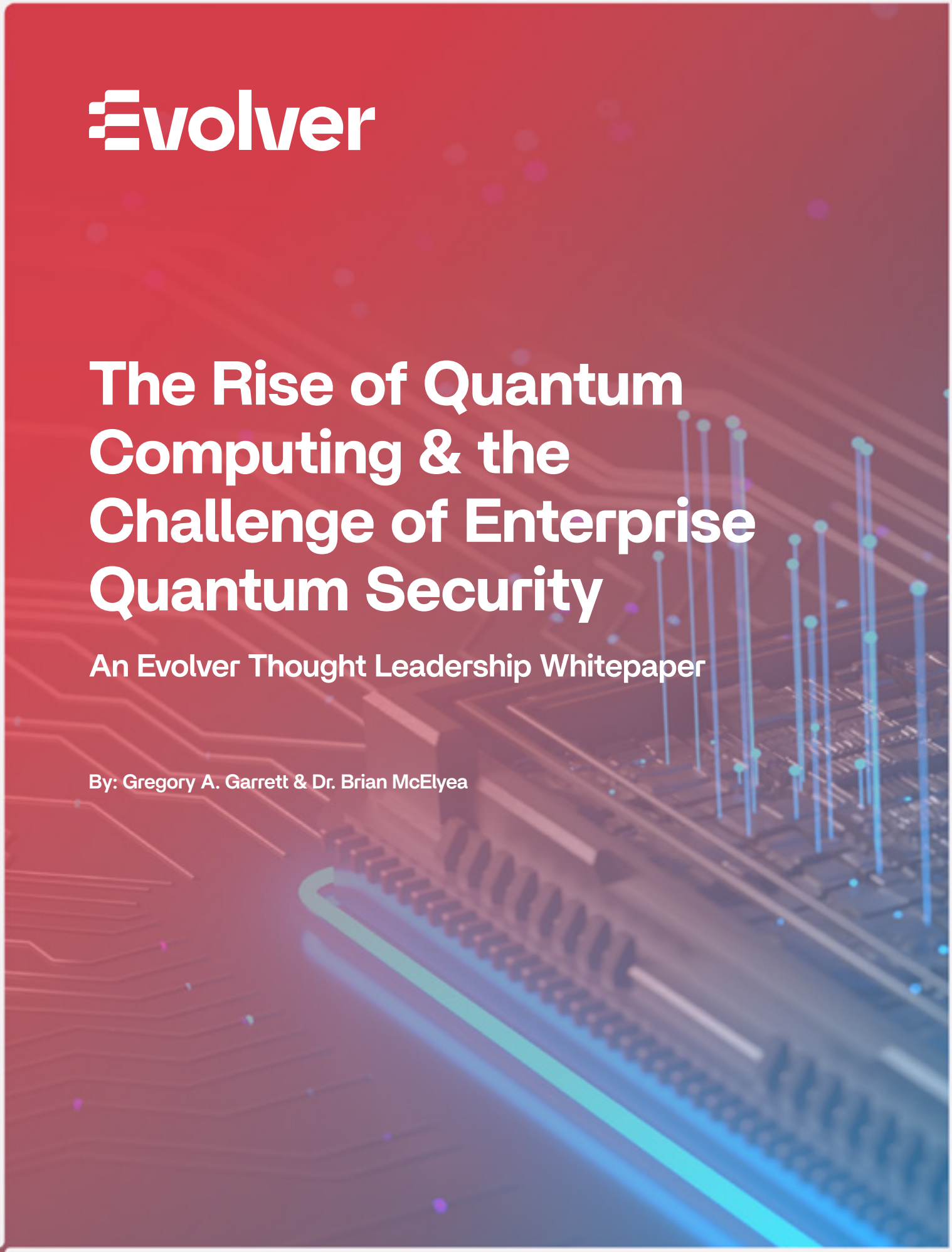
Evolver

The Rise of Quantum Computing & the Challenge of Enterprise Quantum Security

An Evolver Thought Leadership Whitepaper

By: Gregory A. Garrett & Dr. Brian McElyea



Executive Summary

Quantum computing is rapidly transitioning from a theoretical possibility to a practical engineering race. As qubit counts, fidelity, and error-correction techniques improve, the global technology ecosystem is preparing for a future in which quantum computers can solve certain classes of problems dramatically faster than classical computers.[1] Among those problems are he hard math assumptions (integer factorization, discrete logarithms, elliptic curves) that underpin today's public-key cryptography. [2]

