

Post-quantum security starts with migration, not quantum computers

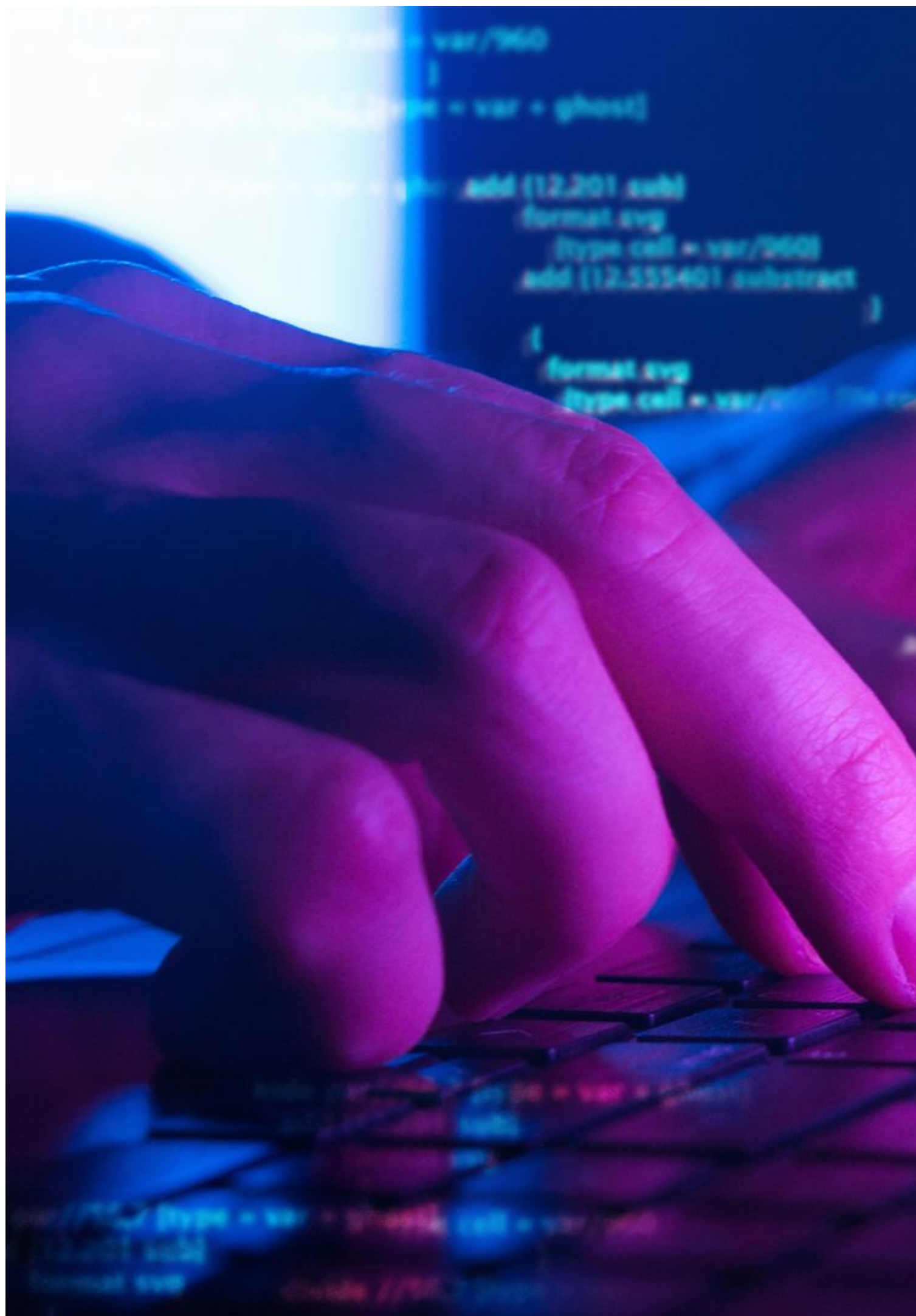
02 July 2026, 10:00

Farhad Aghili

Ludwig De Loch

Why you should prepare long before Q-day arrives

Many organisations still see post-quantum security as a concern for the future. Cryptographically Relevant Quantum Computers (CRQCs), capable of breaking today's public-key cryptography, do not yet exist at an industrial scale, and no one knows with certainty when "Q-day" will arrive. The real question, however, is not when quantum computers will become a reality, but how organisations can prepare for a transition that may take years. Connected products, industrial systems and digital platforms often remain in use for decades. At the same time, regulations such as the Cyber Resilience Act (CRA) and NIS2 require organisations to maintain security throughout the entire lifecycle of their products and systems. As a result, post-quantum security is becoming a major business, architecture and migration challenge. It is a challenge that starts today.



