AI Threat or Quantum Threat: How Enterprise Should Be Prepared

Mrs. Manonmayi Vedam
Independent Researcher

Abstract: The growing concern around AI-driven cyber threats has often overshadowed a deeper structural weakness within enterprise security systems, namely the fragile state of cryptographic foundations that were never built for long-term resilience. While artificial intelligence amplifies the speed and scale of attacks, quantum computing introduces a more disruptive possibility, the obsolescence of widely used public-key encryption. The release of post-quantum algorithms by the National Institute of Standards and Technology marks an important milestone; however, the broader challenge extends beyond algorithm selection to issues of data sovereignty, interoperability, and delayed preparedness. Sensitive assets such as financial systems, healthcare records, national security data, and intellectual property remain exposed under a harvest now, decrypt later strategy already adopted by adversaries. This situation calls for a shift from reactive cybersecurity measures toward crypto-agility, where enterprises actively assess cryptographic inventories, align with emerging standards, embed quantum-resistant mechanisms, and integrate intelligent threat detection with durable encryption strategies. Leading cloud and technology providers including IBM, AWS, Microsoft Azure, and Google Cloud Platform have begun operationalizing quantum-safe initiatives through structured discovery, migration roadmaps, hybrid cryptographic models, and enterprise-wide inventory assessments. The transition toward quantum-safe security is not a temporary fix but a long-term architectural transformation aimed at ensuring governance, compliance, and institutional survival in an evolving threat landscape.

Keywords: Quantum-safe encryption, post-quantum cryptography, Crypto-agility, Data sovereignty, Harvest now decrypt later
All this not just for futureproofing but creating a resilient survival strategy.

How are different organizations are Operationalizing Quantum-Safe Security?

- IBM which contributed to two of the first three algorithms like CRYSTALS-Kyber (encryption) and CRYSTALS-Dilithium (digital signatures) selected by National Institute of Standards & Technology (NIST) for Post-Quantum Cryptography standardization set a pioneered approach on using an Enterprise-grade Quantum Safe Portfolio and Guardium Cryptography manager and their three-pronged approach of Discover, Observe and Remediate enables organizations to
  - Discover Cryptographic assets
  - Assess Quantum Vulnerabilities
  - Prioritize Remediation
  - Transition to Quantum-safe algorithms

  Their Integration with IBMZ a platform which includes built-in quantum-safe capabilities such as Z Crypto Discovery and Inventory (zCDI), secures mainframe environments. IBM also provides structured migration roadmaps for enterprises that are moving to pos-quantum cryptography which is not a patch to remediate but a multi-year architectural transformation.

- AWS's approach on deploying Post-quantum cryptography across several of its key services like AWS Key Management (AWS KMS), Amazon S3, and Amazon CloudFront have implemented post-quantum hybrid key establishment combining Elliptic Curve Diffie-Hellman (ECDH) with ML-KEM to protect against "harvest now, decrypt later" attacks. Services like AWS KMS and AWS Private CA support quantum-resistant signatures and roots of trust with ML-DSA. At the foundation of these implementations is AWS-LC, our FIPS-140-3-validated cryptographic library, which was the first open-source cryptographic module to include ML-KEM in its FIPS validation. Following their existing Shared responsibility Model AWS Plan and implement the PQC upgrades and work on three-pronged approach of Prioritize, Encrypt and Protect
  - Prioritization and Inventory of Enterprise Workloads and Dependencies.
  - Encrypt for Confidentiality by segmenting the services and experiences of Enterprises for migration to Post-quantum cryptography

- Protect against future impersonation by establishing quantum-resistant roots of trust is critical for systems through post-quantum capabilities that can be used for code signing.

- At Microsoft Azure the advancement in Quantum computing is through the Microsoft Quantum Safe Program (QSP) which protects their enterprise infrastructure. Microsoft developed the Majorana 1 quantum processor, 4D geometric error correction codes to align with requirements for PQC and the Azure Quantum Resource Estimator to investigate how enterprise's quantum computing will impact common encryption algorithms.
  The QSP strategy is guided by the three priorities:
  - Make Microsoft quantum safe by updating Microsoft first- and third-party services, supply chain, and ecosystem to become quantum safe and crypto-agile.
  - Support customers, partners, and ecosystems to become quantum safe with appropriate tools and guidance.
  - Promote global research, standards, and solutions for quantum-safe technologies and crypto-agility.

- GCP's approach on Quantum computing is slightly different from the rest of the Cloud Service Providers. They believe that Threat Model, Crypto Agility, and Crypto Key Inventory of Enterprise's Infrastructure would better protect from attacks.
  - Google's Threat model for Post-Quantum Cryptography
  - Cryptographic Agility and Key Rotation

CONCLUSION

AI-driven cyber risks and quantum computing challenges are interconnected but distinct forces exposing long-standing weaknesses in enterprise cryptographic design. The core vulnerability lies not merely in advanced attack techniques but in outdated encryption systems and incomplete cryptographic inventories that limit governance and compliance readiness. Post-quantum standards provide direction, yet sustainable protection requires structured migration, continuous inventory assessment, and integration of quantum-resistant algorithms across hybrid environments. Industry initiatives from major cloud providers demonstrate that quantum readiness demands coordinated planning, workload prioritization, and redesigned trust architectures rather than isolated upgrades. Organizations that move toward crypto-agility, combining long-term cryptographic resilience with intelligent threat monitoring, will be better positioned to safeguard sensitive data and maintain operational continuity in the face of emerging computational capabilities.