This emerging capability has triggered a significant and immediate concern across the U.S. Federal government and industry: a cryptographically relevant quantum computer (CRQC) could render widely deployed software encryption schemes, especially RSA and elliptic-curve cryptography (ECC), effectively obsolete for confidentiality protection. Adversaries, especially nation-state cyber-attack groups are already engaging in "harvest now, decrypt later" (HNDL) operations: mass-collecting encrypted traffic and sensitive archives today in anticipation of breaking them once quantum computers and algorithms mature. [3]

In a memo dated November 18, 2025, the U.S. Department of War, stated ,"Advancements of Quantum Information Science (QIS) and crypto analytically relevant quantum computers requires expedited migration to quantum-resistant cryptography to safeguard the Department's information systems, communications, and personnel."

This whitepaper examines:

- **"The Good" –** how quantum computing promises breakthroughs in materials science, logistics, healthcare, and optimization.
- **"The Bad"** – the specific ways enterprise security architectures are exposed to quantum decryption risk.
- **"The Ugly"** – plausible negative scenarios once Nation-state cyber-attack groups and criminal cyber-attacks groups operationalize quantum capabilities.
- **"The Solutions"** – post-quantum cryptography (PQC), quantum key distribution (QKD), crypto-agility, and data-centric patterns such as "Shrink, Shred, Send & Recombine (3SR)" as components of a quantum-safe strategy.

This paper integrates practical "Pro Tips" throughout and concludes with a logical roadmap for enterprise quantum security, emphasizing cryptographic inventory, crypto-agility, PQC migration, and use of QKD and 3SR techniques aligned with the NIST, "PQC Standardization Process" and the United States, National Security Agency (NSA), Encryption Consulting.

PRO TIP

Executive Alignment: Establish a board-level quantum risk statement. Even a one-page brief that links quantum timelines, data longevity, and regulatory expectations give CISOs and CIOs the mandate to launch PQC discovery and pilot enterprise quantum security capabilities before they become compliance emergencies.

1. The Rise of Quantum Computing: "The Good"

1.1 Quantum principles and computational advantage - Classical computers encode information in bits that are either 0 or 1. Quantum computers use qubits, which can exist in superpositions of 0 and 1, and become entangled so that the state of one qubit is correlated with others. These properties allow certain algorithms to explore exponentially large state spaces more efficiently than classical computers for problem types.[4]

Not every workload benefits from quantum acceleration, but for specific problems such as factoring large integers (Shor's algorithm), searching unsorted spaces (Grover's algorithm), or simulating quantum systems,) quantum computers can outperform classical systems at scale.[5] This asymmetry is at the heart of both the opportunity and risk for enterprise cybersecurity.

1.2 NISQ-era systems - We are currently in the Noisy Intermediate-Scale Quantum (NISQ) era: devices with tens to low thousands of physical qubits, limited coherence times, and significant noise.

These systems are not yet CRQCs capable of breaking modern cryptography, but they are already being tested on:

- Quantum simulation for chemistry and materials (e.g., catalysts, batteries, pharmaceuticals).
- Optimization problems in logistics, portfolio construction, and scheduling.
- Machine learning and sampling for specific niche tasks.

