GSK Global CISO Warns: The Quantum Threat to Enterprise Security Is Already Here

GSK CISO warns quantum threats are already impacting enterprise security as "harvest now, decrypt later" risks accelerate PQC migration urgency.

GSK Global CISO Warns: The Quantum Threat to Enterprise Security Is Already Here

BOSTON, MA, UNITED STATES, May 12, 2026 /EINPresswire.com/ -- The transition to post-quantum cryptography has become one of the most urgent challenges facing enterprise cybersecurity.

According to Michael Elmore, SVP and Global Chief Information Security Officer at GlaxoSmithKline, organizations that fail to act early risk falling irreversibly behind as quantum computing advances toward real-world impact.

Quantum computing is no longer a distant concept. It is an advancing capability with the potential to break widely used encryption standards that underpin global digital infrastructure today. For organizations managing sensitive, long-lived data, the implications are immediate.

> For industries like healthcare and pharmaceuticals, where sensitive data must remain protected for decades, waiting is not an option."
>
> *Michael Elmore*

Adversaries are already adopting "harvest now, decrypt later" strategies, collecting encrypted information today with the expectation that it can be decrypted in the future. As will be explored by industry leaders at Quantum.Tech World taking place June 25 & 26, some of the most valuable enterprise data may already be exposed, even if it remains unreadable for now.

"Post-quantum security is no longer a future problem we can simply ignore or expect vendors to solve for the Enterprise — it's a resilience challenge that will require a new crypto agility approach for future-proofing your crypto resilience," said Michael Elmore, SVP and Chief Information Security Officer, GSK. "For industries like healthcare and pharmaceuticals, where

sensitive data must remain protected for decades, waiting is not an option."

Elmore is expected to outline a practical roadmap for enterprise readiness, emphasizing that the transition to post-quantum security is a multi-year effort requiring immediate action. Key priorities include:

- Establishing full visibility through cryptographic inventories
- Building crypto-agile systems capable of adapting to new standards
- Prioritizing protection of high-risk, long-life data
- Implementing phased, scalable migration strategies

For industries such as pharmaceuticals, where intellectual property, clinical trial data, and patient records must remain secure for decades, the stakes are particularly high. In this context, quantum resilience is becoming a defining factor in long-term competitiveness, regulatory compliance, and organizational trust.

Key Takeaways:

- Global encryption standards are approaching obsolescence
- Sensitive data may already be compromised through "harvest now, decrypt later" strategies
- Post-quantum migration will take years and must begin immediately
- Enterprise, telecom, and government leaders are aligning on action
- These discussions are taking place at Quantum.Tech World 2026 this June

An Industry-Wide Shift, Not an Isolated Warning

This is not a single perspective. It reflects a broader alignment across enterprise, infrastructure, and global standards bodies, all coming together at Quantum.Tech World 2026:

- At IBM, Jai Arun will explore how quantum-safe security and crypto-agility are being embedded into enterprise systems, in "Quantum Computing and Quantum-Safe Security: Scaling Innovation and Securing the Future of Enterprise Computing."
- At AT&T, Rich Baich will address "Entangled Horizons: The Future of Quantum Networks," highlighting how next-generation infrastructure must evolve to support secure quantum-era communications.
- From the National Institute of Standards and Technology, Lily Chen will lead discussions on PQC standards and migration strategies, alongside Rajesh Patil and Steven Menges from enQase, focusing on how organizations transition to quantum-safe and crypto-agile systems in practice.

Across these sessions at Quantum.Tech World, the direction is clear:

- The risk is real and already emerging
- The transition will take years, not months

- The organizations acting now will define the next era of digital trust

Where Enterprise Security Strategy Moves Into Execution

Quantum.Tech World 2026 will bring together leaders from across the Fortune 1000 and global enterprise landscape, including IBM, AT&T, GSK, Mastercard, ExxonMobil, BMO, Boeing, Lockheed Martin, Verizon, Roche, AbbVie, Moderna, and more, alongside government agencies, national laboratories, and leading research institutions.

Quantum.Tech World is where the industry's biggest organizations are actively shaping the next era of computing and cybersecurity, bringing together:
- 1,000+ senior decision-makers across enterprise, government, and research
- 150+ speakers working on real-world deployment across quantum, AI, and HPC
- All 17 U.S. Department of Energy National Laboratories

Attendees will gain insight into:
- How leading organizations are approaching post-quantum migration today
- What crypto-agility looks like in practice at enterprise scale
- Where critical vulnerabilities still exist across sectors
- How quantum, AI, and HPC are converging into a new computing and security stack

 Quantum.Tech World 2026
 Register now to join the conversations

Millie Evans
Alpha Events
quantum.tech@alphaevents.com
Visit us on social media:
LinkedIn
Instagram
YouTube
