Singtel

Hackers are adapting to the quantum age. Is your cyber security ready?

The cyber security reality check

Traditional cryptographic methods rely on binary computation – ones and zeros – to secure information, effectively resisting conventional attacks and ensuring data integrity in a connected world.

But quantum computing changes everything. Unlike classical computers, which process data in binary, quantum computers use qubits – capable of existing in multiple states simultaneously – allowing them to solve complex problems exponentially faster.

This breakthrough threatens to break current encryption standards, making quantum-resistant cryptography essential to securing our digital future.

Binary (0s & 1s)

The foundation of today's encryption.

Qubits

Enables exponential computational power, making traditional security obsolete.

Why cyber security leaders should focus on quantum computing before it's too late

As qubits replace binary, quantum computing can crack even the most stringent encryption in minutes–something classical computers would take years to achieve. This imminent threat has cybercriminals preparing for **"harvest now, decrypt later" attacks,** where they collect encrypted data today, anticipating future quantum capabilities to break it.

Without quantum-resistant encryption, sensitive information stolen now could be exposed the moment quantum decryption becomes feasible.

78%

of U.S. enterprises expect quantum computing to go mainstream by 2030.[1]

73%

of U.S. businesses believe it's only a matter of time before cybercriminals use quantum to break today's encryption.[1]

81%

of U.S. organisations admit they need to improve their quantum security strategy.[1]

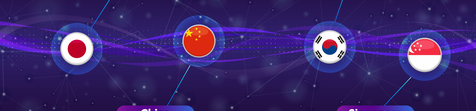
APAC's quantum race

Japan

Introduced its most advanced quantum computer, **QX**, in August 2023. With the power to execute **100 trillion calculations per second**, this superconducting qubit system is set to transform industries like finance, logistics, and manufacturing.[2]

South Korea

Announced a **US$1.3 billion investment** to advance quantum computing over the next decade, targeting to develop a **128-qubit system by 2028.** The plan also includes the creation of a dedicated quantum research hub and support for emerging quantum startups.[2]



China

Achieved **quantum supremacy** with two groundbreaking systems: **Tianyan-504** has set a new national benchmark, exceeding the 500-qubit threshold while matching global leaders like IBM in critical performance metrics, including qubit lifetime and readout fidelity.[3]

The Zuchongzhi 3.0 system, with 105 high-fidelity qubits, generated one million samples from an 83-qubit random circuit in seconds, outperforming Google's Sycamore processor.[4]

Singapore

Driving quantum innovation in Southeast Asia with initiatives, such as the Infocomm Media Development Authority launching Southeast Asia's first **National Quantum-Safe Network Plus (NQSN+)**, aim to fortify Singapore's resilience against quantum threats over the next decade.[5]

The shift from traditional security to quantum-safe solutions

Quantum security demands new expertise. Organisations must upskill teams in **quantum threat analysis, security tools, and zero-trust strategies** to stay resilient.

Moreover, they must prioritise quantum-proofing their networks – the foundation of secure communications and the first line of exposure to cyber threats. Without it, medical records could be altered, military communications intercepted, financial transactions compromised, and more.

The stakes aren't theoretical, they're immediate and real.

Tools for a quantum-safe future

Quantum Key Distribution (QKD)

While traditional cryptography methods rely on mathematical principles, QKD operates on the principles of quantum physics. It creates encryption keys by transmitting light particles across optical links, resulting in a more robust and resistant encryption method.

Post-Quantum Cryptography (PQC)

Not every system can adopt QKD immediately, but that doesn't mean businesses should wait. PQC strengthens existing encryption with quantum-resistant algorithms, securing critical data against future threats while maintaining seamless operations today.

By integrating QKD and PQC, businesses can future-proof their security, ensuring sensitive information stays protected in the quantum era.

How Singtel QSN helps you prepare for a quantum-safe future

Singtel is protecting your organisation with its **Quantum-Safe Network (QSN)**, delivering quantum-resilient encryption. With robust infrastructure and managed network expertise, we help fortify your organisation against future threats, ensuring long-term security for enterprises in finance, healthcare, government, and beyond.

PQC integration
with leading cyber security providers like Palo Alto Networks and Fortinet.

Industry partnerships
with Cisco, Fortinet, and Nokia to integrate quantum-resistant solutions into enterprise security architectures.

Singtel's QSN
secures business data with a scalable quantum-safe solution.

We're building a robust quantum security ecosystem, helping businesses stay ahead of emerging threats and secure their future communications.

Quantum-proof your network and protect your data with Singtel.

Contact us

References

1. KPMG, Quantum Is Coming – And Bringing New Cybersecurity Threats With It
2. Techwire Asia, Quantum Computing Challenges in APAC
3. Quantum Insider, China Introduces 504-Qubit Superconducting Chip, 2024
4. Quantum Insider, Chinese Researchers Say Latest Zuchongzhi 3.0 Experimental Run Matches Willow's Performance, 2024
5. https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/national-quantum-safe-network-plus