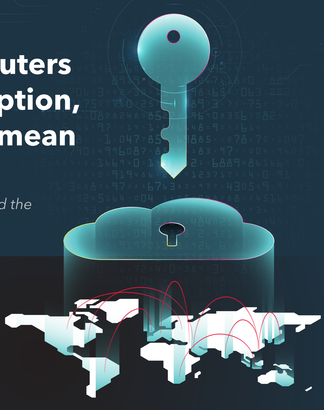
Singtel

Quantum computers can crack encryption, what does that mean for our safety?

How Quantum-Safe Networks hold the key to a new age of cyber threats



In the past, national security was all about protecting the physical, geographical borders of a country. Today, geopolitical warfare shifts to cyberspace at a global scale.

This also results in an increase in cybercrime targeted at businesses.

97%
Organisations saw an increase in cyber threats since rising geopolitical tensions in early 2022[1].

70%
Surveyed leaders stated that geopolitics has influenced their organisation's cyber security strategy[2].

The rise of quantum computing

Quantum computing – a major technology breakthrough on the horizon – could result in more cyber risks. Its potential to break through data encryption has most businesses and organisations already concerned.

73%
Businesses in the US believe the power of quantum will be used to disrupt cyber security[3].

95%
Respondents believe quantum computing's impact on cryptographic security systems is high.

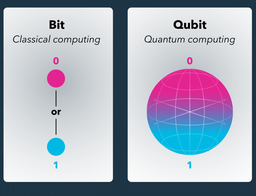
There are already significant investments being made in quantum computing research.

This has seen a drastic acceleration in quantum computing power over the years. Such advancements will amplify the need for new measures that protect data in the future.

$42 billion
Global public investments in quantum technology in 2023[4].

$173 billion
Potential quantum technology market size by 2040.

Why and how quantum computing threatens security



Quantum computers process information using qubits – which can be 0, 1 or both.

This helps them perform many calculations simultaneously, instead of step by step like a traditional computer.

This makes them solve encryption tasks like factorisation in minutes, while classical computers take thousands of years. This is a threat to the security of online data and communications.

Using quantum to defend against quantum

Quantum-Safe Networks can protect against quantum-based cyber threats by using the same principles of quantum physics. These networks include:

Post Quantum Cryptography (PQC)

Quantum-resistant cryptographic algorithms designed to defend against quantum attacks.

Cascading

Adoption of multiple algorithms – if one fails, the other still provides quantum resistant encryption.

Quantum Key Distribution (QKD)

Two remote parties agree on a shared secret key, which cannot be intercepted by an eavesdropper.

Singtel's Quantum-Safe Networks initiative

Appointed by the Infocomm Media Development Authority (IMDA), Singtel is developing Singapore's first Quantum-Safe Network to protect against emerging quantum threats.

- Quantum security solutions to protect enterprises against quantum threats
- A customised programme that can be tried out before adoption
- QKD is deployed over our extensive fibre network across the breadth of Singapore
- Integration with Singtel's domestic networks allowing for easy deployment

Stay ahead of emerging quantum threats with Singtel QSN.

Get in touch today

References

[1] State of Cybersecurity Resilience 2023, Accenture

[2] Global Cybersecurity Outlook survey, Insight Report, World Economic Forum and Accenture

[3] Quantum is coming — and bringing new cybersecurity threats with it, KPMG

[4] Steady progress in approaching the quantum advantage, McKinsey Digital