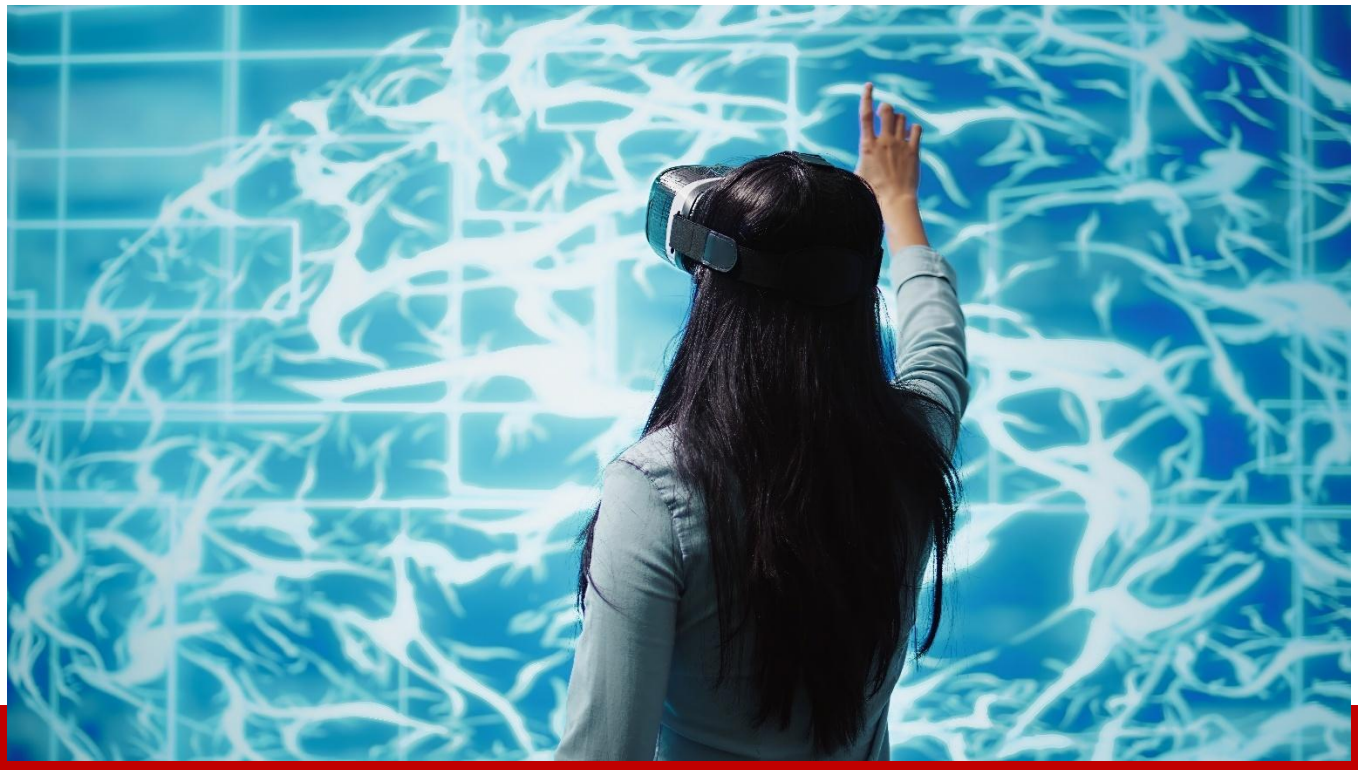

Quantum Computing is Coming: Enterprises Need to Prepare Now

Enhancing Cybersecurity with Post-Quantum Solutions

By Anurag Lal, President and CEO, NetSfere

Quantum computing is coming. When? No one knows for sure. Some experts say 10 years, others say 15 to 20 years.

Many believe quantum computers will be here even sooner. According to a recent survey of more than 900 quantum professionals by QuEra, over 50% of respondents indicated that the pace of quantum computing development is faster (41.2%) or much faster (10.2%) than they expected. The survey also revealed that 40% of respondents say quantum computing will become a superior alternative to classical computing for certain workloads within the next 5 years.

One thing all experts agree upon is that quantum computing is a matter of when not if.

While the arrival of quantum computing holds a lot of promise for advancing healthcare, scientific research, artificial intelligence, and other fields, it also presents cybersecurity risks for enterprises in every sector.

That's because quantum computers will be capable of cracking common cryptographic systems such as RSA that are widely used to protect data today.

