Y2Q CISO and Board Brief

A board-language summary of the quantum readiness control window: why Y2Q is not Y2K, how to run the Mosca inequality, and what management must prove before a post-quantum plan is board-ready.

AUDIENCE: BOARD / CISO / CIO

CONTROL: INVENTORY FIRST

DATE: JUNE 16, 2026

BOARD THESIS

The deadline is not Q-Day. The deadline is Q-Day minus migration time minus secrecy lifetime.

No machine breaks RSA today, and the expert median remains later than the immediate budget cycle. That is not the planning question. The planning question is whether data being created, transmitted, or stored today must remain confidential beyond the arrival window.

For ten-to-fifteen-year obligations, the exposure window can already be open under conservative assumptions.

REQUIRED MANAGEMENT EVIDENCE

Do not approve spend until the plan has these three controls.

- Current cryptographic inventory across systems, protocols, certificates, libraries, vendors, and sensitive data classes.
- Severity-ranked findings tied to retention period, exposure path, algorithm class, and migration effort.
- Vendor-neutral remediation path with ownership, sequencing, independent proof, and auditor-ready attestation.

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.