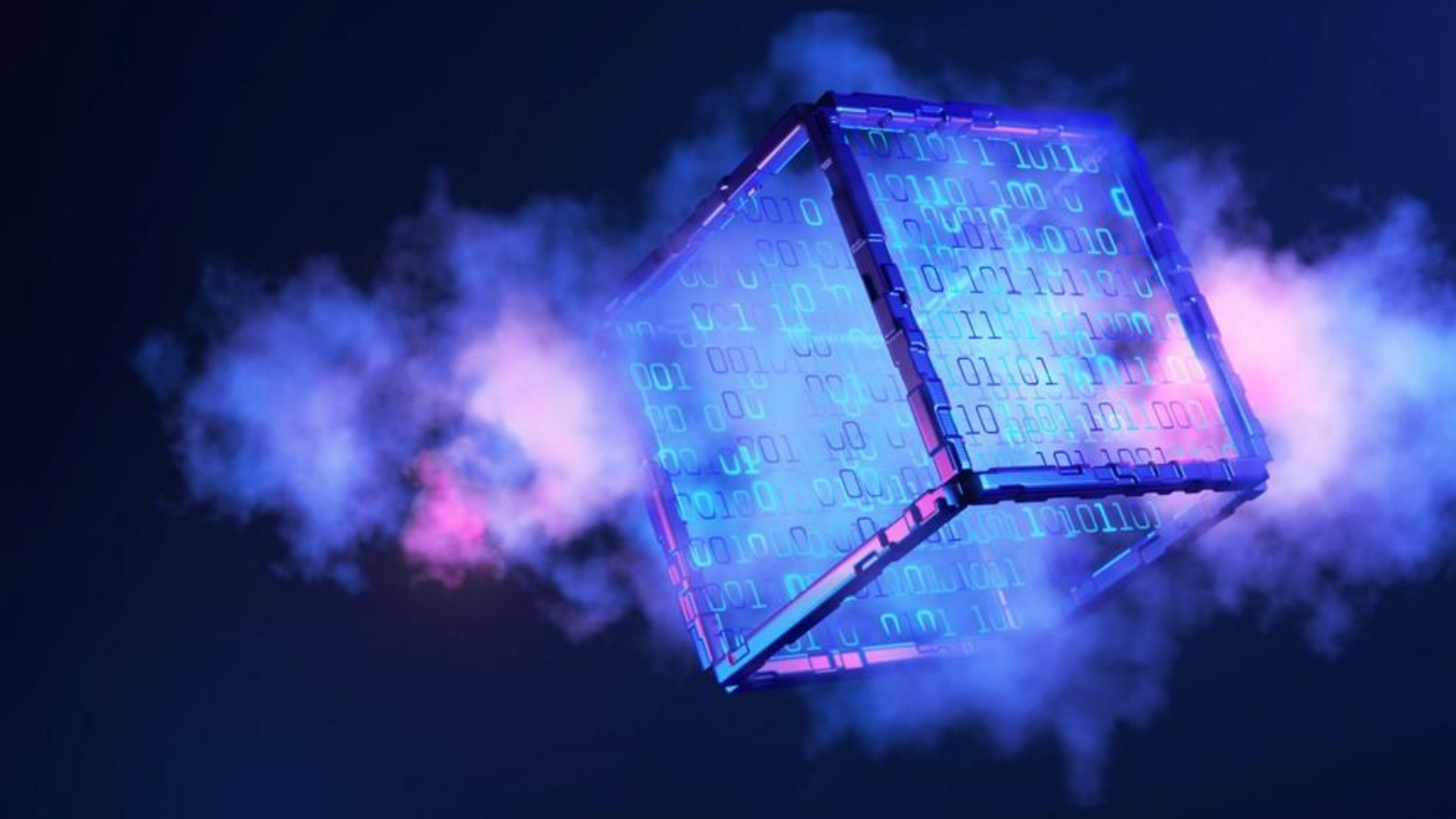
KPMG

The Next Cybersecurity Revolution

Post-Quantum Cryptography

KPMG Southern Africa
June 2024



Quantum computing is crumbling the very foundations on which the digital world has built its security protocols on

The quantum-computing revolution is upon us — a paradigm shift in computing power that harnesses the laws of quantum mechanics to solve problems far too complex for today's classical digital computers.

