ENQUIZIT
A CDW COMPANY

Post-Quantum Cryptography:

Everything You Need To Know To Prepare Your Organization

By Aaron Chapman

If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography… is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

– National Institute of Standards and Technology (NIST), *July 2022*

The advent of quantum computers is a sci-fi fan's dream come true. These computers possess incredible, transformative power, enough to outdo today's super high-performance computers. For example, the Canadian company Xanadu Quantum Technologies reports that Borealis, their quantum computer in the cloud, "can perform a single task 50 million times faster than a classical computer."

Like most technology, this massive advance in computing power is a double-edged sword. While quantum computing can help solve some of humanity's more complex problems, it also paves the way for increased risk at the hands of bad actors—and experts think that quantum computers could be functional by 2030.

Businesses and government agencies that don't adequately prepare will find themselves vulnerable to data breaches and other cybersecurity threats. In this e-book, we will explore the various aspects of the quantum threat, and then we'll explain how to position your organization to stay ahead of the curve.

Part I: Understanding the Quantum-Computing Threat

In a matter of years, quantum-computing advances will have the power to break many of the public-key cryptosystems and encryption methods currently used to secure data and communications. Starting in 2015, the National Security Agency (NSA) raised alarm bells about the potential for hacking and data loss. Other governing and compliance bodies followed suit. Then, in March 2022, the Department of Homeland Security identified transitioning to post-quantum cryptography as a ***priority***.

The scope of the coming threat is hard to overstate. "National security systems could require the most urgent attention, but ultimately **all of U.S. communication infrastructure may need to transition to post-quantum cryptography.** This migration could be complex, costly, and occur over the course of decades," McKinsey recently affirmed.

The Three Risks of Post-Quantum Cryptography

Thinking about transitioning your organization's entire system to post-quantum cryptography feels intimidating, so it's helpful to break down the threat into short-term, medium-term, and long-term risks:

1. **Short-term risk: You wait to implement the new NIST standards.**
   Quantum computing is looming, but your organization is not ready because you're still waiting for "official" standards and protocols to be laid out. Currently, only the Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is available (NISTIR 8413). These reports identify which public-key cryptographic algorithms have been selected to protect information through the advent of quantum computers. Waiting for all eight standards to be approved and published means your organization will be behind the ball. Once NIST has its standards in place, businesses and agencies must be able to act quickly to gain compliance. Time is of the essence. The key here is for agencies to start securing better controls—*right now*—so that all the logistics are in place when NIST publishes its new standards.

2. **Medium-term risk: Your organization gets hacked.**
   The biggest risk, of course, is that the post-quantum "bomb" finally goes off and you are unprepared; your lack of readiness means your organization gets hacked or compromised, causing substantial damage. In some cases, it can take years for organizations to become compliant again after encryption is broken—and many organizations will not survive such an attack. Instead of trying to implement damage control and even retrofit systems with post-quantum cryptography solutions, companies and agencies should proactively reduce risk exposure.

3. **Long-term risk: Old communications put your organization at risk.**
   Once you've transitioned your operations to post-quantum cryptography, another risk remains. Organizations will have to sift through *everything* in their communication networks and ensure it is quantum-safe. This is a mammoth task, as it includes combing through every email exchange (or other network exchange) made over the course of your organization's history. When you reach this point, your organization can determine if swapping out cryptographic encryption is enough, or if another tool is needed in order to verify that your communications are safe.

Potential Quantum Disruptions

Quantum computing will allow bad actors to break the current cryptographic algorithms upon which our digital society relies—including technology created in pre-quantum times. According to McKinsey, some of these vulnerabilities include:

» **Data with a long shelf life.** For instance, a long-term life insurance contract, created years ago, may already be sensitive to future quantum threats. In fact, any long-term data is at risk of interception and future decryption.

» **Physical systems with long development timelines or operational lifetimes.** For example, automotive manufacturers are developing highly connected vehicles that have long development cycles (five years), production cycles (seven years) and vehicle lifetimes (10 years). That means a car developed today will likely still be on the road after 2040—and vulnerable to quantum threats.

Part II: Making a Plan

If you were moving to a new house, you wouldn't try to pack up everything as the truck was entering your driveway. Moving starts with taking inventory of everything you own, and then making a plan to tackle certain rooms first—and transitioning your organization to post-quantum cryptography requires similar planning. Here's a brief synopsis of the steps you should take, pre-migration.

- **Step 1: Inventory your systems.**
  Conduct a complete inventory of all systems currently using cryptographic technologies, such as public-private key pair and key signatures. You might be surprised at how many systems in your organization require cryptography

- **Step 2: Prioritize.**
  Next, identify where—and for what purpose—public-key cryptography is being used. Mark those systems as "quantum vulnerable." Remember that some legacy systems might be better to retire altogether.

