International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V7I1P147
Eureka Vision Publication | Volume 7, Issue 1, 328-337 2026

Original Article

Security Risks for Enterprises in the Post-Quantum Computing World

Milan Gupta
Comprehensive Research Analysis, Independent Researcher, USA.

Received On: 04/02/2026 ***Revised On: 05/03/2026*** ***Accepted On: 11/03/2026*** ***Published On: 17/03/2026***

Abstract - The arrival of cryptographically relevant quantum computers (CRQCs) represents an existential threat to the public-key cryptographic infrastructure underpinning global enterprise operations. Enterprise security today relies on RSA and elliptic-curve cryptography (ECC) for TLS, VPNs, PKI, code signing, and identity systems—all of which are fundamentally broken by Shor's algorithm on a sufficiently powerful quantum computer. The defining risk is time-shifted compromise: adversaries can harvest encrypted traffic today and decrypt it once CRQCs exist, a threat already underway according to U.S. intelligence assessments. NIST finalized three post-quantum cryptographic (PQC) standards in August 2024 (FIPS 203/204/205) and mandates deprecation of quantum-vulnerable algorithms by 2035. Yet only 5% of organizations have implemented quantum-safe encryption and 95% lack formal quantum transition plans. This paper provides a comprehensive, threat-driven analysis across seven dimensions: quantum algorithm impact, harvest-now-decrypt-later (HNDL) threat models, enterprise asset risks (PKI, TLS, VPNs, code signing, cloud, IoT, identity, blockchain, supply chain), sector-specific vulnerabilities (financial services, healthcare, critical infrastructure), cryptographic primitive analysis, migration standards and roadmaps, and enterprise readiness gaps. The convergence of HNDL attacks already underway, multi-decade data sensitivity windows, and 12–15 year enterprise migration timelines means the migration deadline has, for most sectors, already passed.

Keywords - Post-Quantum Cryptography, Quantum Computing, Enterprise Security, HNDL, Shor's Algorithm, NIST PQC Standards, Crypto-Agility, Key Management, TLS, PKI, FIPS 203, FIPS 204, FIPS 205, ML-KEM, ML-DSA, SLH-DSA.

1. Introduction

Quantum computing is transitioning from theoretical curiosity to engineering reality. IBM's 1,121-qubit Condor processor, Google's Willow chip demonstrating below-threshold error correction, and Microsoft's topological qubit research all signal that cryptographically relevant quantum computers (CRQCs) may arrive within the current decade. Expert consensus places a 34% probability of CRQC emergence within 10 years and a 50% chance of breaking encryption by 2031 [4][5].

The consequences for enterprise security are profound. Every TLS handshake, VPN session, PKI certificate, and digital signature in use today relies on mathematical problems integer factorization and discrete logarithms that quantum computers can solve in polynomial time via Shor's algorithm [1]. The defining enterprise risk is not only future attack capability but time-shifted compromise: adversaries can harvest encrypted data today and decrypt it once CRQCs exist.

NIST finalized three post-quantum cryptographic standards in August 2024, removing the last technical justification for inaction. Yet survey data reveals a dramatic readiness gap: only 5% of organizations have implemented quantum-safe encryption, 44% have never heard of NIST's PQC standards, and 95% lack formal quantum transition plans [46][48].

This paper provides a comprehensive, threat-driven analysis organized into seven thematic areas: quantum algorithm impact on enterprise cryptography; HNDL attack models and temporal risk frameworks; asset-specific threat analysis across PKI, TLS, VPNs, code signing, cloud, IoT, identity, blockchain, and supply chain; sector-specific risk profiles for financial services, healthcare, and critical infrastructure; a primitive-level vulnerability analysis; PQC standards and migration challenges; and an assessment of organizational readiness and global regulatory pressure. Mitigation frameworks covering cryptographic inventory, hybrid deployment, crypto-agility, zero-trust integration, and migration governance conclude the paper.

