Skills and Workforce Readiness for the PQC Transition

By Tooba Qasim

Preparing People, Not Just Systems:

When organisations talk about post-quantum cryptography (PQC), the conversation usually starts with algorithms, systems and infrastructure. What often comes much later, sometimes too late is the realisation that **people are the hardest part of the transition**.

Technology can be upgraded. Software can be patched. Architectures can be redesigned. But without the right skills, understanding and coordination across teams, even the best PQC strategy will struggle to move beyond paper.

Preparing for a quantum-safe future is not only a technical exercise. It is a **workforce readiness challenge**.

Why skills matter before deployment, not after

One of the most common mistakes organisations make in large security transitions is treating training as something that happens *after* decisions are made. With PQC, this approach creates real risk.

Post-quantum cryptography introduces new concepts that many experienced professionals have never worked with before: new key sizes, new performance trade-offs, hybrid cryptographic constructions, unfamiliar standards and longer migration timelines. Teams that are not prepared can misconfigure systems, misunderstand risks or resist change simply because the topic feels opaque.

Training early does two important things. First, it reduces fear and uncertainty by replacing vague concerns with practical understanding. Second, it allows teams to contribute meaningfully to planning decisions rather than reacting to them later.

In other words, **skills readiness enables better strategy**, not just smoother execution.

The skills gap is real and it cuts across roles

PQC is sometimes described as “a cryptography problem,” but that framing is misleading. While cryptography specialists play a key role, the transition touches far more parts of an organisation than just the security team.

Security engineers and cryptographers need to understand new algorithms, hybrid deployment models and evolving standards. Architects need to assess how PQC affects system design, performance and interoperability. Infrastructure and network teams must deal with changes in TLS, VPNs and certificate lifecycles. Cloud and DevOps teams encounter PQC through libraries, APIs, container images and CI/CD pipelines.

Beyond technical roles, procurement teams need to evaluate whether vendors have credible quantum-safe roadmaps. Legal and compliance teams must understand long-term data protection obligations and emerging regulatory expectations. Risk and audit teams need to incorporate quantum risk into assessments and reporting. Even executive leadership needs enough awareness to ask the right questions and make informed prioritisation decisions.

PQC readiness is therefore **a shared capability**, not a niche expertise.

Why “learning on the job” is risky for PQC

In many areas of cybersecurity, teams rely on experience, intuition and incremental learning. PQC challenges that approach.

Unlike familiar cryptographic upgrades, PQC involves moving away from algorithms that have been trusted for decades. Decisions made during early pilots such as which systems to migrate first, where to use hybrid approaches, or how to handle legacy dependencies can have long-term consequences.

If teams lack foundational knowledge, they may over-engineer solutions, delay progress unnecessarily, or underestimate hidden dependencies. Worse, they may implement changes in ways that look compliant but do not meaningfully reduce risk.

This is why workforce readiness should be seen as **risk reduction**, not overhead.

Building quantum literacy, not quantum experts

The goal is not to turn every employee into a cryptographer. What organisations need is **quantum literacy**: a shared baseline understanding that allows different teams to communicate clearly and make aligned decisions.

For technical teams, this means understanding where cryptography lives in their systems, what changes with PQC and how hybrid models work during transition. For non-technical teams, it means understanding why timelines exist, why migration takes years rather than months, and why "waiting until it's urgent" is not a safe strategy.

Clear internal education, short briefings, targeted workshops and role-specific guidance goes a long way. Organisations that invest in this early often find that resistance decreases and collaboration improves.

Clarifying ownership and accountability through skills

Skills readiness also supports governance.

When people understand PQC well enough to discuss it confidently, ownership becomes clearer. Security teams can articulate risks. Architects can propose realistic designs. Risk and compliance teams can integrate quantum risk into existing frameworks. Leadership can sponsor programmes with confidence rather than uncertainty.

Without this shared understanding, quantum risk often falls into a grey area where everyone assumes someone else is responsible. Training helps close that gap by making ownership practical rather than theoretical.

Preparing today for tomorrow's workforce needs

Another challenge is sustainability. PQC migration is not a one-off project; it is a multi-year journey that will continue as standards evolve and systems are replaced.

This means organisations should think not only about current staff but also about **future capability**. Hiring, upskilling and retention all matter. Teams that already struggle to find cryptography or PKI expertise may find those skills even more in demand as PQC adoption increases globally.

Building internal capability even at a basic level reduces long-term dependency on scarce external expertise and gives organisations more control over their own timelines.

From awareness to confidence

Ultimately, workforce readiness is about confidence.

When people understand why PQC matters, what is changing and how their role fits into the transition, uncertainty turns into engagement. Instead of asking “why are we doing this?”, teams start asking “how do we do this well?”.

That shift is essential. Organisations that prepare their people early do not just move faster, they make better decisions, avoid unnecessary risk and build a foundation that can adapt as post-quantum cryptography continues to evolve.

Closing thought

Post-quantum readiness is often framed as a race against technology. In reality, it is just as much a race to **build understanding before urgency forces action**.

The organisations that succeed will not be the ones with the most advanced algorithms on paper but the ones whose people are ready, informed, aligned and confident to carry the transition forward.