Awareness Guide

for Securing Data in the Quantum Computing Era for the ICT Sector

2025

هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

EXECUTIVE SUMMARY

Not a fire drill, but a priority. Quantum progress puts **long-lived data** (e.g., health records, biometrics) and **digital signatures** at risk, enabling **"harvest now, decrypt later": attackers copy encrypted data today and unlock it when quantum-capable tools arrive**.

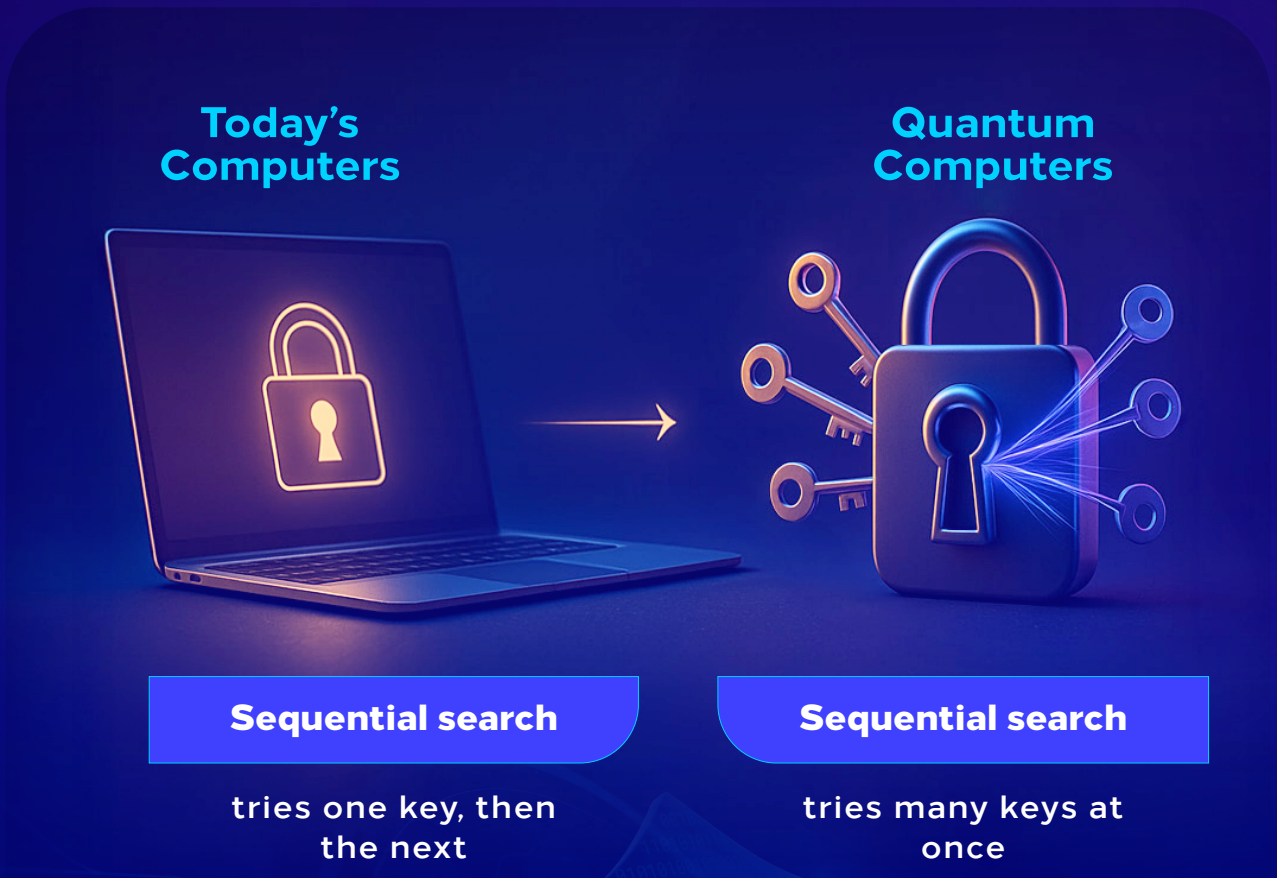
This awareness guide explains **what** quantum is, **why** it is important to act now to safeguard your sensitive services and data, and **how** to prepare with a simple 3-step plan to drive readiness across the organization.

WHAT IS QUANTUM COMPUTING?