2. Quantum Computing Threat Landscape

2.1. Shor's Algorithm and the Collapse of Public-Key Cryptography

Peter Shor's 1994 algorithm solves both the integer factorization problem (IFP) and the discrete logarithm problem (DLP) in polynomial time on a quantum computer, rendering RSA, Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC) fundamentally insecure [1]. RSA-2048, which classical computers would require thousands of years to factor, could be broken by a sufficiently powerful quantum computer in hours or days. For ECC, the algorithm requires approximately $9n + 2\lceil \log_2(n) \rceil + 10$ qubits for an n-bit prime field, meaning P-256 curves need ~2,330 qubits [2]. ECC's shorter key lengths relative to RSA at equivalent

classical security levels make it paradoxically more vulnerable in the quantum era.

In enterprise systems, Shor's algorithm threatens the foundational primitives of TLS handshakes, VPN key exchange, certificate signatures, and authentication systems. All standard key exchange mechanisms in TLS 1.2 (RSA) and TLS 1.3 (ECDHE) are compromised, as are digital signature schemes (ECDSA, RSA-PSS) used for authentication, non-repudiation, and code signing. The mathematical certainty of these attacks contingent only on hardware scale distinguishes the quantum threat from probabilistic classical vulnerabilities [1].

2.2. Grover's Algorithm and Symmetric Encryption Impact

Grover's 1996 algorithm provides a quadratic speedup for unstructured search, effectively halving the bit-security of symmetric ciphers and hash functions [8]. AES-128 drops to ~64-bit security (considered vulnerable), while AES-256 retains ~128-bit security (still secure post-quantum) [3]. SHA-256 preimage resistance reduces from 256 bits to ~128 bits. NIST defines its PQC security levels based on equivalence to breaking AES at these thresholds: Level 1 (AES-128), Level 3 (AES-192), Level 5 (AES-256).

The practical feasibility of Grover's attack is contested. Implementing Grover's as a quantum circuit requires billions of physical qubits, and NIST researchers characterize the attack as largely theoretical at currently envisioned scales, though the agency recommends doubling symmetric key lengths as a precautionary measure [3]. Operationally, this pushes conservative enterprises toward AES-256 and sometimes stronger hash selections depending on confidentiality horizons [8].

2.3. CRQC Timeline Estimates and Expert Consensus

The Global Risk Institute's 2024 Quantum Threat Timeline Report surveyed 32 global experts and found a ~34% estimated probability of a CRQC within 10 years (up from 31% in 2023) and ~14% within 5 years [4]. BCG estimates a 50:50 chance of quantum computers breaking encryption by 2031 [5]. Gartner predicts conventional asymmetric cryptography will be unsafe by 2029 and fully breakable by 2034 [6].

Government timelines reflect these estimates. NSM-10 (May 2022) sets 2035 as the federal PQC migration deadline. NSA's CNSA 2.0 mandates exclusive PQC use for software/firmware signing by 2030 and web/cloud systems by 2033 [7]. NIST IR 8547 targets deprecation of 112-bit quantum-vulnerable algorithms after 2030 and full disallowance after 2035 [8]. The UK's NCSC proposes milestones of 2028 (discovery), 2031 (highest-priority migrations), and 2035 (complete migration) [9].

2.4. Current Quantum Hardware Milestones

IBM's 1,121-qubit Condor processor (December 2023) surpassed 1,000 superconducting qubits, while its 156-qubit Heron chip (2024) achieved 3–5× performance improvement. IBM targets ~200 logical qubits by 2029–2030 and fault tolerance by decade's end [9]. Google's 105-qubit Willow chip (December 2024) achieved the first demonstration of below-threshold quantum error correction, where error rates decreased exponentially as logical qubit grids scaled from 3×3 to 7×7 [10]. Microsoft's Majorana 1 (February 2025) introduced 8 topological qubits, claiming a path to 1 million qubits on a single chip, though significant scientific skepticism remains [11]. IonQ projects ~20,000 physical qubits by 2028.

Gidney and Ekerå (2021) estimated RSA-2048 factoring would require ~20 million noisy physical qubits operating for 8 hours [12]. A May 2025 preprint by Gidney dramatically reduced this to <1 million noisy physical qubits in <1 week—a 20× reduction through algorithmic advances including magic state cultivation and yoked surface codes [13]. If validated, this brings qubit requirements within reach of late-2020s hardware roadmaps.