- **Step 3: Create a migration plan.**
  Once you have a complete inventory of your technologies and have identified which systems are "crypto-agile," you can develop a migration plan for systems transition. This phased approach can include short-term, medium-term, and long-term goals, including mitigating security threats during the actual migration, maintaining hardware and software integrity, and maximizing the operability of your systems.

The Quantum Economy

Public and private sector organizations are increasingly investing in the oncoming quantum era. How big is quantum?

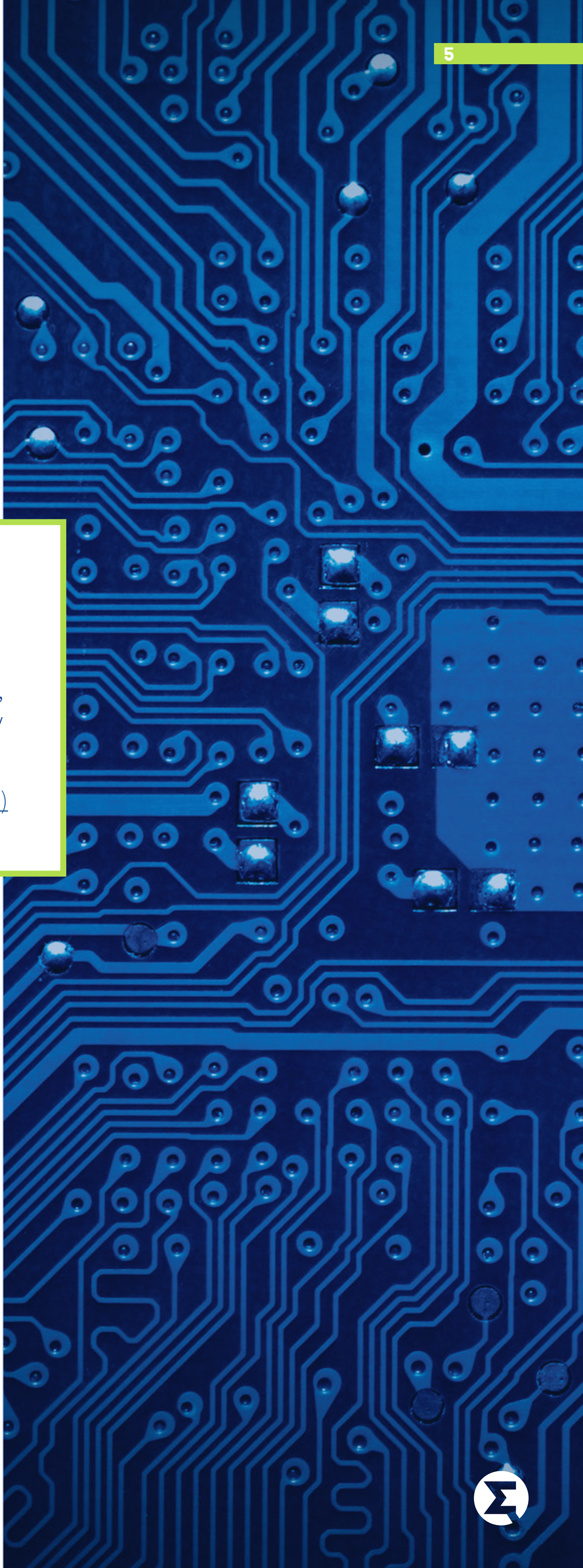
- Spending on quantum security will grow to about $3.5 billion in 2024.
- In 2021, the quantum-computer market earned $490 million, with estimates of public funding surpassing $24 billion.
- The cybersecurity market is forecasted to grow to $3 billion per year, reaching $30 billion by 2030.

Part III: Get Certified for Quantum Readiness

Making the transition to post-quantum cryptography is a monumental, systems-wide task. For organizations getting serious about seeking conformance to DHS and NIST recommendations for post-quantum planning and readiness, partnering can be a force multiplier. Enquizit's Post-Quantum Readiness Assurance Framework sets you up for success, helping you take control of the process and move forward strategically.

> Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.
>
> – National Institute of Standards and Technology (NIST)

Here's how our framework works. First, we help your organization conduct an inventory of all of your systems that use cryptographic technologies. From this inventory, we can identify where and for what purpose public-key cryptography is being used; then we mark those systems as "quantum vulnerable." Next, we develop a migration plan for these systems. This will ensure a smooth transition upon publication of the new post-quantum cryptographic standards. Finally, we ensure that your team is ready to do the migration. If not, our team is available to help, every step of the way.



The Post-Quantum Clock is Ticking

The upcoming transition to post-quantum cryptography is so massive and daunting that it's earned the name **"Encryptogeddon."** The key to success lies in assessing and mitigating risk exposure in a deliberate—not reactionary—fashion. To catch up to this powerful version of the future in which quantum computers are a reality, organizations must prepare ***now***.

Enquizit helps government agencies, universities, and large companies migrate to the AWS Cloud, and then optimize their operations once they are there. Want to learn more about Enquizit's Post-Quantum Cryptography Solutions? Visit us at www.enquizit.com.