM	Cryptography Bill of Materials - an inventory of the cryptography in your environment.
Certificate / PKI	The digital ID cards proving a website or vendor is who it claims, and the system that issues them.
Code signing	A vendor's digital signature on software, proving an update is genuine and untampered with.
Crypto-agility	Being able to change cryptographic algorithms without rebuilding your systems.
ECC	Elliptic Curve Cryptography - a compact form of public-key encryption. Quantum-vulnerable.
ePHI	Electronic protected health information - patient data covered by HIPAA.
Fault-tolerant	A quantum computer with enough error correction to complete long calculations reliably.
FIPS	Federal Information Processing Standards - NIST's official technical specifications.
FN-DSA	FIPS 206, based on FALCON - a fourth NIST signature standard, still in draft.
Grover's algorithm	A quantum method that speeds up key guessing. Far less threatening than commonly claimed.
HNDL	Harvest Now, Decrypt Later - steal encrypted data today, unlock it years from now.
HQC	NIST's backup key-encapsulation standard, selected in 2025 and built on different math than ML-KEM.
HSM	Hardware Security Module - a dedicated appliance that stores encryption keys.
Hybrid cryptography	Running an old and a new algorithm together so both must be defeated.
Lattice cryptography	The leading post-quantum approach, based on multidimensional grid problems.
ML-KEM / ML-DSA / SLH-DSA	The three finalized NIST post-quantum standards - key exchange, signatures, and backup signatures.
NIST	The U.S. agency that sets federal cryptographic standards.
PQC	Post-Quantum Cryptography - encryption designed to survive quantum attack.
Public-key encryption	Lets two strangers agree on a secret over an open channel. The part quantum breaks.
Q-Day	The point at which quantum computers can break today's encryption. A window, not a date.
QKD	Quantum Key Distribution - a physics-based alternative most agencies advise against.
Qubit	A quantum bit. Unlike a normal bit, it can hold a blend of 0 and 1 at once.
RSA / Diffie-Hellman	The most widely used public-key algorithms. Both quantum-vulnerable.
Shor's algorithm	The 1994 quantum method that breaks RSA, Diffie-Hellman, and ECC.
Symmetric encryption	Same key locks and unlocks. Largely safe from quantum attack.

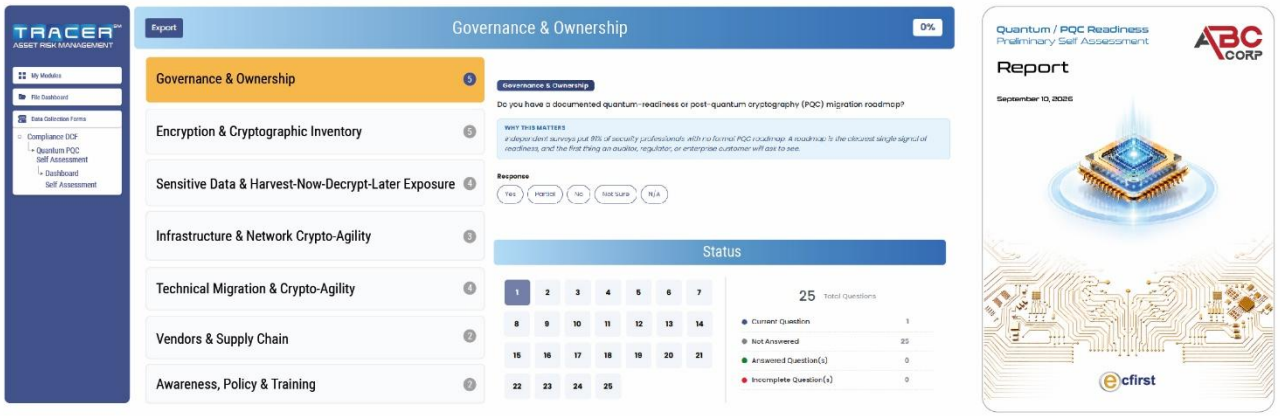
References

1. Kaufman, Natalie. *"Why Quantum Computing Is a Threat to Cybersecurity."* The Wall Street Journal, Aug. 25, 2026. wsj.com/tech/cybersecurity/quantum-computing-threat-cybersecurity-62d293b1
2. ecfirst. *"Quantum Computing Cyber Risk"* infographic, 2026.
3. NIST. *FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)* — Post-Quantum Cryptography Standards, approved Aug. 13, 2024. csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved
4. NIST. *IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards*, 2024. nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
5. Trusted Computing Group. *State of Post-Quantum Cryptography Readiness* survey of 1,500 security professionals, 2025. trustedcomputinggroup.org
6. Quantum Computing Cybersecurity Preparedness Act, Pub. L. No. 117-260, 6 U.S.C. §1526; and Executive Order, *"Securing the Nation Against Advanced Cryptographic Attacks,"* June 22, 2026. uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section1526
7. IBM Research. *"NIST's post-quantum cryptography standards are here."* Aug. 2024. research.ibm.com/blog/nist-pqc-standards
8. IBM Newsroom. *"IBM Delivers New Quantum Processors, Software, and Algorithm Breakthroughs on Path to Advantage and Fault Tolerance."* Nov. 12, 2025.
9. IBM Quantum. *"IBM lays out clear path to fault-tolerant quantum computing."* ibm.com/quantum/blog/large-scale-ftqc
10. IBM Institute for Business Value with the Cloud Security Alliance. *Secure the Post-Quantum Future: 2025 Quantum-Safe Readiness Report*, Oct. 2025. ibm.com/thought-leadership/institute-business-value
11. CISA, NSA, and NIST. *Quantum-Readiness: Migration to Post-Quantum Cryptography*, Aug. 2023. cisa.gov/quantum
12. McKinsey & Company. *Quantum Technology Monitor 2026: A Commercial Tipping Point*, Apr. 28, 2026. mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026
13. Mosca, Michele, and Marco Piani, Global Risk Institute / evolutionQ. *Quantum Threat Timeline Report 2025*, Mar. 9, 2026. globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b
14. Google Quantum AI. *Quantum Echoes on Willow: Toward Real-World Applications*, Oct. 22, 2025, published in *Nature*. blog.google/innovation-and-ai/technology/research/quantum-echoes-willow-verifiable-quantum-advantage
15. Gidney, Craig, Google Quantum AI. *How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits*, May 23, 2025. arxiv.org/abs/2505.15917
16. DigiCert. *Quantum Readiness Outlook*, 1,001 respondents, Jul. 23, 2026. digicert.com/news/quantum-security-deployment-remains-stuck

Quantum Cyber Risk | Readiness

ecfirst

Quantum Cyber Risk Self Assessment



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.

Q-Day

The period when quantum computers can break Standard encryption

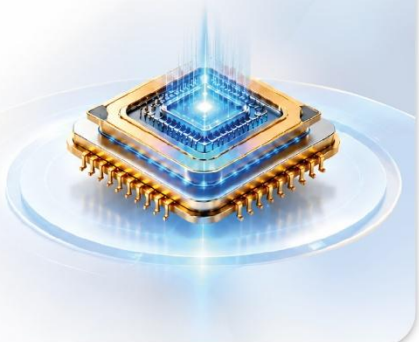
a window, not a date

Quick Links

- Home
- FAQ | Quantum Cyber Risk
- References
- Glossary
- AI-Powered Assistant Bailey

Quantum Cyber Risk Playbook

Infographics | Brief | Brochure



Peter.Harvey@ecfirst.com

www.ecfirst.com