Quantum computing is a new type of computing that helps us solve extremely complex problems. Unlike classical computers, which execute operations sequentially, a quantum computer can evaluate many possibilities at the same time.

Think of a lock with millions of keys: a normal computer tests them one by one, **a quantum computer can test many at once**.

For certain problems, **quantum computing makes the process much faster and opens new opportunities**, for example, in vaccine design, it can check huge numbers of molecule shapes at the same time, so promising options show up sooner.



WHY ACT NOW?

Encryption is like a giant puzzle that would take classical computers thousands of years to solve. A sufficiently powerful quantum computer could break it in hours or days, making today's digital locks unsafe.

Even before such machines arrive, the threat is real: attackers can copy encrypted data now and decrypt it later using future quantum power, a strategy known as **Harvest Now, Decrypt Later**. This drives the urgent need for **Post-Quantum Cryptography (PQC)** to protect sensitive data against future quantum attacks.

PQC involves developing **quantum-resistant encryption methods** that remain secure even against quantum-powered attacks.

Although the quantum threat has not yet fully materialized, history has shown this pattern before. Weak-by-design algorithms such as WEP and RC4 proved how quickly risk becomes real; similar weaknesses have had real-world impact.

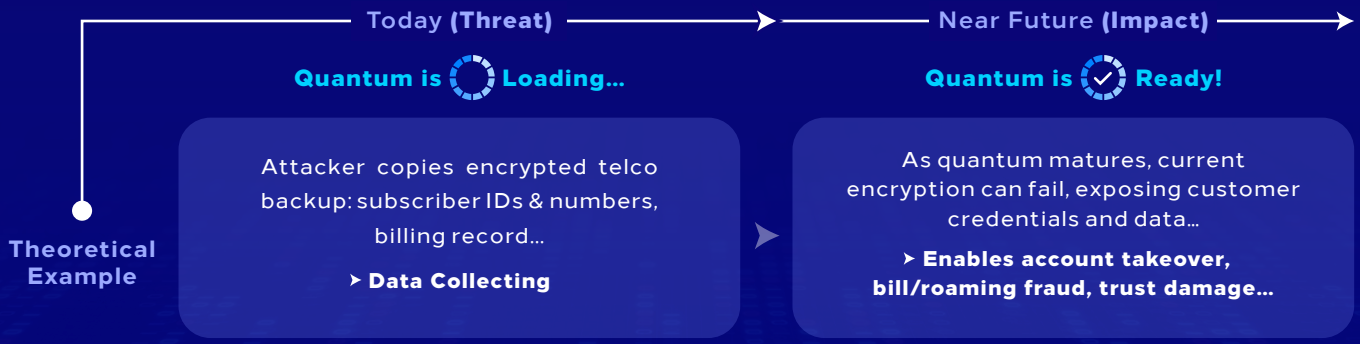
WEP Wi-Fi (2001–2007)

Many ISP-supplied home routers shipped with WEP by default. WEP used RC4 (an old encryption algorithm, now considered weak and deprecated) plus a short, repeating setup code, so by capturing some traffic attackers could crack the Wi-Fi key in 5–10 minutes. A 2007 retail breach exploiting WEP exposed **~45M payment cards with >$250M** in direct costs.[1]

RC4 in TLS (2013–2015)

Still protected ~30–50% of web traffic, yet a 16-character HTTPS cookie could be recovered in ~52–75 hour, **enabling account takeover**; RC4 was deprecated in 2015.[2]

Illustrative Example: How the Risk Plays Out



[1] BankInfoSecurity. (n.d.). TJX hacking incident shows cracks in payment card systems. https://www.bankinfosecurity.com/tjx-hacking-incident-shows-cracks-in-payment-card-systems-a-222

