EBOOK

POST QUANTUM CRYPTOGRAPHY READY

A Practical Guide for Navigating the Quantum Shift in Cybersecurity

digicert®

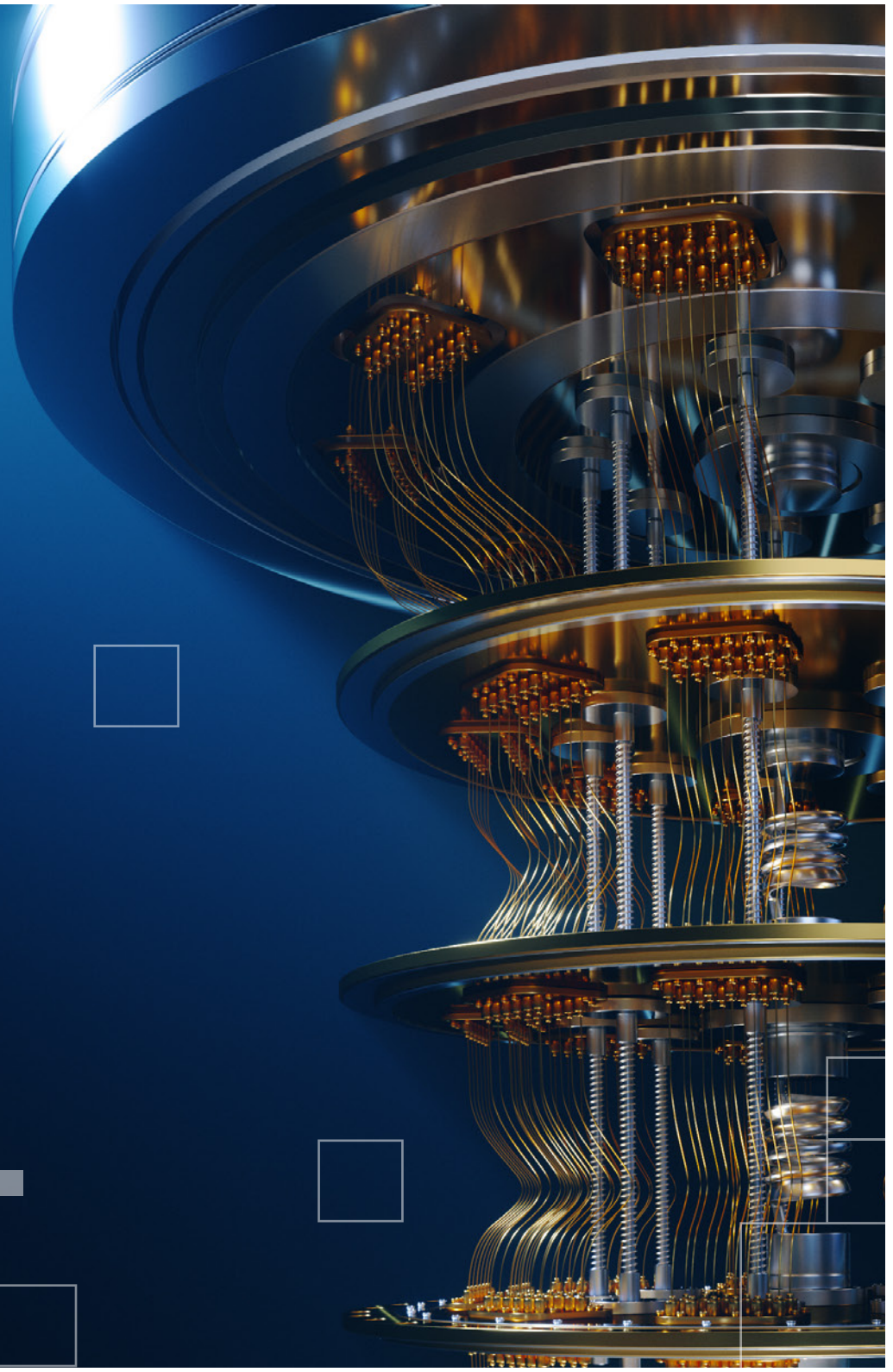


TABLE OF CONTENTS

INTRODUCTION:

THE KEYS TO THE CRYPTO CASTLE

You work tirelessly to protect your business and its assets, people, and data. To use a brick-and-mortar metaphor: Your doors have double locks, your windows are shatterproof, an alarm system detects movement inside; and perhaps a security guard patrols the perimeter. You have layered defenses, but a new enemy threatens to break through even your most robust security measures.

