GSMA

Guidelines for Quantum Risk Management for Telco

Executive Summary Version 1

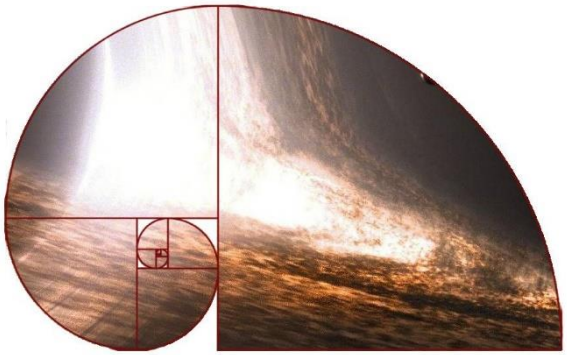
22 September 2023

XX Sept 2023

GSMA

Quantum Cryptanalytic Risk Management for Telcos

Cryptographically Relevant Quantum Computers pose new threats to telecommunication systems and significant new cybersecurity challenges because they disrupt some widely used encryption algorithms and protocols. A Quantum Cryptanalytic Risk Assessment informs a holistic, balanced, and full lifecycle risk management program that drives significant change to the cryptographic mechanisms used by network operators.



The overall objective is to ensure that key stakeholders and business owners have the information required to make proportionate, well-informed decisions in the right timeframes. Quantum Cryptanalytic Risk Assessment for Telecommunications is a critical methodology that supports network operators and the extended telecommunication supply chain in building a multi-year plan to address quantum risk.

Recommendations			
Governance	*Capability*	*Risk Management*	*Planning for Transition*
Build board-level awareness of the quantum risk. Establish an organisation-wide governance process to manage quantum risk. Identify an executive owner, and roles and responsibilities to include quantum risk.	Develop organisational capability to manage quantum risk. Update education and training programs to increase understanding of the quantum risk. Monitor the development of tools to facilitate the transition.	Adapt a Risk Framework to Manage quantum risk for your organisation. Integrate Quantum risk into Enterprise Risk Management. Perform a Quantum Cryptanalytic Risk Assessment to prioritise critical systems and data for mitigation. Identify and manage residual risk.	Determine the organisation's current cryptographic estate. Determine the organisation's data assets, data protection requirements, and data longevity. Prioritise the assessment of critical applications and services. Create a transition plan, based on the Quantum Cryptanalytic Risk Assessment and informed by the organisation's risk appetite.

Threat Identification

Two attack categories should be considered for threat identification:

- immediate threats from “Store now, Decrypt later” where sensitive data with a long shelf life can be accessed once a Cryptographically Relevant Quantum Computers is available; and
- future threats that originate from actors which will have access to Cryptographically Relevant Quantum Computers . The result of the impact assessment aids the analysis and prioritisation for identified threats.

Risk Frameworks

The document provides an analysis of how some common risk assessment frameworks, such as Mosca’s methodology, Crypto Agility Risk Assessment Framework, NIST Risk Management Framework, NIST Cybersecurity Framework and ISO may be adapted specifically for the telecommunications ecosystem, using relevant use cases as examples.

Common considerations across risk assessment frameworks and Quantum Cryptanalytic Risk Assessment include definition of roles and responsibilities, threat identification, asset and cryptographic inventory, impact calculation, and control selection.

The application of the risk assessment framework is an ongoing process. The identification of threats is dynamic:

- The discovery of new vulnerabilities,
- Changes in government and industry regulations,
- The issuance of updated best practice is all on-going,

requiring system update. As a result of all these processes, the cryptographic and asset inventory are dynamic.

Supply Chain

Introducing Quantum Cryptanalytic Risk Assessment into supply chain and business partnership relationships should be integrated in an organisation's overall risk plan. Whether that is through security requirements in formal agreements, or a general requirement that suppliers and partners are educated and aware of the quantum threat potential adverse impact on both companies.

Conclusion

- Organisations must consider how quantum computing impact their operations wherever cryptography is implemented.
- This typically takes the form of a risk assessment.
- Building the right teams and formulating mitigation plans is key to preparing for the quantum future.