QUANTUM
THINK TANK

Insight that protects. Foresight that leads

The Case for Urgent Action

By Tooba Qasim
December 2025

www.cyberlondon.com | info@cyberlondon.com

Why Waiting Is the Riskiest Choice

The shift to quantum-safe cryptography is often described as a long-term project, something to be addressed **"sometime in the future."** That framing is comforting but it is also misleading.

The real urgency is not about the day a cryptographically capable quantum computer appears. It is about the **data and systems we are securing right now**, and how long they need to remain trustworthy. Decisions made today will determine whether that data remains protected in ten, twenty, or even fifty years' time.

This is why quantum conversation has moved from academic discussion to operational reality. The risk is no longer hypothetical and the cost of delay is becoming clearer.

The Risk Is Already Here, Even If the Machines Are Not

One of the most important shifts in thinking comes from understanding a simple idea: encrypted data stolen today does not lose its value just because it cannot be decrypted immediately.

Advanced threat actors already operate on a long horizon. They collect encrypted communications, databases, backups and intellectual property and store them. When cryptographic protections weaken in the future, that data can be revisited and decrypted retrospectively. This strategy, commonly referred to as **"harvest now, decrypt later,"** turns quantum risk into a present-day concern rather than a future one .

For organisations that manage long-lived data medical records, legal agreements, financial histories, identity data, sensitive research, or government information, this risk is especially acute. Even if systems appear secure today, the exposure window has already opened.

Why Early Action Is Not Optional

Post-quantum migration is not something that can be switched on overnight.

In practice, cryptography is deeply embedded across applications, cloud services, internal networks, identity systems, firmware, hardware security modules, and vendor platforms. Many organisations only discover how widespread their cryptographic dependencies are when they start looking for them.

Unwinding and updating these dependencies takes time. It involves understanding where algorithms such as RSA and elliptic-curve cryptography are used, working with vendors to understand roadmaps, testing new configurations, preparing hybrid environments and updating operational processes. None of this happens quickly and all of it requires coordination across teams that do not always work closely together.

Delaying this work does not make it easier later. It compresses timelines, increases operational risk, and forces rushed decisions.

The Timeline Is Shrinking, Not Expanding

While no quantum computer today can break real-world encryption, the pace of progress in quantum hardware continues to surprise even cautious observers.

In recent years, advances in qubit counts, coherence and error-correction techniques have moved faster than many early roadmaps predicted. Systems such as Google's Sycamore and newer generations of processors from IBM and others have demonstrated steady, incremental progress. Each individual breakthrough may not be decisive but together they reduce confidence in assumptions built around very long cryptographic lifetimes.

This does not mean that "Q-day" is imminent. It does mean that **planning on the assumption of unlimited time is increasingly risky**.

Global Guidance Is Remarkably Consistent

Across regions and institutions, the guidance is strikingly aligned.

Standards bodies and national cybersecurity agencies are not telling organisations to panic or to replace everything immediately. They are saying something far more measured: **start preparing now, transition gradually and avoid waiting until pressure arrives**.

The U.S. National Institute of Standards and Technology has already standardised multiple post-quantum algorithms and continues to expand its portfolio. The UK's National Cyber Security Centre has published clear migration timelines, emphasising early discovery and

prioritization. European institutions, through ETSI and ENISA, are integrating post-quantum readiness into broader digital resilience strategies.

The message is consistent: preparation must begin well before quantum capabilities become operationally relevant.

Urgency Does Not Mean Recklessness

Acting early does not mean abandoning proven security practices or rushing into untested technologies. In fact, the opposite is true.

Early movers have the advantage of time. They can pilot hybrid approaches that combine classical and post-quantum algorithms, test performance impacts, engage vendors thoughtfully and align with evolving standards. They can build crypto-agility into systems so that future changes become manageable rather than disruptive.

Organisations that wait risk being forced into emergency upgrades under regulatory pressure or after a major incident, precisely the situations where mistakes are most costly.

This Is a Strategic Investment, Not Just a Security Fix

Preparing for quantum-safe cryptography is often framed as a defensive necessity but it is also a strategic choice.

Organisations that act early reduce long-term disruption, protect high-value data, and demonstrate resilience to customers, partners and regulators. They are better positioned to meet emerging compliance expectations and to operate confidently in an environment where digital trust is increasingly scrutinised.

The data you protect today may still matter decades from now. That alone makes preparation worthwhile.

Why the Time to Start Is Now

The quantum threat is not a single event waiting in the future. It is a timeline problem. Systems being designed and deployed today must remain secure in a world where cryptographic assumptions are changing.

Waiting increases risk, increases cost and reduces options. Starting early creates flexibility, control and resilience.

The case for urgent action is therefore simple: organisations that begin preparing for quantum-safe cryptography now will face the future from a position of strength, not urgency.

About the author: Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security protocols and exploring the security and performance of PQC on hardware and resource-constrained devices.