OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

Post-Quantum Cryptographic Inventory: A Vital Step for Future Security

July 11, 2025

— Categories: Crypto

As the world edges closer to a quantum computing revolution, a new term is gaining traction in cybersecurity circles: “cryptographic inventory.” With quantum computers poised to dismantle existing encryption standards, understanding this concept is crucial for any organisation aiming to safeguard its digital assets in the coming decade.

The term “Q-day” refers to the moment when quantum computers become capable of breaking widely used encryption algorithms like RSA-2048 and ECC-256. These algorithms currently protect vast swathes of sensitive data, estimated at 200 zetabytes globally. Experts predict Q-day could arrive within the next three to fifteen years, with IBM’s recent roadmap suggesting the early 2030s as a likely timeline for this “quantum apocalypse.”

The stakes are high. Sophisticated hackers and state-backed actors are already engaging in “harvest now, decrypt later” strategies, stockpiling encrypted data for future decryption. A successful attack by a Cryptographically Relevant Quantum Computer (CRQC) could expose sensitive information and cause economic losses in the trillions.

Western governments are not standing idle. The White House and the European Union have issued post-quantum cryptography (PQC) roadmaps to guide critical sectors, including government agencies, financial institutions, and private enterprises. Last year, the National Institute of Standards and Technology (NIST) published its first PQC standards under the Federal Information Processing Standard (FIPS). These standards include three deployable algorithms, with a fourth in development, selected from 82 submissions since 2016.

The UK, alongside the US and EU, has set ambitious deadlines: highly sensitive organisations must transition to PQC algorithms by 2030, with all others following by 2035. This shift will render current public key cryptography obsolete, underscoring the urgency of preparation.

At the heart of any robust cybersecurity strategy lies a simple principle: you cannot protect what you do not know. A cryptographic inventory, a comprehensive catalogue of an organisation's cryptographic assets, is the foundation for transitioning to a quantum-safe environment. Without it, organisations risk being blindsided by the quantum threat.

Cryptographic infrastructure underpins digital trust, securing everything from financial transactions to sensitive communications. As Vladimir Soukharev, Vice President of Cryptographic Research and Development at InfoSec Global, a Keyfactor Company, stated in a recent interview with Cybernews, "Many organisations don't realise how tremendous this transition is." Soukharev, a co-author of the July whitepaper Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow, produced in collaboration with HSBC and Thales, emphasises the scale of the challenge.

The 31-page report, shared exclusively with Cybernews, outlines how organisations can address current cryptographic weaknesses while meeting compliance requirements and minimising business risks. It warns that the transition to PQC will be technically complex, resource-intensive, and may not be feasible for some legacy systems. "Realistically, it should be done as soon as possible," Soukharev advises. He recommends completing the inventory process by the end of 2026 to meet the 2030 deadline for sensitive organisations.

The whitepaper highlights the need for clear timelines to avoid underestimating the resources required. "If companies only focus on the final deadline, they're likely to face delays," Soukharev notes.

The transition to PQC will affect every layer of technology, encrypted network traffic, digital signatures, certificates, software, hardware, cloud services, IoT, 5G, AI, blockchain, and more. The whitepaper advocates for automation to streamline the discovery of cryptographic assets, given the inefficiency of manual processes and the dynamic nature of modern IT environments.

However, automation has its limits. The report notes that many tools struggle with compatibility across on-premises, cloud, and hybrid systems, potentially creating blind spots. Human oversight remains essential to ensure comprehensive coverage. Soukharev is cautious about relying on artificial intelligence for this task, warning that “AI often provides improper, outdated, and wrong expertise” in the complex field of cryptography. He also highlights security concerns, noting that cryptographic inventories contain highly sensitive data that should be processed on-premises to avoid compliance risks.

For Chief Information Security Officers (CISOs) and other technology leaders, the message is clear: preparation must begin now. A cryptographic inventory is not just a technical exercise; it is a strategic imperative for ensuring business continuity in a post-quantum world. By starting early, organisations can mitigate risks, comply with emerging standards, and secure their place in a quantum-safe future.