Operational Readiness

By Tooba Qasim

What Happens After PQC Goes Live

Rolling out post-quantum cryptography is not the finish line. In many ways, it is the moment when the most important questions begin.

Up until deployment discussions tend to focus on algorithms, standards and architectures. Once systems are live, the conversation shifts to something far more practical:

Does this actually work at scale, under pressure and in the real environments we operate every day?

Operational readiness is about recognising that cryptography does not live on whiteboards. It lives inside software stacks, hardware devices, networks and monitoring systems all of which behave in ways that are sometimes messy, unexpected and difficult to predict.

When "Mathematically Secure" Is Not the Same as "Operationally Secure"

One of the most misunderstood aspects of cryptography is the difference between an algorithm being secure *in theory* and being secure *in practice*.

Even if a cryptographic algorithm is mathematically sound, the way it is implemented can leak information. This is where **side-channel attacks** come in and they do not require breaking the mathematics.

A simple way to think about side-channel attacks is this:

Instead of attacking the lock, an attacker watches *how the lock behaves*.

Information can leak through timing differences, power consumption, memory access patterns, cache behaviour or even electromagnetic signals. None of this requires understanding the underlying cryptography. It requires observing how a system behaves while it performs cryptographic operations.

This matters especially for post-quantum cryptography.

Many PQC algorithms involve larger keys, more memory usage and more complex arithmetic than traditional RSA or elliptic-curve implementations. That complexity increases the number of places where subtle implementation mistakes can occur.

There is also a maturity factor. RSA and ECC implementations have been deployed, attacked, fixed and hardened for decades. PQC implementations by comparison are new. They are improving rapidly but they are not yet as battle-tested in real operational environments.

The key operational message is simple: **with PQC, implementation quality matters as much as algorithm choice**.

Hardware Reality: Where Theory Meets Constraints

Another challenge that often appears *after* rollout is hardware behaviour.

Post-quantum algorithms frequently consume more CPU, require more RAM and produce larger keys and signatures. On modern servers, this may show up as a small performance hit. On constrained hardware, it can be far more disruptive.

Operational teams have already begun encountering issues when PQC is introduced into environments that rely on smart cards, TPMs, hardware security modules (HSMs), embedded systems or IoT and operational technology devices.

These systems were often designed with tight resource limits and long lifespans. Introducing cryptographic operations that are heavier than expected can lead to performance degradation, unexpected failures, timeouts, or incompatibilities with hardware accelerators.

In some cases, systems silently fall back to classical cryptography when PQC operations fail which can completely undermine the security objective if it goes unnoticed.

This is not theoretical. These are exactly the kinds of issues that surface only once systems are running in production.

Monitoring and Visibility: Knowing What Is Actually Running

Operational readiness requires visibility.

It is not enough to assume that post-quantum cryptography is active. Teams need to be able to observe which algorithms are actually being used, whether hybrid modes are functioning correctly and whether any components are failing or falling back without warning.

This means updating monitoring and logging practices to include cryptographic indicators, handshake failures, unexpected latency and protocol negotiation behaviour. Without this visibility, organisations may believe they are running quantum-safe systems while critical components quietly behave otherwise.

For security operations centres, this represents a shift. Cryptography is no longer a static background feature. It becomes something that must be observed, validated and occasionally investigated as part of normal operations.

Incident Response in a Post-Quantum World

Incident response plans also need adjustment.

If a cryptographic incident occurs in a PQC-enabled environment, responders need to know which algorithms were in use, whether hybrid modes were active and how keys were managed across systems. Without this context, it becomes difficult to assess impact or determine whether an incident has long-term implications for data confidentiality.

Operational teams should treat cryptographic failures, unexpected negotiation behaviour, degraded performance or hardware incompatibilities as signals worth investigating not just technical glitches to be patched and forgotten.

Third-Party and Vendor Readiness

No organisation operates in isolation.

Cloud platforms, identity providers, network equipment vendors and managed service providers all play a role in cryptographic operations. Operational readiness includes understanding how these partners handle PQC, what hybrid support they offer and how failures are surfaced.

Vendor readiness is not just about roadmap statements. It is about behaviour under load, under failure and during upgrades. These details matter far more in production than in procurement documents.

The Operational Mindset Shift

The most important change required for post-quantum cryptography is not technical. It is cultural.

Operations teams are used to treating cryptography as something stable and invisible. PQC changes that assumption. It introduces new algorithms, new performance characteristics and new failure modes that must be understood and managed.

Being operationally ready does not mean everything must be perfect. It means teams are prepared to observe, respond and improve as systems evolve.

Post-quantum cryptography is not a one-time deployment. It is a new operational reality and like all operational realities, it rewards preparation, visibility and experience over assumptions.