Why post-quantum security matters today

Almost every organisation relies on public-key cryptography today, including RSA and ECC. This technology protects software applications, connected products, industrial systems, cloud environments, communication protocols, and identity and certificate infrastructures. Quantum computers threaten part of this foundation. Once Cryptographically Relevant Quantum Computers (CRQCs) become powerful enough, they are expected to break the public-key cryptographic mechanisms that are widely used today. No one knows exactly when this will happen. However, uncertainty is no reason to delay preparation. The transition is no longer a theoretical exercise. The first post-quantum cryptography standards have already been published.

One major concern is the "harvest now, decrypt later" scenario. Attackers can collect encrypted sensitive data today and decrypt it in the future, once quantum technology has matured. Organisations that handle confidential information with a long-term value may already face a risk of future exposure.

Another challenge is the long lifespan of digital systems. Many products and infrastructures developed or deployed today will still be operating when quantum threats become a reality. This includes industrial machines, connected products, IoT devices, OT environments, embedded systems, and long-life software platforms. The longer a system remains in service, the less time you will have to complete a smooth migration in the future.



Migration is the real challenge

Discussions about post-quantum security often focus on new algorithms and standards. In practice, technology is only part of the challenge. The real task is to understand where cryptography is used, how deeply it is embedded and how you can evolve systems without disrupting operations. Many organisations already face practical questions:

- Where is cryptography used in our systems?
- Which components depend on vulnerable mechanisms?
- Which mechanisms may need replacement in the future?
- Which suppliers introduce cryptographic dependencies?
- Can systems be updated remotely?
- What are the operational risks of migration?
- What is the impact on performance or interoperability?

These questions go beyond cryptography. They touch system architecture, software lifecycle management and system engineering. The first step is to know exactly where cryptography is used. It is often embedded more deeply than organisations expect. You may find it in communication stacks, middleware, PKI infrastructures, hardware security modules, firmware, third-party software and cloud services. Migration is therefore rarely a simple algorithm swap. It needs planning, prioritisation and a phased approach.

Every sector faces different challenges

Connected products, machines and embedded systems

For organisations developing connected products, industrial machines or IoT solutions, lifecycle limits often form the biggest challenge. Many of these systems:

- Remain in use for many years
- Have limited computing resources
- Are difficult to update
- Depend on fixed hardware capabilities
- Include multiple suppliers and protocols

In these environments, post-quantum readiness depends on updatability, crypto-agility, modular architectures and lifecycle-aware design. The goal is not only to secure systems today. You also need to ensure they can evolve safely over time. This becomes even more important under the Cyber Resilience Act. It strengthens responsibilities across the full lifecycle of digital products.

SaaS providers and digital platforms

SaaS providers often have more flexibility to update systems. Even so, they also face several challenges. Important considerations include:

- The long-term confidentiality of customer data
- Cryptographic dependencies in cloud environments

- Identity and certificate management
- Integrations with external services
- Compliance and trust requirements

These topics are becoming more important for healthcare, finance, energy and critical infrastructure. Preparing for the post-quantum era is becoming part of broader resilience and trust strategies.

Manufacturing companies and industrial operators

Industrial companies may not develop the underlying technologies themselves, but they often rely heavily on digital infrastructures and connected production environments. As a result, they face challenges such as legacy systems, long replacement cycles, supplier dependencies and limited visibility into the embedded technologies that support their operations.

Many industrial environments were never designed with crypto-agility or future cryptographic migration in mind. As connectivity continues to grow, it becomes increasingly important to understand not only where cryptography is used, but also how dependent business operations are on it.



Organisations do not need to replace all cryptography today. But this is the right moment to identify where it is used and what a future migration could look like. When post-quantum security becomes necessary, preparation will make the difference.

Where should you start? In the next article, we explore practical steps your organisation can take today to prepare for post-quantum security migration.

[Read the next article](#)

This article is part of a two-part series on post-quantum security.

Part 1: Post-quantum security starts with migration, not quantum computers ?

Part 2: [How can you prepare your organisation for post-quantum security? A practical roadmap](#)

Authors



Farhad Aghili



Ludwig De Locht