Major technology vendors, national labs, and startups are scaling qubit counts, exploring error-correcting codes, and experimenting with different physical implementations: superconducting qubits, trapped ions, neutral atoms, photonics. Press coverage refers to an eventual "Q-Day" when a CRQC can break widely used cryptosystems; some expert surveys put non-trivial probability on this occurring before 2035. Some research suggests it could be as early as 2029. [6,7]

1.3 Economic and mission benefits - For large commercial companies and U.S. Federal government agencies, quantum computing promises:

- Faster R&D cycles by simulating molecules and materials at atomic precision, reducing the need for expensive physical experimentation.
- Enhanced optimization of supply chains, transportation, and energy grids, potentially driving cost savings and resilience
- Risk analysis and portfolio optimization in finance, improving scenario exploration and hedging.

These "good" outcomes drive aggressive investment in quantum R&D by the U.S., European Union, China, and other nations.[8] However, the same algorithms that accelerate beneficial workloads also undermine the hardness assumptions that keep today's encrypted data safe.

PRO TIP

Strategic Opportunity Mapping: Create a dual-track quantum roadmap: one lane for mission use cases (simulation, optimization) and another for security impacts (PQC transition). Treat them as a single portfolio so that every quantum innovation project also budgets for cryptographic and data protection.

2. The Challenge of Enterprise Quantum Security: "The Bad"

2.1 Public-key cryptography (PKC) - Most enterprise security architectures rely on public-key cryptography for:

- TLS/HTTPS key exchange for web traffic.
- Virtual Private Network (VPN) tunnels between sites and users.
- Email encryption and digital signatures.
- Code signing, firmware validation, and device attestation.

Algorithms such as RSA and ECC rely on the difficulty of factoring large integers or solving discrete logarithm problems. Shor's algorithm shows that a sufficiently large, error-corrected quantum computer can solve these problems in polynomial time, making current key sizes effectively breakable. [9, 10]

Even if a CRQC is not yet available, cybersecurity decisions must account for data lifespan. Highly sensitive information (e.g., classified material, critical infrastructure designs, and medical records) must remain confidential for decades. If an adversary were to record encrypted traffic today and decrypt it in five, ten or fifteen years, the damage could still be severe, which is a core driver of the HNDL threat model. [11, 12]

2.2 Regulatory and policy drivers - U.S. federal policy is already aligning around post-quantum cryptography (PQC):

- NIST Post-Quantum Cryptography Standardization has selected several algorithms—CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON, and in August 2024 published three Federal Information Processing Standards (FIPS 203, 204, 205) for key encapsulation and digital signatures.[13]
- The NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) sets targets for transitioning National Security Systems to quantum-resistant algorithms(QRAs) by the early 2030s, with full migration for U.S. federal systems aiming to complete around 2035 [14, 15]

Enterprises doing business with U.S. Federal government agencies or regulated sectors will be under increasing pressure to inventory their cryptographic assets, demonstrate plans for crypto-agility and PQC migration, and align with emerging sectoral guidance.[16, 17] Without a deliberate strategy, organizations risk a fragmented, ad hoc response, creating inconsistent security guarantees and new failure modes. [18]

Start with a Crypto Inventory: Treat cryptographic asset discovery as a first-class project, not a side task.

Use a combination of:

- Code scanning for libraries and key sizes,
- Network inspection for protocol usage (TLS, SSH, IPsec), and
- Vendor questionnaires for embedded and third-party systems.

Tag each use case with data sensitivity and required confidentiality lifetime; this becomes your PQC migration priority matrix.

3. The Possible Negative Consequences of Quantum-Powered Cyber-Attackers: "The Ugly"

Once CRQCs become operational for adversaries, the cyber threat landscape could shift in several ways. While timelines are uncertain, scenario planning is essential. [19, 20]

3.1 Mass decryption of historical data - Adversaries engaging in HNDL operations today—recording VPN traffic, exfiltrated databases, satellite links, and encrypted messaging—could later apply quantum cyber-attacks to:

- Decrypt sensitive diplomatic and military communications, revealing historical negotiations, alliances, and operational details.
- Expose long-lived personal data, such as healthcare records, genomic data, and financial histories
- Compromise distributed ledger systems whose signature schemes are not quantum-safe, undermining the integrity of past transactions.[21]

In some cases, the historical record itself becomes a weapon for coercion, blackmail, or strategic manipulation. [22]