Quantum computers are a wake-up call for cybersecurity. Their exponentially enhanced computational power will render traditional cryptographic measures obsolete overnight, shattering traditional encryption like a rock through a windowpane. Businesses that fail to implement quantum-safe cryptography along with their existing security measures are placing their data at an unacceptable level of risk.

Even nascent quantum computers could selectively steal master keys, code-signing keys, and other foundational cryptographic assets to bypass security with forgery. Bad actors can spoof validations, infiltrate systems, and defraud enterprises at a massive scale before quantum-safe measures are implemented.

A proactive approach is critical, especially given the reality that this transition will take longer than you think. The possibility of "Harvest Now, Decrypt Later" schemes, where hostile individuals or nation-states hoard data to crack later, has been hotly debated by experts, but it's one of many potential doomsday scenarios that could occur once cybercriminals gain access to quantum computing.

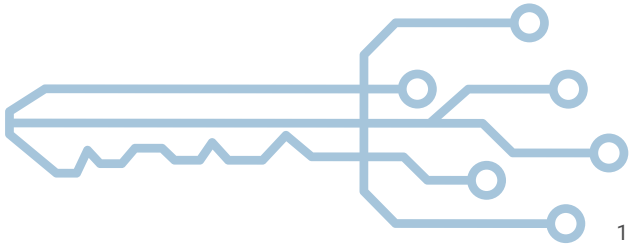
Although the timeline remains ambiguous, quantum computing is an inevitability that requires proactive measures that embrace cryptographic agility. By layering quantum-safe encryption alongside existing security, adopting contingency plans, and prioritizing adaptability, you can stay secure as quantum (and other) capabilities come online.

The future belongs to those who get ahead of this existential threat with a commitment to proactive readiness. The following guide offers tangible steps to take to prepare, starting today.

The crypto-agile mindset

Cryptographers are planning for "Q-Day" when the world goes quantum. But the truth is that Q-Day isn't just one day, but every day from now on. And as the world continues to evolve, you need to be ready to adapt your playbook on the fly, because non-quantum threats aren't going anywhere. That's why crypto-agility represents the best approach: layer quantum-safe security with existing protocols and a solid plan to adapt to a changing threat landscape as needed.

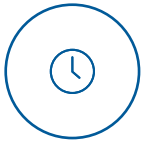
Quantum readiness means being prepared for any contingency, quantum or otherwise. A business built to adapt to changing circumstances will be more successful than the business that tries to nail it on day one. Protect your castle with strong locks and have the barbed wire fence ready and security guards on speed dial. Build in the scalability and agility that you already need to handle the exponential number of devices and certificates already on your network and for ever-shrinking certificate lifespans.



THE POST-QUANTUM CRYPTOGRAPHY PRIMER FOR SECURITY PROS

WHO Every company will need to rethink how they implement security on the internet today to prevent significant loss tomorrow.

Those who are already on the journey to crypto-agility are in good company. Strong correlation exists between high-performing organizations and a heightened sense of urgency about post-quantum cryptography (PQC).



WHEN While no exact timeline exists, most cryptographers agree that true quantum computing is less than 10 years out. Taking encryption lifecycles into consideration, companies should explore crypto-agile protocols and create an implementation plan now because the transition to PQC will take longer than you think. Systems you are deploying over the next few years may have to be designed now to accommodate these changes.

WHY Post-quantum cyberattacks put businesses in every industry at risk of massive financial and reputational loss. In healthcare, hospitals and insurers must secure HIPAA-protected data to maintain compliance and patient trust.

Unprepared consumer goods, manufacturing, and technology companies put their employee data and intellectual property on the line. For financial companies and those subject to regulatory requirements like GDPR, a customer data breach jeopardizes their ability to conduct business at all. Today's guidance for quantum readiness will quickly evolve into compliance mandates.