Quantum computers apply the unique behavior of quantum physics to computing, introducing unprecedented capabilities to traditional programming methods. From transforming drug research, energy use, manufacturing, cybersecurity and communications to enhancing AI applications, autonomous-vehicle navigation, financial modelling and more — quantum is poised to unlock a new reality.

Classical computing—also known as binary computing—relies on bits, which exist in one of two states at any point in time. Quantum computing uses Qubits which exist in multiple states simultaneously. This property means that quantum systems are uniquely suited for solving multi-variable problems that collapse to a single answer, reducing the time required to solve specific problems. One of these problems happens to be the cryptography algorithms that our digital world has built its security protocols on for the last 40 years.

Darren Lentz
Senior Manager
Technology Assurance
KPMG Southern Africa
+27 60 997 4815
darren.lentz@kpmg.co.za

Quantum's emerging threats demand solutions

One of the most significant cyber risks associated with quantum computers is their ability to break widely used cryptographic algorithms, such as RSA and elliptic curve cryptography (ECC). These algorithms secure data transmission and storage by relying on the computational difficulty of specific mathematical problems. However, quantum computers can solve these problems exponentially faster than classical computers, rendering current encryption methods vulnerable.

"Harvest-now, decrypt-later" attacks enable adversaries to steal encrypted files and encrypted communication over the web as we speak and store them until advancements in quantum computers emerge that enable them to decrypt this information.

Cryptography is the basis on which we achieve the principles of **Confidentiality**, **Authenticity** and **Integrity** in information security, which means the threat landscape is broad and the most unprecedented the digital world has ever seen. The risk landscape includes the following critical areas:

- Web browsing
- Storage
- Remote access and authentication protocols
- Software and Code signing
- Digital signatures
- Communication and data transfer
- Crypto currencies
- IoT devices

The quantum-risk landscape at a glance

There is little time to lose for organizations to gain a deeper understanding of the risks quantum may pose to their operations and security. For every organization that holds and processes data, they should consider the lifetime value of the data that they use, and the impact of that data being used or misrepresented by bad actors. For example:

Sensitive organizational data: Highly confidential data held by military services, national intelligence, finance and government organizations.

Critical infrastructure providers: Organizations whose complex systems are critical to the functioning of communities, cities, provinces and countries, including healthcare, transportation, utilities and telecommunications. Imagine, for example, the potentially disastrous impact of quantum disrupting the operation of a city's sprawling power grid.

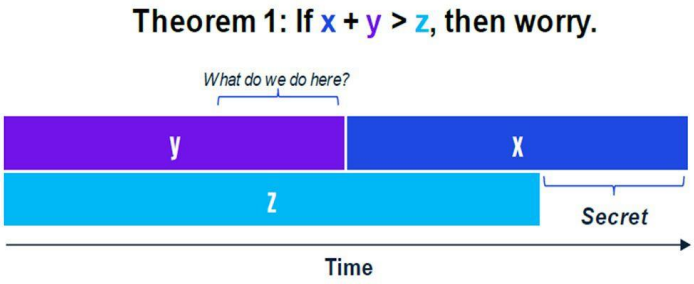
Long-life infrastructure providers: Organizations providing systems that are built to have a long life span for profitability, including satellite communications, payment terminals, Internet of Things (IoT) sensor networks and transportation. Whether data consists of customer information, medical records, biometric data or government classified data, a breach can have catastrophic financial, reputational and legal consequences. And some organizations are currently unaware of cyber attackers already accessing and storing encrypted company data with the aim of decrypting it in the future using a quantum computer.

Personal data handlers: Organizations managing personal data with a long confidentiality span are required by law to protect such data, including government, healthcare, financial firms and insurance organizations. They need to ensure protection over an extended period of 5, 10, 20 years or more.

"Quantum computing will upend the security infrastructure of the digital economy. Quantum technology in general promises to disrupt several areas of advanced technology and bring unprecedented capabilities that can be harnessed to improve the lives of people worldwide. At first glance it appears to be a curse to security, as cryptographic algorithms that proved to be secure for decades may be breached by quantum computers. This is in fact a blessing in disguise since this challenge gives us a much-needed impetus to build stronger and more-resilient foundations for the digital economy."

- Dr. Michele Mosca, Institute for Quantum Computing, The University of Waterloo

"Mosca's Theorem"[1], illustrated below, suggests the timeframe required to protect data. Dr. Michele Mosca's theorem stresses the need for organizations to begin applying diligence in the post-quantum space right away. It states that the amount of time that data must remain secure (X), plus the time it takes to upgrade cryptographic systems (Y), is greater than the time at which quantum computers have enough power to break cryptography (Z).