3.2 Attacks on critical infrastructure and government systems - A quantum-capable adversary could exploit weakened cryptography to impersonate privileged users or devices by forging digital signatures, break VPNs and secure tunnels protecting operational technology (OT), and subvert software update channels to deliver signed malware into critical environments.[23] Because many of these systems have long lifecycle components, they are especially exposed to long-horizon quantum threats.[24]

3.3 Financial markets and digital assets - Financial institutions, exchanges, and custodians depend on strong cryptography for transaction integrity, secure APIs, and protection of proprietary algorithms. A CRQC could, in principle, undermine legacy signature schemes used in blockchains and cryptocurrencies, enabling double-spend or key theft, and older PKI-based schemes that have not migrated to PQC.[25] The result could be rapid erosion of trust in digital financial infrastructures, with cascading economic impacts.[26]

War Game Quantum Breach: Run a cybersecurity tabletop exercise that assumes an adversary can retroactively decrypt five years of your encrypted email and messaging traffic. Challenge stakeholders to answer:

- Which datasets would cause the most damage if exposed?
- Which identities and trust anchors would be undermined first?
- How would you re-establish trust in software updates and remote access?

Use the lessons to refine your PQC priorities, data minimization, and incident response playbooks.

4. Post-Quantum Cryptography & Quantum-Resistant Technologies (QRTs): Possible Solutions

No single technology eliminates quantum risk. Instead, enterprises must combine post-quantum cryptography including, Quantum-Resistant Algorithms (QRAs), Quantum Key Distribution (QKD), Quantum Crypto Agility (QCA), and data-centric protections like Shrink, Shread, Send, & Recombine (3SR) into a coherent strategy.

4.1 Quantum-Resistant Algorithms (QRAs) - post-quantum cryptography (PQC) refers to cryptographic algorithms designed to be secure against both classical and quantum adversaries but implemented on conventional computers. NIST's standardization process has identified leading candidates across several mathematical families.[27]

Key algorithm classes , include Lattice-based, Hash-based, Code-based, and multivariate schemes used as alternates where different assumptions are desired.[28] A pragmatic

adoption pattern is crypto agility, designing systems that can support multiple algorithm suites and rotate them without redesigning the entire protocol or application.[29, 30]

4.2 Quantum Key Distribution (QKD)

Quantum key distribution (QKD) uses quantum states (usually photons) to establish symmetric keys between two parties, with the guarantee that any eavesdropping introduces detectable disturbance.[31]

Pros:

- Offers information-theoretic security when combined with a one-time pad, independent of computational assumptions.[32]
- Provides natural eavesdropping detection through quantum measurement principles.[33]

Limitations and challenges:

- Distance and rate constraints: practical QKD systems currently operate over tens to low hundreds of kilometers in fiber or free space, with key generation rates much lower than classical optical links.[34, 35]
- Infrastructure requirements: need for specialized hardware and, often, trusted nodes or satellite links.[36]

PRO TIP

Pilot Hybrid PQC:

Start with hybrid key exchange and hybrid certificates in a contained environment such as internal APIs or B2B partner links. Measure: latency and bandwidth impact, library and HSM compatibility, and operational complexity of key and certificate management. Use these pilots to harden your crypto-agility patterns before extending PQC to customer-facing services.

PRO TIP

Pilot Hybrid QKD:

Use QKD for your most important assets "crown jewel" links, for example: data center interconnects carrying highly sensitive keys or strategic command traffic. Require that any QKD deployment: integrates with PQC-based authentication, has a clear lifecycle and maintenance plan, and demonstrably adds value beyond what PQC + robust key management already provides.

4.3 Quantum Crypto Agility (QCA)

Quantum Crypto Agility is a term used to denote a NIST PQC compliant method which leverages local quantum randomness and Federal Information Protection Standards (FIPS) approved random number generation to provide data and encryption segregation and transmission via multi-modalities of communication (via high-speed 4G/5G wireless communications, satellite communications, high-speed fiber optic cables, and/or microwave communications).

