

Breaking Encryption: Y2Q and the Quantum Countdown

Session companion for the Qtonic Quantum Corp executive briefing on Y2Q, harvest-now-decrypt-later, cryptographic inventory, and post-quantum migration governance.

AUDIENCE: BOARD / CISO / CIO

CONTROL: INVENTORY FIRST

DATE: JUNE 16, 2026

SESSION ARC

From false comfort to governed execution.

The session separates fixed-date Y2K thinking from quantum migration reality, then moves through retroactive exposure, the 2029 control window, signal verification, and board governance.

The operating conclusion is direct: inventory first, proof second, remediation third.

AUDIENCE ACTION

What leadership should ask for next.

- Run the Mosca inequality on the organization's own retention and migration numbers.
- Commission a cryptographic inventory before selecting a remediation vendor.
- Require severity-ranked exposure findings and independent attestation for any board-approved PQC program.

TEN TAKEAWAYS

01

The comfort of Y2K is misplaced

Y2K had a fixed date, a mechanical fix, and a clean test. Quantum has no single date, no one-time patch, and no morning where leadership knows it worked.

02

The break comes later, but the deadline already passed

The deadline to act is the break date minus migration time minus the years your data must stay secret.

03

Run the Mosca inequality

If secret lifetime plus migration time is greater than time to a capable quantum computer, the data is already exposed.

04

The risk is retroactive

Adversaries can harvest encrypted traffic now and decrypt it later once the machine exists.

05

Treat 2029 as a control window

The late 2020s through 2035 are the migration-control window. 2029 is a readiness finish line, not a doomsday claim.

06

The near-term tail is fattening

Operators are migrating, capital is flowing, and error-correction work is attacking the hardest bottleneck.

07

The cure is already written

NIST finalized the post-quantum standards in 2024. The gap is knowing where the organization is exposed.

08

Sorting signal from noise is the real skill

Serious resource estimates and viral claims can look identical for a week. The differentiator is verification discipline.

09

The work has an order

Inventory, then proof, then remediation: find the cryptography, prove exposure, then fix it on a vendor-neutral path.

10

Boards should hold one rule

Do not approve a post-quantum plan until management can show current inventory, severity-ranked findings, and a vendor-neutral remediation path.

For follow-up, use the Y2Q resource hub at <https://qtonicquantum.com/y2q> or request a scoped QScout review. Qtonic Quantum Corp.