WHAT TO DO NEXT:

ASSESS YOUR CURRENT QUANTUM READINESS

The most important step is knowing your current cryptographic landscape, so you know your system at least as well as potential attackers do.

Begin by conducting a comprehensive audit of your existing cryptographic infrastructure, algorithms, and protocols. Identify potential vulnerabilities and areas where quantum computing could pose a threat to your security measures. These entry points represent the map of your vulnerabilities, as well as your guide to where you'll implement quantum certificates. As needed, collaborate with experts in quantum computing and cryptography to understand the implications of quantum advancements on your security posture.

Find your baseline

- What cryptographic keys are you currently using and where? Do you already have an inventory?
- When will certificates expire, and which ones protect long-term, high-value data?
- What systems and data are currently protected by non-quantum-safe algorithms?
- Are data and crypto assets located on premises or in the cloud?
- How are your software packages updated, and what kinds of third-party components do they contain?
- Which use cases does this cryptography support (e.g., data at rest encryption, machine identity, secure email)?

This information will help you create the foundation for an inventory of cryptographic keys and their characteristics.

Build a framework that survives the shift

Armed with insights from your baseline assessment, it's time to proactively build crypto-agility into your cryptographic framework. But first, a reminder. Quantum-readiness won't be achieved in a day, and there is no one-and-done solution. You're essentially retrofitting the world's cybersecurity infrastructure to be quantum safe, so the goal is a kind of "crypto-agility" wherein outdated cryptographic assets can be replaced without undue disruptions to infrastructure and business operations.

Start here

- Create an inventory of your certificates, algorithms, and other cryptographic assets.
- Define a transition plan for each use case that keeps necessary stakeholders informed and communicates needed budget allocations. PQC algorithms will require more computing resources than current algorithms, so plan accordingly.
- Swap out encryption algorithms for roots of trust (e.g., your organization's private certificate authorities), firmware for long-lived devices, and any other assets that produce signatures that need to be trusted for a long time.
- Explore ways to incorporate quantum-safe algorithms into your products as you engage your vendors to understand their plans.
- Stay abreast of news and emerging standards by subscribing to the DigiCert blog.
- Embracing a forward-thinking approach to cryptography will help your business mitigate the risks posed by quantum computing and ensure the long-term security of your data and digital assets.

ESTABLISH A CRYPTO CENTER OF EXCELLENCE (COE)

To bolster crypto-agility, establish a dedicated Crypto Center of Excellence (CoE) to serve as the focal point for executing transition plans, sharing knowledge, and establishing best practices within your organization.

Empower your CoE team to stay at the forefront of cryptographic advancements through continuous learning and engagement with digital trust experts. By centralizing crypto-expertise within a dedicated CoE, your business can accelerate its journey toward crypto-agility and lead the way for others in your industry.

CoE project ideas

- While NIST works to standardize implementation methods, start to test PQC algorithms against your own networks and protocols. Leverage DigiCert's Quantum Safe Playground to experiment with solutions.
- Explore tools and solutions that can help with discovery, inventory, and management of cryptographic assets.
- Experiment with phased implementation approaches to minimize disruption and ensure security coverage throughout the transition.
- Generate a PQC Handbook with key contacts and standard operating procedures.

Transform an existential threat into a quantum leap forward

When the first cryptographically relevant quantum computer comes online, the cybersecurity protocols we've counted on for years will no longer be enough to keep our data safe. Yes, quantum computers are an extinction event—for outdated cybersecurity methods. But it doesn't have to be the end of the world, thanks to scientists, engineers, and industry groups currently working on new frameworks. With each passing day, more resources come online to support this process.

By proactively planning for the future, businesses position themselves defensively against the looming threat of post-quantum cyberattacks. Seize this moment to transform an existential crisis into a quantum leap forward toward a more resilient digital future.

CONCLUSION:

REMEMBER, YOU'RE NEVER ALONE

At DigiCert, we have been protecting web traffic for two decades. Our approach to SSL/TLS has evolved to meet the pace of innovation yet remains true to original cryptography methods invented in the 1970s. We work directly with NIST and play an active role in developing the solutions that will shape our collective PQC future.

We can help you guard your crypto castle.

Enter the Quantum Safe Playground.