IBM Newsroom

IBM Report Details Steps to Secure Data for Quantum Era

As quantum-powered cyberthreats loom closer, experts outline a plan of action

YORKTOWN HEIGHTS, N.Y., January 17, 2023 - The IBM Institute for Business Value (IBV), IBM's thought leadership think tank, has published its Security in the Quantum Era report. This in-depth analysis of the quantum security landscape unveils the need for "quantum-safe" strategies today to maintain the integrity and security of highly sensitive data in the future. Additionally, the report maps out a clear path as to how organizations can work across their ecosystem to protect data from cybercriminals tapping into the power of quantum computers.

IBM security and cryptography experts provide clear actions on how organizations can:

- **Prepare for potential quantum threats** by educating teams on quantum-safe cryptography, such as the new algorithms identified by the U.S. National Institute of Technology, and how businesses can identify near-term and achievable cryptographic goals.
- **Discover potential vulnerabilities** by using quantum-safe cryptographic assessments, including how to place an ecosystem on a common approach to governance.
- **Transform operations** by performing analyses which can spot cryptographic dependencies between business-critical systems that might leave data vulnerable.
- **Observe the threat landscape** by developing a dashboard to promote visibility and observability.

According to the report, "Over the next several years, widespread data encryption protocols, such as public key cryptography standards like RSA and ECC, could become vulnerable. In fact, any classically encrypted communication which could be wiretapped is at risk, potentially already exposed to exfiltration, with the intention of harvesting that data once quantum decryption solutions are viable."

"Considering that the digital economy is estimated to be worth $20.8 trillion by 2025, the repercussions could be staggering," according to World Economic Forum, August 17, 2022.

Data related to national security, infrastructure, medical records, and intellectual capital can retain or increase in value over time. As such, cybercriminals can employ “harvest now, decrypt later” strategies to steal data which could be decrypted once quantum computers reach a critical mass. Additionally, cryptography is used to secure highly complex and critical infrastructure networks and global digital ecosystems, all of which could take decades to secure against quantum threats.

To learn more about why it is imperative that sensitive data must be secured today against future quantum attacks and how this can be achieved, download “Security in the quantum computing era”.

IBM has spent years building a global team of top cryptography experts to develop quantum-safe schemes and preparation plans. Just in the last year, IBM has deployed the industry’s first quantum-safe system, IBM z16; launched a suite of IBM Quantum Safe services; contributed to the development of three of the four algorithms chosen by NIST for post-quantum cryptography standardization; and became a founding member of the GSMA Post-Quantum Telco Network Taskforce.

For additional perspective on the immediate need for quantum-safe strategies, watch a virtual panel discussion between IBM, NIST, and Vodafone executives, moderated and recorded by The Economist:

Register: Commercializing Quantum Insight Hour

How to safe-guard data with post-quantum cryptography algorithms

Panel & Moderator:

- Dr. Scott Crowder, Vice President, IBM Quantum Adoption and Business Development
- Dr. Lily Chen, Manager of Cryptographic Technology Group, NIST
- Luke Ibbetson, Head of Group R&D, Vodafone Group
- Hal Hodson, Special Projects Editor, The Economist, moderator

Contact:

Chris Nay
IBM Communications
cnay@us.ibm.com
