Singtel

Racing against the quantum threat

The quiet breach timeline

2015
Start of Quantum-Safe (QS) migration

2025
Last non-QS data exchange

2029
Quantum computers are publicly available

Non-QS data is vulnerable

Time required for QS migration

Long information lifetime

TIME TO MOVE QUICKLY... **ACT NOW**

Organisations need to plan now to ensure the long-term confidentiality of their critical information.

In the quantum era, cyber attackers intercept encrypted data and quietly store it away. They aren't trying to break it now, they're waiting. This tactic, known as **"hack now, decrypt later,"** banks on the moment when quantum computers gain the power to crack today's encryption. Sensitive information stolen today stays hidden for years, only to resurface when quantum capabilities make it vulnerable. By then, the damage—whether financial, personal, or national—will already be done.

Healthcare

Encrypted patient records, once considered secure, can be decrypted and sold. This poses a threat to patient privacy, regulatory compliance, and trust in healthcare systems.[1]

The butterfly effect

When encryption breaks, no sector is safe from quantum threats. It ripples across industries.

Critical infrastructure

From energy grids to banking systems, critical services depend on encrypted control systems. Quantum attacks could exploit firmware or steal credentials, disrupting entire economies.[2]

Supply chain

Signed firmware, cloud-access credentials, and sensitive IP are all at risk. Complex quantum supply chains create new vulnerabilities, while decrypted code can be copied, cloned, or corrupted.[3]

The quantum clock is ticking

From national strategies to tech breakthroughs, quantum computing is advancing. It's not too late to change course.

Predictions are everywhere

- **IBM pledged a quantum leap** by 2029, with Quantum Starling—a fault-tolerant quantum computer capable of executing 100 million quantum gates on 200 logical qubits.[4]
- **Global quantum arms races intensified.**
  - Japan launched its QX system, **capable of 100 trillion calculations per second.**[5]
  - South Korea committed **US$1.3 billion towards a 128-qubit system** by 2028.[5]
  - China surpassed **500 qubits with Tianyan-504** and outpaced Google with Zuchongzhi 3.0.[5,7]
  - Singapore launched the region's **first National Quantum-Safe Network Plus (NQSN+).**[8]

Quantified risks

65% of organisations
expressed concern about "harvest now, decrypt later" attacks.[10]

30% of businesses
confessed they were still ignoring the quantum threat altogether, citing a lack of budget and resources.[10]

Experts projected that it would take
12 years
for most enterprises to integrate quantum-safe standards fully. National security mandates have already marked 2035 as the deadline.[11]

What quantum safe should look like

Classical cryptography was built on binary logic — ones and zeros that held strong against traditional attacks. However, quantum computing introduced qubits, capable of processing vast possibilities simultaneously.

This exponential leap in power puts today's encryption at risk, exposing sensitive data to future decryption.

What's needed now is cryptography built for a quantum world that's resistant by design. It's why businesses need post-quantum cryptography, and Singtel's Quantum-Safe Network is built to deliver it.

Future-proof your business with Singtel Quantum-Safe Network

Singtel's Quantum-Safe Network (QSN) helps your business get quantum-ready to better protect your data transition to quantum-resilient architectures.

Post-Quantum Cryptography
Integrated with cyber security leaders like Palo Alto Networks and Fortinet.

Industry partnerships
Developed with Cisco, Fortinet, and Nokia to embed quantum-resistant protection across environments.

Scalable and future-ready
Offers a secure, flexible foundation that adapts to evolving enterprise needs.

Powered by PQC, scalable infrastructure, and trusted partners, **Singtel QSN** secures communications across sectors.

The story is fictional, the quantum threat is not. Start defending today with Singtel.

Prepare now

References

1 TechTarget, How can quantum computers be used in healthcare?, 2025
2 Quantum Insider, Quantum Computing And Critical Infrastructure: PQC Is Released, What Now?, 2024
3 Risk Ledger, The Opportunities and Risks of Quantum Computing for Supply Chain Cyber Security, 2024
4 IBM, How IBM will build the world's first large-scale, fault-tolerant quantum computer, 2025
5 Techwire Asia, Quantum Computing Challenges in APAC, 2024
6 Quantum Insider, China Introduces 504-Qubit Superconducting Chip, 2024
7 Quantum Insider, Chinese Researchers Say Latest Zuchongzhi 3.0 Experimental Run Matches Willow's Performance, 2024
8 National Quantum-Safe Network Plus, IMDA
9 KPMG, What is the cyber security risk from quantum computing?, 2024
10 Capgemini, Nearly two-thirds of organizations consider quantum computing as the most critical cybersecurity threat in 3–5 years, 2025
11 IBM, The quantum clock is ticking: How quantum safe is your organization?, 2024