FOR IMMEDIATE RELEASE

99% of Fortune-1000 Companies Lack Quantum Cybersecurity Programs as Computing Threats Accelerate

Qryptonic survey of 147 CISOs reveals critical readiness gaps; JPMorgan Chase and HSBC case studies demonstrate successful quantum-secure implementations

NEW YORK, NY — June 17, 2025 *— Only 1% of Fortune-1000 companies have established funded, board-mandated quantum cybersecurity programs, according to new research from Qryptonic Research LLC. The finding comes as quantum computing advances rapidly, with recent hardware breakthroughs significantly shortening the timeline for potential encryption vulnerabilities.*

The survey, conducted in May 2025 with 147 Chief Information Security Officers from Fortune-1000 enterprises, found that while 74% of companies are conducting assessments or limited pilots, 25% have no quantum migration plan at all. The research highlights a dangerous gap between the accelerating pace of quantum development and enterprise preparedness.

Quantum Computing Milestones Compress Timeline

Recent quantum computing achievements underscore the urgency:

- *IBM demonstrated its "Condor" system with 1,121 qubits (December 2023)*
- *Google's "Willow" achieved 105 error-corrected qubits, bringing RSA encryption vulnerability within a decade (December 2024)*
- *IonQ's $1.08 billion merger with Oxford Ionics targets fault-tolerant processors by 2029 (June 2025)*

"The quantum computing landscape has transformed from theoretical risk to imminent business challenge," said Jessica Gold, Head of Marketing and PR at Qryptonic. "Organizations collecting encrypted data today face the real possibility of that data being decrypted by quantum computers tomorrow."

Industry Disparities in Quantum Readiness

The research reveals significant variations across sectors:

Leading adoption: *Financial services (40%), government agencies (35%), and critical infrastructure*

Lagging sectors: *Manufacturing (10%), retail (15%), and logistics*

This disparity is corroborated by independent research from Deloitte (November 2024) showing only 30% of organizations taking meaningful action, despite 52% assessing their exposure.

Proven Implementation Paths

Major financial institutions are demonstrating successful quantum-secure implementations:

***JPMorgan Chase** deployed a Quantum-Secured Crypto-Agile Network (Q-CAN) across three U.S. data centers, achieving:*

- *100 Gbps hybrid TLS implementation using X25519 + Kyber-768*
- *45-day pilot with minimal latency impact (+6 ms)*
- *$30 million in new assets under management from quantum-aware clients*

***HSBC** successfully secured tokenized digital bonds using post-quantum cryptography:*

- *Achieved 1,000 transactions per second using Dilithium signatures*
- *Received FCA regulatory sandbox approval*
- *Completed first fully PQC-secured digital bond issuance in the EU*

Federal Investment Underscores Urgency

The U.S. government has allocated $7.1 billion for federal quantum cryptography migration from fiscal year 2025-2035, with the Quantum Computing Cybersecurity Preparedness Act mandating full cryptographic inventories by 2027.

"Organizations must prepare now. The transition journey will be lengthy and demands global cooperation," noted Matt Scholl, Chief of NIST's Computer Security Division, in 2024 guidance that led to NIST's finalization of post-quantum cryptography standards including CRYSTALS-Kyber and CRYSTALS-Dilithium.

Qryptonic Offers Rapid Assessment Solution

To address the critical need for quantum risk assessment, Qryptonic has developed Q-Scout™, a comprehensive cryptographic inventory service that identifies quantum vulnerabilities in seven days. The service provides:

- *Complete cryptographic inventory from cloud to operational technology*
- *Risk-weighted scorecard aligned with NIST and ENISA standards*
- *Board-ready 12-month migration blueprint*
- *Typical identification of $3-5 million in quick-win cost savings*

"You can't mitigate what you don't measure," said Jason Nathaniel Ader, Co-Founder and Chief Innovation Officer at Qryptonic and author of **The Quantum Almanac 2025-2026**. *"With 99% of Fortune-1000 companies unprepared for quantum threats, immediate action is crucial for maintaining competitive advantage and ensuring long-term security."*

About the Research

The Qryptonic Quantum-Risk Survey was conducted in May 2025, interviewing 147 Fortune-1000 CISOs across multiple sectors through anonymous questionnaires with follow-up validation. The full research report and methodology are available at qryptonic.com/quantum-research.

About Qryptonic

Qryptonic: Post-Quantum Ready — Permanently.

Qryptonic is the global leader in enterprise post-quantum security advisory, providing vendor-neutral cryptographic risk solutions for financial institutions, governments, and high-risk industries. We help organizations achieve permanent cryptographic resilience before Q-Day 2028, and keep them protected against Harvest Now, Decrypt Later attacks.

Qryptonic Research LLC is a division of Qryptonic, LLC, dedicated to advancing quantum cybersecurity research and developing actionable insights for enterprise quantum readiness.

Access Q-Scout™ Quantum Risk Assessment

Organizations can rapidly assess their quantum vulnerability exposure with Q-Scout™, Qryptonic's NIST-aligned cryptographic inventory service backed by a $1 million guarantee. The comprehensive assessment is delivered in just seven days.

For more information or to initiate your quantum risk assessment, visit qryptonic.com/q-scout or contact our enterprise team at (888) 2-QRYPTONIC.

Media Contact

Jessica Gold
Head of Marketing and PR
Qryptonic, LLC

Secure Your Enterprise for the Quantum Era

Offices: New York, NY | Miami, FL | Be'er Sheva, Israel
Email: info@qryptonic.com
Phone: +1 (888) 2-QRYPTONIC