Post-Quantum Security, Explained for People Who Sign the Checks

A plain-English briefing for business leaders

By Charlo Mouton

Most security problems announce themselves. A breach shows up in the logs, a customer calls, a regulator sends a letter. The quantum problem is different. The damage can start years before anyone notices, and by the time it is obvious, the data is already gone.

This piece explains what the risk is, what has already changed, and what a sensible business should do about it in the next 12 to 24 months. No physics degree required.

The short version

Almost everything your company does online is protected by two kinds of math. One kind keeps data secret while it moves between systems (encryption and key exchange). The other kind proves who sent something and that it was not altered (digital signatures). Today, most of that work is done by algorithms called RSA and elliptic-curve cryptography.

Those algorithms are safe against today's computers. They are not expected to be safe against a large, working quantum computer. Nobody can tell you the exact year one will exist. But the people responsible for setting security standards decided they could not wait to find out, and they have already published the replacements.

Why "not yet" is not the same as "not a problem"

The risk most leaders miss is called **harvest now, decrypt later**.

An attacker does not need a quantum computer today to cause you trouble later. They only need to copy your encrypted traffic or files now and store them. Storage is cheap. When the decryption capability arrives, they open the archive.

So the real question is not "when will quantum computers arrive?" It is "how long does my data need to stay private?"

- A marketing email: a few days.
- A customer's financial history, a health record, a merger file, a long-term contract: ten years or more.

If the answer for some of your data is "longer than the time until a capable quantum computer exists," that data is already exposed in a practical sense. That is the whole

argument for acting early.

Signatures have a related problem. If a signature scheme can be broken, someone could forge approvals, software updates, or financial instructions that look legitimate. Anything that relies on long-lived signing keys, such as firmware, identity systems, or blockchain accounts, needs a plan.

What has already changed

This is not a forecast. In August 2024, the U.S. National Institute of Standards and Technology (NIST) published its first three post-quantum cryptography standards:

- **ML-KEM** (FIPS 203), for establishing shared encryption keys. This replaces the key-exchange role RSA and elliptic curves play today.
- **ML-DSA** (FIPS 204), a general-purpose digital signature scheme.
- **SLH-DSA** (FIPS 205), a signature scheme built on hash functions. It is slower and produces larger signatures, but it rests on very conservative assumptions, which makes it a good backup.

NIST has also selected an additional key-establishment algorithm (HQC) as a backup to ML-KEM, and its draft transition guidance proposes phasing out today's vulnerable algorithms over the next decade, with deprecation around 2030 and disallowance around 2035 for many uses. Large vendors are already shipping hybrid modes in browsers, messaging apps, and cloud services.

In other words, the replacement parts exist. The work now is installing them.

What this means in business terms

You do not need to understand lattice math to manage this risk, the same way you do not need to understand metallurgy to replace the locks on a building. You need to know four things.

1. Where your cryptography lives. Most companies cannot answer this today. Encryption is buried in vendor products, libraries, VPNs, payment gateways, identity providers, and backup systems. The first project is an inventory: what systems encrypt or sign data, with which algorithms, and who controls the upgrade.

2. Which data has a long shelf life. Rank your data by how long it must stay confidential. Health, financial, legal, and identity data usually sits at the top. That ranking tells you where to start.

3. Who you depend on. For most businesses, the bulk of the migration happens inside vendors' products. Ask your critical vendors a direct question: "What is your post-quantum roadmap, and which NIST algorithms are you adopting?" A vague answer is useful information.

4. How quickly you can swap algorithms. Security teams call this *crypto-agility*. A system that hard-codes one algorithm deep in its design is expensive to fix. A system that treats the algorithm as a replaceable part can be upgraded with a configuration change and a test cycle. Agility is the real goal, because the standards will keep evolving.

A practical 12-to-24-month plan

1. **Name an owner.** Someone in security or IT should own the quantum transition, with a short quarterly report to leadership.
2. **Build the inventory.** Start with internet-facing systems, identity, payments, and anywhere long-lived data is stored.
3. **Prioritize by data lifespan.** Protect the long-shelf-life data first.
4. **Use hybrid modes where available.** Hybrid key exchange combines a classical algorithm with ML-KEM, so you are protected as long as either one holds. It is the cautious middle path most major vendors have taken.
5. **Put it in contracts.** Add post-quantum readiness questions to vendor reviews and renewal terms.
6. **Test before you need to.** Post-quantum keys and signatures are larger than today's. That can affect bandwidth, storage, hardware tokens, and older devices. Find those limits in a pilot, not during an emergency.

Being honest about what "quantum-ready" means

A word of caution about marketing language. Using a NIST-standardized algorithm is not the same as being certified. Formal validation (for example, FIPS 140-3 module validation) is a separate, lengthy process. And a system can use post-quantum algorithms in one layer while still relying on classical cryptography in another.

I have seen this up close. At Galaxia, the ecosystem I founded, we built post-quantum tooling using ML-KEM, ML-DSA, and SLH-DSA at the application layer through an open-source library, running on a public testnet. We are also clear in our own documentation that this implementation is not FIPS-validated and that on-chain signatures on the underlying network remain classical. Saying that plainly costs nothing and earns trust. Buyers should expect the same honesty from every vendor.

When someone tells you a product is "quantum-proof," ask three questions:

- Which algorithms, and in which part of the system?
- Is the implementation validated, or just built on the standard?
- What still depends on classical cryptography?

The bottom line

Post-quantum security is a migration, not a product you buy once. The standards are published, the deadlines are taking shape, and the biggest risk, data stolen today and read later, is already in play. Companies that start with an inventory, prioritize long-lived data, and push their vendors for specific answers will handle this calmly. Companies that wait for a headline will be doing it in a hurry.

Charlo Mouton is a writer and the founder of Galaxia, a Web3, fintech, and AI ecosystem with post-quantum and compliance tooling on public testnet. He writes about security, compliance, and healthcare operations for business readers.