Fact Sheet

Cogito Group

Prepare for PQC now

Why prepare for Quantum Cryptography now?

Quantum computing poses both significant opportunities and challenges for current cryptographic systems. While widespread quantum computing might still be years away, organisations must begin preparing for post-quantum cryptography (PQC) today to mitigate future risks.

Here are key reasons why preparation is essential:

1. Quantum Computers Can Break Current Encryption

- **Risk to Cryptography**: Quantum computers, due to their advanced processing power, will be capable of breaking widely-used cryptographic algorithms such as RSA, ECC, and Diffie-Hellman. These algorithms form the backbone of internet security, protecting everything from online banking to private communications.
- **Vulnerability Window**: Data that is encrypted today with classical algorithms could be decrypted in the future once quantum computers become powerful enough. Sensitive information, if intercepted now, could be compromised in the future. This is known as the **"harvest now, decrypt later"** threat.

2. Long Cryptographic Transition Timeline

- **Complex Infrastructure**: Replacing existing cryptographic systems with quantum-safe alternatives is not a simple task. It involves updating not only encryption algorithms but also certificates, protocols, hardware, and key management systems.

- **Gradual Adoption**: Moving to PQC will likely take years, as organisations will need to:
    - Migrate digital certificates to quantum-safe versions.
    - Ensure new cryptographic standards are compatible with existing systems.
    - Manage hybrid cryptographic environments (using both classical and quantum-safe algorithms) during the transition.
- **Preparation Time**: The longer organisations wait to prepare, the more rushed and costly the transition will be once quantum computers become operational.

3. Post-Quantum Standards Are Emerging

- **NIST Standardisation**: The National Institute of Standards and Technology (NIST) is actively developing PQC standards. Once finalised, these standards will become the global benchmark for quantum-safe encryption.
- **Adopting Early**: Staying ahead of the curve by monitoring and adopting these standards early ensures a smoother transition once quantum-safe algorithms are officially recommended.

4. Regulatory and Compliance Requirements

- **Future Regulations**: Governments and industry sectors will soon mandate quantum-safe cryptography for securing sensitive information. By preparing now, organisations can ensure compliance with future regulations and avoid penalties or rushed transitions.
- **ISO Standards**: New cryptographic standards for quantum-safe algorithms will likely be incorporated into international standards, including those related to data privacy, financial security, and government communications.

5. Mitigating Business Risks

- **Prevent Data Breaches**: Failure to adopt quantum-safe encryption can lead to future data breaches, loss of intellectual property, or exposure of sensitive customer data.

- **Customer Trust**: Preparing for quantum cryptography shows that an organisation is proactive in ensuring the long-term security of its customers' data, thereby strengthening customer trust and reputation.

6. Industry Leadership and Competitiveness

- **First-Mover Advantage**: Organisations that prepare early for the quantum future can position themselves as leaders in cybersecurity. Being quantum-ready can become a competitive differentiator, particularly in industries where data security is critical (e.g. finance, healthcare, defense).

- **Innovation**: Quantum computing is expected to drive innovation in various fields, such as drug discovery, AI, and supply chain optimisation. Organisations that understand quantum technologies early can capitalise on these advancements.

7. Hybrid Cryptography Approach

- **Transition Period**: Before fully adopting PQC, hybrid cryptography (combining classical and quantum-safe methods) can help organisations secure their systems during the transition period. Preparing now ensures that companies are ready to implement these hybrid solutions.

- **Backward Compatibility**: It is important to ensure that quantum-safe solutions can integrate seamlessly with existing systems, requiring time for thorough testing and validation.

8. The Importance of Future-Proofing

- **Long-Term Data Security**: Many organisations store sensitive data with long retention periods (e.g., financial records, government documents). Ensuring that this data remains secure for the long term requires adopting quantum-safe encryption today.

- **Cyberattack Readiness**: As quantum computing technology progresses, cyber attackers are likely to exploit organisations that haven't transitioned to quantum-safe encryption, leading to data breaches or loss of service. Preparing now minimises this risk.

9. Cost and Resource Planning

- **Budgeting for Migration**: Transitioning to PQC requires both time and financial investment. Preparing now allows organisations to spread out costs over time, rather than facing high, sudden expenses once quantum computing becomes a reality.
- **Workforce Development**: Organisations need to train their workforce in quantum computing fundamentals and PQC to ensure that staff are equipped to handle the upcoming changes.

Conclusion

Preparing for quantum cryptography now is crucial to ensuring that your organisation is future-proofed against the coming quantum threat. While quantum computers capable of breaking current encryption may still be years away, waiting too long to prepare could leave your organisation vulnerable, scrambling to adopt new technologies. Proactive preparation helps mitigate risks, ensures compliance with emerging standards, and positions your organisation as a leader in security innovation.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.