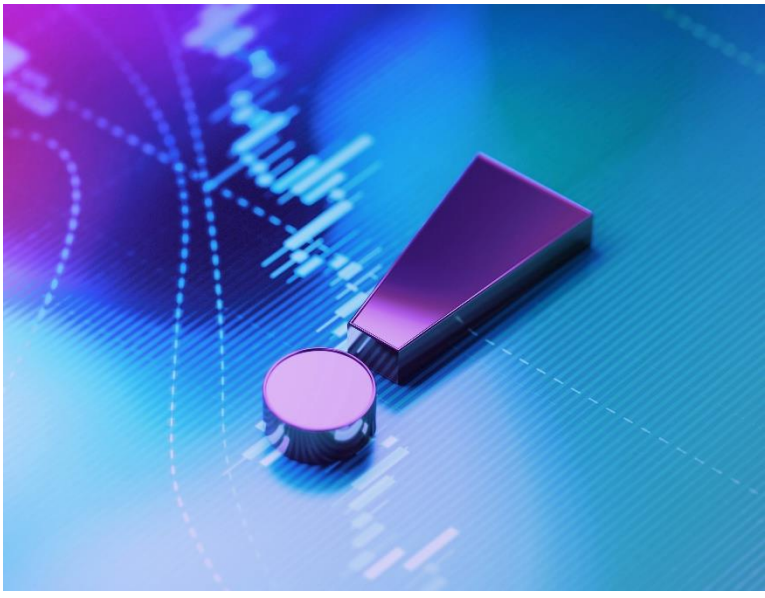
Preparation is key:

- **X:** number of years you need to keep your secrets safe.
- **Y:** number of years to re-tool your existing infrastructure.
- **Z:** number of years for a quantum computer to be built.
- If **X+Y > Z**, **risks** are **high** because **secrets are revealed**.

Once organizations are aware of their risk environment, they should be in a position to prioritize activity and mitigate or eliminate risks. However, this may not be a quick or simple process and may take years for each organization.

Managing technical debt, for example, can be a significant challenge for organizations relying on systems that will be incapable of running modern cryptographic profiles. There is now an opportunity to evaluate migration timelines and understand how long it will take to make infrastructure quantum resistant. To do this, organizations should understand the challenge and allocate budgets for both the mitigation and ongoing monitoring that the post-quantum world will require.

It's critical that organizations not only prepare for the quantum threat in their long-term risk planning, but also strengthen data protection now to help minimize quantum's potentially disruptive and costly impacts.



[1] Mosca's Theorem, Michele Mosca

Act now to help combat quantum's risks

While quantum computing may seem like a futuristic science fiction concept, the technology is indeed poised to exert major consequences across today's cybersecurity capabilities. We believe innovation is needed without delay.

The National Institute of Standards and Technology (NIST) has chosen four encryption tools that it says are designed "to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day." [2] The four encryption algorithms will become part of NIST's post-quantum cryptographic standard and all are expected to be finalized and ready for use in 2024.[3]

[2] https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

[3] https://csrc.nist.gov/projects/post-quantum-cryptography

Where to start as the power of quantum advances

Organizations can start to prepare by gaining a precise understanding of potential risks across their value chain. They should also identify methods to become more cryptographically agile in updating and deploying new cryptographic techniques as they become available. It's also crucial to create end-of-life strategies for the data, products and systems that will become obsolete or unable to support new cybersecurity requirements in a quantum-computing world.

Here are key questions to ask going forward as quantum evolves:

- How long does your data need to be secure and are you liable for its management?
- What is the actual and reputational damage in case of a compromise?
- How long will it take for your system to migrate to quantum secure protocols?
- Do you have an inventory of all your cryptographic assets?
- Are you liable for a third-party service or cloud provider and are they are moving to a quantum-safe environment?

Key actions to help mitigate quantum risks:

1. Provide insightful awareness training, education and roadmaps to senior leadership
2. Discover and identify current cryptographic assets
3. Implement roadmaps and solutions to modernize cryptographic environments
4. Provide guidance on investing in quantum-resistant technologies
5. Develop contingency and mitigation plans to prevent a quantum attack
6. Continuously monitor the fast-evolving quantum and security environment

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Document Classification: KPMG Public