The concept behind quantum crypto agility (QCA) is that quantum resistant algorithms (QRAs) will all be eventually broken, so every organization in both the U.S. government and industry needs a back-up plan to ensure enterprise quantum security as efficient, flexible, and cost-effective as possible.

Quantum crypto agility is an architectural approach first developed and tested by Quantum Xchange in partnership with AT&T and Verizon. Evolver has partnered with Quantum Xchange to create the Evolver SHIELD solution to provide U.S. Federal government agencies with a NIST compliant PQC and FIPS approved quantum security system.

The Evolver SHIELD solution provides cost-effective enterprise quantum security at scale. It also enables agencies to focus on securing the network that data travels on to strengthen the existing infrastructure against quantum attacks, while minimizing disruption to existing communication operations. This approach to enterprise quantum security is currently being tested by the U.S. Department of Homeland Security (DHS), Customs and Border Protection (CBP) at numerous locations nationwide.

PRO TIP

"The Quantum Industry Coalition (QIC), which consists of Amazon Web Services (AWS), Google, IBM, Microsoft, Accenture, Quantum Xchange, and others believe that agencies handling sensitive government data should already be actively preparing for the transition and should begin migrating high-risk information systems to FIPS/NIST validated PQC using QCA where possible."[37]

4.4 Shrink, Shred, Send & Recombine (3SR) Data Technology

Beyond cryptographic primitives, enterprises can reduce quantum risk by changing how data itself is stored, moved, and exposed. One such pattern described as "Shrink, Shred, Send & Recombine (3SR)" aligns with principles from data minimization, data dispersal, and secret sharing.

While "3SR" is not a formal standard term, its components map to well-understood techniques such as secret sharing, erasure coding, tokenization, and multi-cloud data dispersal.[38]

1. **Shrink** – Reduce the data footprint by encrypting and tokenizing sensitive fields, applying differential privacy or redaction for analytics, and minimizing retention of raw records.
2. **Shred** – Fragment sensitive objects into multiple cryptographic or information-theoretic components, for example by using Shamir-style secret sharing schemes or erasure coding.
3. **Send** – Distribute fragments across independent channels or domains, including separate cloud providers, distinct network paths, or different administrative domains.
4. **Recombine** – Reconstruct data only within tightly controlled, PQC-protected environments, under strong identity verification and just-in-time access controls.

From a quantum-security perspective, 3SR helps because an adversary must acquire multiple fragments from independent domains and possess the cryptographic capability to break any underlying encryption.[39] HNDL operations become more complex because capturing one channel or storage domain is insufficient. If combined with PQC and strong symmetric ciphers, the overall system becomes significantly more resilient even under future quantum capabilities. 3SR does not replace PQC; it complements it by reshaping the attack surface so that a single cryptographic failure does not automatically expose full, coherent datasets.

PRO TIP

Build a Quantum-Safe Reference Implementation:

Stand up a small, end-to-end "quantum-safe enclave" that includes: PQC-enabled ingress (TLS/VPN), PQC-aware identity and PKI, A 3SR-protected data store, and operational observability around performance and failure modes. This enclave becomes your living blueprint for scaling PQC, QKD, and 3SR patterns across the wider enterprise.

5. Summary & Conclusion: The Need for Enterprise Quantum Security

The rise of quantum computing is a bifurcating force: on one path, organizations harness quantum capabilities for discovery, optimization, and competitive advantage; on the other, adversaries weaponize CRQCs to break legacy public-key cryptography, decrypt historical data, and undermine digital trust.[40, 41] Because the data we encrypt today may still matter years from now, enterprises cannot wait for the on-set of Q-Day to act. NIST's standardization of PQC algorithms and the NSA's CNSA 2.0 roadmap provide a clear signal: start migrating now, with quantum crypto-agile architectures capable of evolving as standards and implementations mature.

