BTR: Quantum Threats Are Rising, and So Are the Tools to Fight Them

SILVER SPRING, MD, UNITED STATES, September 9, 2025 /EINPresswire.com/
-- The global race toward practical quantum computing is accelerating, prompting an urgent effort across government and industry to prepare today's digital infrastructure for the moment conventional encryption breaks.

> 2025 is becoming the year when everyone realizes they're behind. If your data needs to stay protected for the next five or ten years, and it's not quantum-safe today, it's already at risk."
>
> *Rebecca Krauthamer, QuSecure*

Known as "Q-Day," that theoretical milestone — when quantum computers mature to the point that they defeat current cryptographic systems — could arrive by the end of this decade, according to security experts. Based on recent White House Executive Orders to advance quantum readiness, a growing number of experts believe it could come sooner. While the exact timing is uncertain, the threat is already active. Adversaries are harvesting encrypted data today in anticipation of decrypting it once quantum capability catches up.

"People talk about Q-Day like it's a future event," said Rebecca Krauthamer, Co-Founder and CEO of QuSecure, a cybersecurity company that provides post-quantum cryptography (PQC) solutions, in a recent executive conversation. "But from a risk management perspective, we're already there. Data that's being stolen now could be exposed later by quantum technology. This is worrisome for data that has a long shelf life, like medical records, intellectual property, or classified communications."

Krauthamer, whose background includes advanced artificial intelligence (AI) and quantum algorithm research, launched QuSecure after a U.S. Air Force grant prompted her to explore the national security implications of quantum decryption. The company's flagship platform, QuProtect, is designed as an encryption overlay to help organizations prepare for post-quantum threats without overhauling their infrastructure while also allowing them to take inventory of their current encryption.

Beyond Bigger Computers: A Different Type of Threat

Unlike classical machines, quantum computers don't just process faster — they process

differently. By leveraging the principles of superposition and entanglement, quantum machines can explore multiple problem-solving paths simultaneously, giving them the ability to break today's most widely used public key encryption methods.


Rebecca Krauthamer, QuSecure

"At scale, with about 4,000 error-corrected qubits, a quantum computer could reverse-engineer the mathematical problems underlying conventional encryption," Krauthamer said. "A quantum machine could solve in hours a problem that could take longer than the heat death of the universe for a classical computer."

This vulnerability is not just theoretical. Governments around the world — including the U.S., U.K., Australia, and South Korea — have launched formal efforts to develop and adopt PQC. In the United States, the National Institute of Standards and Technology (NIST) finalized its first set of PQC algorithms in 2024. These are now part of a broader federal mandate for agencies to begin migrating to quantum-resistant systems.

Crypto-Agility: The New Security Paradigm

The technical solution to quantum threats lies in math — specifically, in cryptographic algorithms designed to resist quantum attacks. But the implementation challenge is strategic and architectural, not just mathematical. Effective defense lies in deploying new cryptographic algorithms that are mathematically resistant to quantum attacks. The real challenge is not inventing the math, but integrating these algorithms across complex, legacy systems in a scalable and agile way.

"As a result, you don't need a quantum computer to defend against one," Krauthamer said. "What you need is the ability to swap out your encryption algorithms — quickly, centrally, and at scale. That's what crypto-agility is all about."

Rather than treating post-quantum cryptography as a one-time upgrade, the principle of crypto-agility treats the challenge associated with the threat as a continuous operational requirement. QuSecure's platform enables this flexibility across distributed environments. Its software establishes a "service mesh" that layers quantum-safe encryption controls over existing networks

without requiring users to replace legacy systems or modify end-user behavior.

“It’s like putting a secure, quantum-ready blanket over your communications,” Krauthamer explained. “It is a smart cover that lets you change algorithms at the push of a button as new threats or standards emerge.”

From Fighter Jets to Financial Networks

While QuSecure’s roots are in military applications — including encryption for aircraft and satellite communications — its platform is now being adopted across telecommunications, banking, and critical infrastructure sectors. These are industries where sensitive data is not only high-value but also long-lived, making it especially vulnerable to “harvest now, decrypt later” attacks.

Krauthamer cited one ongoing use case involving aging aircraft like the B-52 bomber. “You can’t send a technician into space or retrofit legacy planes every time encryption standards change,” she said. “So we’ve built a digital solution that allows secure key exchanges and post-quantum encryption upgrades without needing to physically replace systems.”

The same logic applies to data centers, financial systems, and cloud environments that span decades-old mainframes to next-generation SaaS. QuSecure’s architecture is designed to integrate across this sprawl, automatically discovering where encryption lives and ensuring crypto-agility across each layer — from device to application.

While awareness of quantum threats has long been confined to government labs and academic circles, regulatory momentum is bringing the issue into the C-suite. Since 2022, a series of executive orders, national standards, and legislative mandates have created a formal migration timeline in the U.S. and abroad.

“We’re seeing a massive shift,” Krauthamer said. “2025 is becoming the year when everyone realizes they’re behind. If your data needs to stay protected for the next five or ten years, and it’s not quantum-safe today, it’s already at risk.”

Several countries have announced formal post-quantum migration plans. Australia has set a 2030 deadline. The U.K. and South Korea have published draft frameworks and moved up quantum-safe deadlines. The European Union is expected to release its roadmap in the summer of 2025. In the U.S., NIST and CISA have launched guidance requiring federal agencies to adopt quantum-safe standards and demonstrate crypto-agility across their networks.

Economics of Agility

According to Krauthamer, the economics of crypto-agility are compelling. Traditional encryption upgrades often involve multi-year, manual migrations — including labor-intensive inventories

and custom patching across disparate systems.

“We have customers who’ve been through this before,” she said. “They’ve spent years identifying where encryption lives, coordinating vendor upgrades, and ensuring compliance. With crypto-agility, all of that becomes a push-button process that makes it possible to avoid the usual sunk costs and complexity.”

The model also creates downstream value. Telecommunications providers, for instance, are beginning to treat post-quantum readiness as a competitive differentiator — offering it to customers as part of premium data protection packages.

“Cybersecurity has traditionally been viewed as a cost center,” Krauthamer said. “Now, crypto-agility is creating new revenue opportunities. It’s not just about protecting data. It’s about building trust in your digital infrastructure.”

Despite the clear threat, many organizations remain passive — unsure of how to assess the risk or begin the transition. Krauthamer emphasizes that the first step doesn’t require a deep understanding of quantum mechanics or cryptography.

“You don’t need to be a quantum scientist to prepare,” she said. “You just need to know what kind of data you have, how long it needs to be protected, and whether it’s being transmitted securely.”

The time to act, she added, is now.

“Some data, once stolen, can’t be recovered — no matter how strong your encryption becomes later,” Krauthamer warned. “The only real protection is to adopt post-quantum cryptography before that data is compromised. That means identifying your vulnerable assets and making sure they’re protected today, and not when Q-Day inevitably arrives.”

Click Here to Read the Q&A Based on this Interview.

Airrion Andrews
BizTechReports
email us here