WHITEPAPER

The Executive Guide to Post-Quantum Cryptography

What board members and executive teams need to understand about quantum computing, cryptographic risk, and why the transition to post-quantum cryptography is a business decision, not just a technical one.

Why This Belongs on the Board Agenda

Post-quantum cryptography sounds like an engineering problem. It isn't, or at least not only. Every organisation of meaningful size holds data that needs to stay confidential for years, sometimes decades: financial records, health data, intellectual property, government and defence information, customer identities. Cryptography is the control that keeps that data confidential today. A sufficiently capable quantum computer would be able to break the cryptographic algorithms most of that protection currently relies on.

The technical detail of how that happens matters less to a board than the business consequence: any data encrypted with a vulnerable algorithm today, if intercepted and stored now, could potentially be read once that capability exists — regardless of when exactly that turns out to be. This is not a future problem with a future deadline. It is a present exposure with a future trigger.

The Core Idea: Harvest Now, Decrypt Later

An adversary does not need a quantum computer today to benefit from one in the future. They only need to capture and store encrypted traffic now, then decrypt it once the technology matures. Security teams call this "harvest now, decrypt later." It quietly changes the maths of when "later" actually starts to matter.

If your organisation holds data that needs to stay confidential for five, ten, or twenty years — and most regulated industries do — then the relevant question isn't "when will quantum computers be able to break RSA and ECC." It's "how much of our long-lived sensitive data is already exposed to that future risk, today, because of decisions made about cryptography years ago."

Different sectors carry very different exposure windows. Banking and financial services routinely need confidentiality across decades of account and transaction history. Healthcare records frequently require protection for the lifetime of a patient. Government and defence information can require confidentiality for fifty years or more. For all of these, the exposure clock on “harvest now, decrypt later” started the day the data was first encrypted with a vulnerable algorithm — not the day quantum computers arrive.

What "Post-Quantum" Actually Means

Post-quantum cryptography (PQC) is not a single product or a single algorithm. It’s a category of cryptographic algorithms designed to remain secure even against an adversary with a large-scale quantum computer, because they rely on mathematical problems that quantum algorithms don’t have an efficient shortcut for (unlike the problems RSA and elliptic-curve cryptography rely on).

The US National Institute of Standards and Technology (NIST) ran a multi-year, open, international evaluation process and has published the first generation of these standards: ML-KEM (FIPS 203) for establishing shared keys, ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) for digital signatures, with a further signature scheme (FN-DSA, expected as FIPS 206) in the standardisation pipeline. Other national bodies — including France’s ANSSI, Germany’s BSI, and the UK’s NCSC — track and align with the same standards, alongside the US National Security Agency’s CNSA 2.0 timeline for national security systems.

The detail of each algorithm matters to engineers. What matters to a board is simpler: credible, vetted replacements now exist. The open question for most organisations isn’t “is there a standard to move to” — there is — it’s “do we know where we’d need to apply it, and in what order.”

The Question Most Organisations Can’t Yet Answer

Ask any security leader “where does our organisation use cryptography that would need to change?” and the honest answer, in most organisations, is: nobody fully knows. Cryptographic decisions were made incrementally, by different teams, in different systems, over many years — in TLS configurations, in application code, in certificate authorities, in hardware security modules, in third-party software nobody has audited in years.

That is precisely the gap Enterprise Cryptographic Exposure Management (ECEM) exists to close: a continuous discipline of discovering where cryptography is actually used, building a living inventory of it, assessing exposure in business terms, and producing a realistic, prioritised roadmap — rather than a one-off audit that’s stale within a quarter.

What Good Readiness Looks Like

An organisation that is genuinely prepared can answer five questions with evidence, not estimation:

- Where is cryptography actually used across our environment?
- Which algorithms protect our most critical and longest-lived data?
- What is our realistic exposure if that data is harvested today?
- Which systems should be prioritised first, and why?
- What does a credible, resourced migration timeline actually look like?

None of these require the migration to already be finished. They require the organisation to have done the discovery and assessment work that makes a real decision possible — which is a governance achievement well before it's an engineering one.

© 2026 Quantum Sentinel™. All rights reserved.
Registered as a limited company in England and Wales under company number: 17317113. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.