A practical enterprise quantum security program should:

1. Establish governance and risk appetite for quantum threats at the C-Suite level.
2. Inventory cryptography across the entire enterprise including software applications, protocols, and vendor supply chains, focusing on long-lived, high-value data.[42]
3. Segment data and apply practical principles to minimize and fragment what an adversary can harvest and decrypt later.
4. Conduct pilot programs using the QCA approach, using the Evolver SHIELD solution
5. Evaluate PQC high-value links, with careful attention to lifecycle and authentication.
6. Deploy and maintain quantum crypto agility (QCA) architecture so that new PQC standards and implementations can be adopted without systemic rewrites.[43, 44]

We view enterprise quantum security as a vital long-term digital transformation, not a one-time upgrade. By combining post-quantum cryptography encryption management, data-centric protections, and disciplined cybersecurity zero-trust architecture and governance, organizations can position themselves to reap the benefits of quantum innovation while defending against its most dangerous consequences.

Works Cited

"Quantum Computing Will Make Cryptography Obsolete. But Computer Scientists Are Working to Make Them Unhackable." Live Science, 2025. [1, 4, 7, 10, 20, 41]

National Institute of Standards and Technology. "PQC Standardization Process." Computer Security Resource Center. [2, 27, 28]

Palo Alto Networks. "Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat." Cyberpedia, Palo Alto Networks. [3, 11]

National Institute of Standards and Technology. "What Is Post-Quantum Cryptography?" NIST Cybersecurity, 13 Aug. 2024. [5, 9, 23]

"The Quantum Apocalypse Is Coming. Be Very Afraid." Wired, 2025. [6, 8, 19, 26, 40]

DuBose, Rich, and Mohan Madhvapathy Rao. "Harvest Now, Decrypt Later: Why Today's Encrypted Data Isn't Safe Forever." HashiCorp Blog, 21 May 2025. [12]

"Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography." Computer Security Resource Center, National Institute of Standards and Technology, 13 Aug. 2024. [13]

United States, National Security Agency. The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0): Algorithms and Transition Strategy. 30 May 2025. [14, 24]

Encryption Consulting. "The Commercial National Security Algorithm Suite 2.0 and Quantum-Resistant Cryptography." Encryption Consulting Blog, 24 July 2025. [15, 44]

Cloudflare. "State of the Post-Quantum Internet in 2025." Cloudflare Blog, 28 Oct. 2025. [16, 18, 30, 38, 39, 42]

TechRadar Pro. "Cyber Resilience in the Post-Quantum Era: The Time of Crypto-Agility." TechRadar Pro, 2025. [17, 29, 43]

Mascelli, John. "'Harvest Now Decrypt Later': Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks." Finance and Economics Discussion Series, Federal Reserve Board, 2025. [21, 22, 25]

Diamanti, Eleni, et al. "Practical Challenges in Quantum Key Distribution." NPJ Quantum Information, vol. 2, 2016, article 16025. [31, 33, 34]

ID Quantique. "Quantum Key Distribution (QKD)." IDQ Quantum-Safe Security, ID Quantique. [32, 35, 36]

E. Zervigon, CEO, Quantum Xchange. Testimony to the Hosue Homeland Security Committee. December 17, 2025. [37]

About the Authors

Gregory A. Garrett is the Chief Operating Officer and Chief Innovation Officer for Evolver. He leads all of Evolver's technology thought leadership and technology business units, which provide provide advanced IT, AI, cybersecurity, electronic security, and eDiscovery services to federal agencies and Fortune 500 companies.

With over 25 years of executive experience and a background as a CIO, CTO, CISO, and COO, he has managed more than $40 billion in global tech contracts and served in key roles across both large and mid-sized firms.

A retired U.S. Air Force Colonel and accomplished author, Garrett has also contributed extensively to industry thought leadership through 24 books, more than 150 articles, expert testimony, and over 250 speaking engagements.

Dr. Brian McElyea is an accomplished cybersecurity executive recognized for leading largescale digital transformation initiatives and building high-performing Cyber Centers of Excellence that drive mission-aligned security outcomes.

With over two decades of leadership across healthcare, defense, and federal sectors, he has guided global organizations through the complexities of risk management, compliance, and modernization with measurable results.