Frequently Asked Questions on Financial Sector Risks from Quantum Computing

1. **What is the threat quantum computing poses to current cryptography?**

   Cryptographic algorithms currently used to secure communications over the internet will become vulnerable to successful attacks when a cryptographically relevant quantum computer is created. Adversaries could use quantum machines maliciously to defeat our current encryption technologies with relative ease.

2. **Why should organizations begin planning for a post-quantum cryptography environment now?**

   Transitioning to new technologies for a post-quantum cryptography environment is a sizeable task that takes significant time to complete. As your organization plans its migration to quantum-safe protocols, consider the time needed to secure data, the migration time to cryptographic systems that are secure against both quantum and classical computers, the time for a cryptographically relevant quantum computer to become operational, and the time needed to coordinate with external partners, test systems, and train your workforce. Planning now for this change in security capabilities will expedite your organization's security transition so that it is ready once a cryptographically relevant machine is created.

3. **How long will it take for a cryptographically relevant quantum computer to be operational?**

   This is currently unknown; however, experts that the G-7 CEG has consulted suggest that there is a high enough possibility for the development of a cryptographically relevant quantum computer within a decade to create urgency in beginning the lengthy process of deploying defensive measures.

4. **You mention the need to start planning now, but the quantum threat is not expected to materialize for several years at the soonest. If the threat may be several years away, why can't firms just wait to see how the technology develops?**

There are several factors driving the need to start planning now, including:

1. **Implementation timeline:** It will take significant time for firms to develop governance structures and plans for their transition to post-quantum technologies. Implementation will be very time consuming, especially for large organizations with multiple forms of encryption technologies in use. All these technologies will need to be identified and migrated to safer technologies, and this effort will need to be coordinated with a wide range of third parties with whom the firm communicates.
2. **Testing:** Changes to encryption technologies have the potential to create performance issues in the systems that rely on them. These systems will need to be tested to ensure they still operate according to expectations.
3. **Harvest now, decrypt later:** Adversaries may be collecting encrypted data today with the expectation that they will be able to decrypt these data once quantum technologies are available. Any data that are not protected from quantum computing threats now are potentially vulnerable to decryption by adversaries at a later date.

5. **What should I be asking of my vendors today?**

   Engage with your third-party vendors to discuss their post-quantum roadmaps and timelines, how they intend to address the quantum threat, and what impacts the transition will have on their customers.

6. **What are the National Institute of Standards and Technology (NIST) Post Quantum Cryptography public-key algorithms?**

   In 2017, NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key algorithms. Three digital signature algorithms – CRYSTALS-DILITHIUM, FALCON, and SPHINCS+, as well as one public-key encryption and key establishment algorithm – CRYSTAS-KYBER, were chosen. Three Federal Information Processing Standards (FIPS) have been published by NIST in August 2024 based on these algorithms:

   1. **FIPS 203:** Specifies a cryptographic scheme called Module-Lattice Based Key-Encapsulation Mechanism (ML-KEM), which is derived from the CRYSTALS-KYBER public-key encapsulation mechanism submission. It is designed for general encryption purposes, such as creating secure websites.
   2. **FIPS 204:** Specifies the digital signature scheme called the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), which is used for identity authentication and data threat detection and is derived from the CRYSTALS-DILITHIUM submission.
   3. **FIPS 205:** Specifies the digital signature scheme called Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), which is derived from the SPHINCS+ submission.

   NIST is planning to release a fourth FIPS specifying a digital signature algorithm based on FALCON in late 2024 and further FIPS in the future.

7. **Should organizations purchase commercial post-quantum cryptography solutions now?**

   While some quantum resilient technologies may be available for purchase now, it will take time for vendors to fully incorporate these technologies within products and services. Once post-quantum cryptography solutions that integrate the standards developed by NIST are available, organizations should integrate them into their security capabilities.

8. **What resources or reports can readers refer to learn more about what international organizations are doing to prepare for a quantum future?**

   Other international agencies, groups, and standard setting bodies are exploring the matter, including NIST, the European Union Agency for Cybersecurity (ENISA), the Bank of International Settlements (BIS), and the U.S. Department of Homeland Security (DHS).

   For more information on how these organizations are exploring the implications of quantum cryptography, please visit:

   NIST: Post-Quantum Cryptography | CSRC (nist.gov)

   ENISA: Post-Quantum Cryptography - Integration study — ENISA (europa.eu)

BIS: Project Leap: quantum-proofing the financial system (bis.org)

DHS: Post-Quantum Cryptography | Homeland Security (dhs.gov)