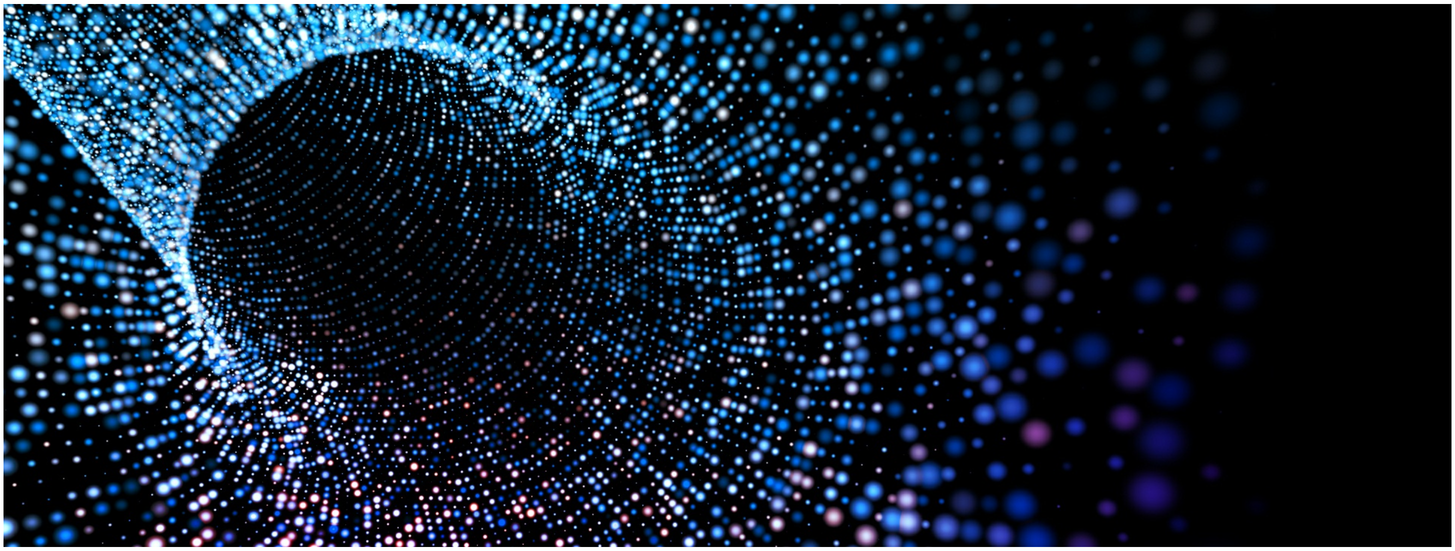
IBM Newsroom

IBM, Vodafone, and GSMA Members Outline Critical Pathways to Protect Telcos Against Quantum-Era Cyberthreats

Experts say adoption of standards within the next few years is essential to help secure telco data and infrastructure from quantum-powered cyberattacks



February 23, 2023 — As part of the Post-Quantum Telco Network Taskforce, GSMA has published, with contributions from members IBM, Vodafone, and others, the Post Quantum Telco Network Impact Assessment: an in-depth analysis of the quantum security threats facing the telecommunications industry and a detailed, step by step list of potential solutions to prepare for these threats.

The report, which debuted ahead of GSMA's annual Mobile World Congress in Barcelona, maps out a clear path for telco organizations to work across their ecosystems to protect data from cybercriminals acting today to tap into the potential power of future quantum computers. It includes:

- A telco-specific assessment of the business risk of quantum cyber threats, including four of the highest impact attack types: store now, decrypt later; code signing and digital signatures; rewriting history; and key management attacks.
- Discussion of standardization for hardware and software changes, such as SIM cards, public key infrastructure, digital certificates and CPE devices.
- Specific approaches to quantum-safe algorithms and risk assessment frameworks, including code-based, lattice-based, hash-based, multivariate-based, and hybrid approaches.
- Timelines of several government plans that have been launched to implement quantum-safe encryption (Australia, Canada, China, France, Germany, Japan, New Zealand, Singapore, South Korea, the UK and the U.S.).
- Examples of quantum-safe applications to several telco domains, including devices, 5G networks, SIMs, Operating systems, ERP, infrastructure and the cloud.

According to the report, it is widely considered that by 2032 there will be completion of a large fault-tolerant quantum computer capable of running crypto-analytic algorithms that could threaten current cryptographic approaches.

The advent of such technology requires immediate preparation, as some forms of attack may be retrospective (e.g. "store now, decrypt later”). Motivated bad actors may be harvesting and storing data now in order to decrypt it once certain quantum computing capabilities become available. As stated in the report, such actors may do this to “undermine the security of data with long-lived confidentiality needs, such as corporate IP, state secrets or individual bio-data.”

To learn more about these issues and what can be done today to protect against future quantum attacks, download thePost Quantum Telco Network Impact Assessment.

IBM has spent years building a global team of cryptography experts to develop quantum-safe schemes and preparation plans. Just in the last year, IBM not only contributed to the development of three of the four algorithms chosen in 2022 by the US National Institute of Standards and Technology (NIST) for post-quantum cryptography standardization; the team also deployed the industry’s first quantum-safe system, IBM z16; launched a suite of IBM Quantum Safe services; and was an initial member of the GSMA Post-Quantum Telco Network Taskforce.

Media Contact:

Resham Parikh
Resham.Parikh@ibm.com

---

https://stage.mediaroom.com/ibmnewsroom/2023-02-23-IBM,-Vodafone,-Other-GSMA-Taskforce-Members-Outline-Critical-Pathways-to-Protect-Telcos-Against-Quantum-Era-Cyberthreats