INNOVATION

Start Small, Start Now: The Executive's Guide To Deploying Hybrid Post-Quantum Encryption

By Federico Simonetti, Forbes Councils Member.

Xiid's CTO, Federico Simonetti, is a security expert with a background in ethical hacking, law enforcement and academia.

Quantum risk is already here.

Every CEO and CTO now owns a problem that will outlive their tenure: the organization's cryptography. The uncomfortable reality is that quantum risk is not a "someday" issue. It's already embedded in today's infrastructure through data that can be stolen now and decrypted later.

Waiting for standards to be perfectly finalized before acting is like waiting for a hurricane to make landfall before boarding up the windows. By the time the storm hits, it's far too late.

Start with your crypto footprint.

The first move is deceptively simple: map your cryptography footprint. Most organizations cannot answer basic questions like which protocols they use where, how keys are generated and rotated, or which vendors terminate and decrypt traffic in the middle. Without that inventory, a post-quantum strategy is only a slide deck.

Leaders need a living catalog of where TLS, VPNs, database encryption, application-level crypto and machine-to-machine authentication live, and which are tied to long-lifecycle assets that will still be running when practical quantum attacks arrive.

From there, the objective is agility, not heroics. A viable transition plan isn't a rip-and-replace project that halts the business. Instead, it's a controlled layering of quantum-safe capabilities over what already works. The priority is a crypto-agile architecture: systems, APIs and networks that can adopt new algorithms, swap suites and run hybrids without rewrites. This is especially critical for assets expected to last 10 to 30 years, where the encryption chosen today must survive multiple generations of attackers and hardware.

Make hybrid post-quantum the default.

True post-quantum protection will be hybrid for a long time. Organizations need schemes that are simultaneously resilient against classical attacks and quantum-enabled adversaries, combining well-vetted existing algorithms with NIST-recommended post-quantum primitives in layered designs. That hybrid posture buys time: if any one algorithm is weakened, the combined system remains robust. It also lets teams adopt post-quantum encryption incrementally, starting with the most sensitive data paths and long-lived IP or OT.

At the operational level, key hygiene will matter more than ever. Ephemeral keys that exist only for the life of a session, aggressive automatic rotation and re-keying triggered by time or data thresholds all shrink the window of opportunity for attackers. This is particularly important in a world of harvest-now-decrypt-later (HNDL) campaigns, where adversaries quietly stockpile encrypted data, banking on future quantum capabilities to unlock it. Shorter key lifetimes and minimized reuse limit the value of anything an attacker manages to steal today.

Implement end-to-end, vendor-proof encryption.

Another non-negotiable principle: end-to-end, vendor-proof encryption. Many current “security” architectures depend on break-and-inspect designs where intermediaries decrypt traffic for scanning, effectively inserting a standing backdoor into every connection. Those patterns are fundamentally incompatible with serious post-quantum security.

Any point where a third party can routinely see traffic in the clear becomes a high-value, high-liability target. Future-ready designs maintain continuous encryption across the full path, with intermediaries enforcing policy based on deterministic, end-to-end, predictable and enforceable criteria rather than payload visibility.

Boards should not wait for technology teams to volunteer this topic. These questions belong on this quarter’s agenda:

• Where are our cryptographic dependencies, especially in systems designed to last decades?

• How agile are our vendors? Can they support hybrid post-quantum encryption and rapid algorithm changes without major disruption?

• Do our security architectures rely on break-and-inspect or man-in-the-middle designs that will become untenable as quantum threats mature?

• Most importantly, what are the first few concrete steps the company can take this year to begin deploying hybrid post-quantum encryption on our highest-value assets?

Start small, but start now.

The organizations that win this transition won't necessarily be the ones with the most dramatic roadmap slide; they will be the ones that start small and start early. Pilot hybrid post-quantum encryption on a critical internal service, wrap a long-lifecycle system in quantum-resilient tunnels or modernize key management around automation and ephemerality.

When "quantum later" abruptly becomes "quantum now," the only defensible position to customers, regulators and shareholders will belong to leaders who treated cryptography as a strategic asset and acted before the deadline was written for them.

By Federico Simonetti, COUNCIL POST | Membership (fee-based). Xiid's CTO, Federico Simonetti, is a security expert with a background in ethical hacking, law enforcement and academia. Read Federico Simonetti's full executive profile here.
Find Federico Simonetti on LinkedIn. Visit Federico's website.