PQC Migration Planning

By Tooba Qasim

The Case for Urgent Action: Why Waiting Is the Most Expensive Option

There is a natural tendency in cybersecurity to prioritise what is visible and immediate. Active breaches, ransomware incidents, regulatory fines and operational outages demand attention now. Quantum risk, by contrast, feels distant. It does not break systems today. It does not trigger alerts. It does not show up in incident response dashboards.

That is precisely why it is dangerous.

Post-quantum cryptography is not about reacting to an attack that has already happened. It is about responding to a change in the rules of trust before that change becomes unavoidable.

The organisations that struggle most during major security transitions are rarely the ones that lacked technical expertise. They are usually the ones that waited too long to begin.

The Time Lag Problem Most Organisations Underestimate

One of the biggest misconceptions about post-quantum migration is the belief that it can be handled like a normal upgrade. Patch the cryptographic library, rotate some keys and move on.

In reality, cryptography is deeply embedded. It lives inside protocols, identity systems, certificate chains, APIs, hardware devices, legacy applications, cloud services and third-party integrations. Many organisations do not even have a complete view of where cryptography is being used, let alone how easy it is to replace.

When security leaders finally ask, *"How quickly could we migrate if we had to?"*, the honest answer is often uncomfortable.

Even without quantum pressure, many organisations already struggle with basic cryptographic hygiene: tracking certificates, rotating keys, managing lifecycles and avoiding outages caused by misconfiguration. Adding post-quantum requirements on top of this complexity increases friction not reduces it.

Urgency in this context is not panic. It is recognising that time is a dependency just like budget and skills.

Why ‘Later’ Quietly Turns Into ‘Too Late’

Waiting feels safe because nothing breaks immediately. Systems continue to function. Encryption still works. Customers do not complain.

But while organisations wait, three things continue to happen in parallel.

First, encrypted data continues to be generated, transmitted and stored at massive scale. Some of that data medical records, legal files, long-term contracts, sensitive communications will still be valuable many years from now.

Second, adversaries continue to collect data opportunistically. They do not need to break encryption today for this to be useful later.

Third, infrastructure continues to age. Systems that are deployed now may still be running when post-quantum migration becomes mandatory, even if they were never designed with that transition in mind.

By the time urgency feels unavoidable, options tend to be fewer, more expensive and more disruptive.

Urgency is about Planning, not Deployment

An important clarification: acting urgently does not mean deploying post-quantum algorithms everywhere tomorrow.

Urgency means starting the work that cannot be rushed later.

It means understanding where cryptography exists across the organisation, which systems depend on it, which data must remain confidential long-term and which vendors and partners are involved in cryptographic trust chains.

It also means recognising that post-quantum migration will almost certainly involve hybrid approaches, where classical and post-quantum cryptography coexist for years. That coexistence requires testing, governance and architectural decisions that take time to mature.

Organisations that begin this work early have room to experiment, pilot and adapt. Organisations that wait are forced to compress years of learning into months.

The Human and Organisational Bottleneck

Technology is only part of the challenge.

Post-quantum readiness touches teams that do not normally work closely together: security engineering, enterprise architecture, infrastructure, procurement, legal, risk and compliance. Decisions about cryptography affect contracts, vendor relationships, regulatory interpretations and operational resilience.

Without early awareness and internal alignment, post-quantum initiatives risk stalling before they even begin. Ownership becomes unclear. Budgets are delayed. Responsibility is pushed sideways.

Urgent action at this stage is about creating shared understanding. It is about ensuring that leadership, technical teams and risk owners are asking the same questions even if they do not yet have all the answers.

Regulators Are Signalling Direction, Not Deadlines (Yet)

Another reason urgency matters is that regulatory expectations are forming now not later.

Governments and national cybersecurity authorities are increasingly framing post-quantum security as a long-term resilience issue, not a niche research topic. Guidance documents, migration timelines and policy statements are designed to give organisations space to prepare but they also establish expectations.

Historically, when cryptographic transitions become regulatory requirements, organisations that have already begun preparation tend to influence how “reasonable” compliance is interpreted. Those that have not often end up reacting to externally imposed timelines.

Starting early is not just about technical readiness; it is about strategic positioning.

Urgency Without Fear

There is no need for alarmism. Cryptographically relevant quantum computers are not available today. Classical encryption is still doing its job.

But the window between *“this is theoretical”* and *“this is urgent”* is often much shorter than expected especially when organisational complexity is involved.

Post-quantum readiness is one of those rare security challenges where the cost of early action is relatively low and the cost of late action can be disproportionately high.

The goal of urgency is not to rush deployment. It is to avoid being rushed later.

A Closing Perspective

From a community perspective, the post-quantum transition is not about winning a race or claiming technical superiority. It is about building resilience collectively, learning from shared experience and ensuring that trust in digital systems does not fracture under pressure.

Urgent action at this stage means starting conversations, mapping dependencies and asking uncomfortable questions before they become unavoidable ones.

Those questions are not a sign of weakness. They are a sign that preparation has begun.