[2] Vanhoef, M., & Piessens, F. (2015). RC4 NOMORE. https://www.rc4nomore.com/

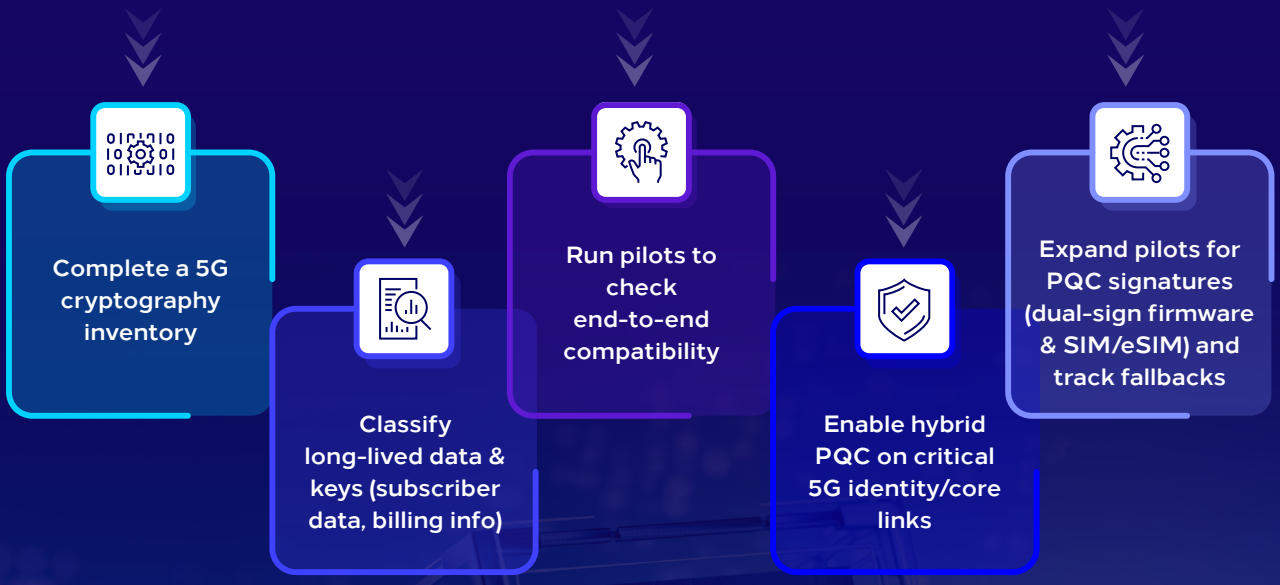
QUANTUM READINESS IN ACTION

The takeaway is clear: retire weak cryptography before incidents and adopt hybrid PQC now. Quantum isn't breaking production encryption today, but it is a near-term strategic risk for organizations with long-lived data and complex systems. A wait-and-see approach costs more: once weaknesses are exploited at scale, breach, compliance, and migration costs surge compared with early action.

Real-World Cases

Web platform (browsers/CDNs): According to Cloudflare Radar, hybrid post-quantum TLS now protects ~50% of HTTPS traffic globally. [3]

Telecom (5G pilot): A major telecom operator ran a pilot on a 5G network using post-quantum cryptography to protect customer data. The goal was to reduce "Harvest Now, Decrypt Later" risk and prepare to scale. Service worked as expected; errors were monitored. [4]



These examples shows that organizations can—and should—start preparing now.

[3] Cloudflare. (n.d.). Adoption and usage: Post-quantum encryption. Cloudflare Radar. Retrieved October 19, 2025, from https://radar.cloudflare.com/adoption-and-usage#post-quantum-encryption

[4] Weissberger, A. (2023, December 20). SK Telecom and Thales trial post-quantum cryptography to enhance users' protection on 5G SA network. IEEE ComSoc Technology Blog. https://techblog.comsoc.org/2023/12/20/sk-telecom-and-thales-trial-post-quantum-cryptography-to-enhance-users-protection-on-5g-sa-network/

A SUGGESTED COURSE OF ACTION

01

Identify Long-Term Exposure Areas

- Sensitive data with a long retention period (10+ years).
- Critical infrastructure systems and embedded devices.
- Legacy systems that are difficult to update.
- Cryptographic keys, credentials, and high-value internal assets.

02

Define Strategic Actions

- Define internal capability needs for post-quantum cryptography (PQC) adoption.
- Verify vendors' ability to shift to post-quantum cryptography (PQC).
- Monitor global guidance (NIST, ETSI, ENISA).
- Integrate PQC into transformation plans.
- Assign quantum risk to your enterprise risk register.
- Map and inventory all cryptographic assets and dependencies.
- Classify and prioritize data by longevity and sensitivity.

03

Drive Readiness Across the Organization

- Ensure quantum risk is addressed through governance oversight and board-level visibility.
- Build knowledge and capability through executive briefings, team training, and awareness sessions.
- Execute pilot projects with post-quantum cryptography (PQC) technologies and evaluate system and vendor crypto-agility.
- Leverage global resources such as the NIST PQC Migration Guide and ENISA briefings.

هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

cst.gov.sa