Preparing for a post-quantum future that is 10-15 years away might not be a priority for organizations, but it should be. There are quantum attack risks such as harvest now decrypt later (HNDL) that are occurring today. In these HNDL attacks, cybercriminals steal encrypted data in anticipation of using quantum computers to decrypt it. They are mining data from messaging apps, collaboration tools, and other systems, putting sensitive business data at risk of exposure and exploitation. A recent Deloitte poll revealed that over 50% of professionals from organizations considering quantum computing benefits believe that their organizations are at risk for HNDL attacks.

A proactive approach to integrating post-quantum cryptography is an essential prepare now approach enterprises should take to safeguard the integrity and confidentiality of sensitive data and ensure a quantum-safe future.

Impact of quantum computing on current encryption methods

Quantum computers solve complex problems much faster than classical computers, making traditional cryptography algorithms vulnerable to quantum attacks. According to QuintessenceLabs, a conventional computer needs 300 trillion years to crack RSA 2048 prime number factor encryption. A 4,099-qubit quantum computer would need just 10 seconds to crack the same RSA key.

Gartner predicts that advances in quantum computing will make the asymmetric encryption used in almost all software, billions of devices worldwide, and most of the communications over the internet unsafe by 2029 and fully breakable by 2034.

Current landscape of post-quantum cryptography

Quantum-safe cryptography is now available to help organizations secure sensitive data and communications for the era of quantum computing.

This post-quantum cryptography (PQC) – also known as quantum-proof cryptography, quantum-safe cryptography, or quantum-resistant cryptography – is an entirely new field of cryptography that uses complex mathematics to protect data and systems from quantum computing attacks.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) recently finalized its principal set of post-quantum encryption standards designed to withstand cyberattacks from a quantum computer.

The result of an eight-year effort and ready for immediate use, these standards contain the encryption algorithms' computer code, instructions for how to implement them, and their intended uses.

NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

A proactive approach to PQC integration

Threats like HNDL highlight the critical importance of taking a proactive approach to integrating PQC and preparing for a quantum-safe future.

Even as the post-quantum future looms, many organizations are lagging in implementing PQC standards. A report by Entrust found that while 61% of global respondents plan to migrate to PQC within the next five years, less than half of organizations globally (41%) are presently preparing for the transition.

Considering that quantum computing risk affects systems, security tools, applications, and network infrastructure throughout the enterprise, integrating PQC is essential to protecting the security and privacy of sensitive data.

Enterprises can take the following proactive steps to help ensure a quantum-safe future:

- **Develop a PQC transition plan:** Create a plan for the integration of post-quantum cryptography into organizational infrastructure. This plan should include timelines for integrating PQC and allocate the resources needed for phased implementation.
- **Evaluate and inventory current cryptographic infrastructure:** A roadmap developed by the Department of Homeland Security (DHS) in partnership with NIST to reduce risks related to the advancement of quantum computing technology advises organizations to consider the following factors when evaluating a quantum vulnerable system:

1. Is the system a high-value asset based on organizational requirements?
2. What is the system protecting (e.g. key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
3. What other systems does the system communicate with?
4. To what extent does the system share information with federal entities?
5. To what extent does the system share information with other entities outside of your organization?
6. Does the system support a critical infrastructure sector?
7. How long does the data need to be protected?

- **Ensure third-party applications and services support post-quantum cryptography:** Understand the PQC status of third-party vendor technology such as communication and collaboration platforms. Not all solution providers are PQC-ready. Enterprises should ensure that the technology service providers they use support post-quantum cryptography now or are actively working to do so.
- **Monitor regulatory developments:** As a post-quantum future looms, policymakers will be updating compliance requirements related to PQC standards. Enterprises should monitor evolving regulations to ensure their cryptographic practices are compliant with current regulations and standards.

Wrapping up

The era of quantum computing is coming. To future-proof security, protect data against quantum attacks, comply with evolving regulations, and remain crypto-agile, enterprises need to prepare now.

About the Author

Anurag Lal is the President and CEO of NetSfere. With more than 25 years of experience in technology, cybersecurity, ransomware, broadband, and mobile security services, Lal leads a team of talented innovators who are creating secure and trusted enterprise-grade workplace communication technology to equip the enterprise with world-class secure communication solutions. Lal is an expert on global cybersecurity innovations, policies, and risks.

Previously Lal was appointed by the Obama administration to serve as Director of the U.S. National Broadband Task Force. His resume includes time at Meru, iPass, British Telecom, and Sprint in leadership positions. Lal has received various industry accolades including recognition by the Wireless Broadband Industry Alliance in the U.K. Lal holds a B.A. in Economics from Delhi University and is based in Washington, D.C. For more information, please visit https://www.netsfere.com/.