3. Harvest-Now, Decrypt-Later Attacks

3.1. Formal Threat Models and Temporal Risk Frameworks

HNDL attacks represent the most immediate quantum-era threat: adversaries intercept and store encrypted data today, awaiting quantum decryption capability. A landmark paper in MDPI Telecom formally models HNDL as a temporal cybersecurity risk, introducing the vulnerability condition $L_d > H_a$ (where L_d = data confidentiality lifetime and H_a = attacker decryption horizon). Their analysis of over 100 primary sources concludes that 98–100% of healthcare records and 95–100% of government-classified data encrypted today are likely to face retroactive decryption under the HNDL model [14].

Data confidentiality horizons frequently exceed migration windows, enabling harvest-now exploitation. This shifts post-quantum risk from a future problem to a present data-protection problem—especially for long-retention backups, archives, regulated records, intellectual property, and sensitive communications [10]. The Federal Reserve's 2025 working paper established that the HNDL threat began at the inception of Shor's algorithm in 1994 and remains ongoing, and that blockchain data from 2009 onward is subject to this threat [15]. A separate paper proposes the Quantum-Adjusted Risk Score (QARS) model, extending Mosca's inequality into a multi-factor formula incorporating timeline, sensitivity, and exposure dimensions [16].

3.2. Mosca's Theorem and Migration Urgency

Michele Mosca's theorem provides the canonical framework for quantifying migration urgency: if $x + y > z$, then worry—where x = years data must remain secure, y = years to complete migration, and z = years until CRQC arrival [17]. Applied to enterprise sectors using conservative estimates (z = 10 years), the analysis reveals that healthcare and critical infrastructure sectors are already in critical status:

Table 1. Mosca's Inequality Applied to Enterprise Sectors (z = 10 years assumed)

Sector	x (Data Shelf Life)	y (Migration Time)	x + y	Status
Healthcare	60–80 years	5–10 years	65–90	CRITICAL
Critical Infrastructure	20–50 years	5–15 years	25–65	CRITICAL
Financial Services	7–30 years	3–5 years	10–35	HIGH
Government/Defense	25–75 years	5–15 years	30–90	CRITICAL
Technology Sector	5–15 years	3–7 years	8–22	HIGH

3.3. Evidence of State-Actor HNDL Campaigns

The U.S. government has acknowledged HNDL as an active threat. NSM-10 explicitly references 'record-now-decrypt-later type attack' and states that 'diligent preparation and migration to PQC is the best long-term solution' [18]. A joint NSA/CISA/NIST advisory (August 2023) warned that 'Cyber actors could target our nation's most sensitive information now and leverage future quantum computing technology to break traditional non-quantum-resistant cryptographic algorithms' [19]. The Congressional Research Service documented nation-state actors downloading encrypted data from U.S. government and critical infrastructure operators 'today with the hopes of using quantum computers to decrypt that data at some point in the future' [20].

Documented infrastructure for data harvesting exists. Demchak and Shavitt (2018) demonstrated that China Telecom used BGP hijacking to misdirect 15% of global internet traffic, with subsequent targeted hijacking of traffic to financial institutions, government sites, and media organizations [21]. Mastercard's 2025 R&D white paper characterizes HNDL as primarily a state-actor threat: 'The immense resources required to indiscriminately store and curate petabytes of encrypted traffic... would be beyond a criminal enterprise' [22].

4. Enterprise Threat Models and Asset Risks

This section enumerates core enterprise assets and frames quantum risk as both confidentiality compromise (future decryption of captured traffic) and integrity/authentication collapse (forging of signatures and certificates).

4.1. PKI and Certificate Ecosystems

Enterprise PKI depends on signature schemes (RSA/ECDSA/EdDSA) and certificate validation rules (X.509). The primary quantum risk is signature forgery: if an attacker can forge a CA or intermediate signature, they can mint seemingly valid certificates, enabling pervasive impersonation and man-in-the-middle attacks. NIST explicitly notes ECDSA/RSA vulnerability to Shor's algorithm in transition guidance [15]. Migration complications arise because certificate ecosystems are interdependent and slow to change the WebPKI ecosystem (roots, CAs, CT logs, revocation) is particularly challenging to adapt quickly to PQ signatures [16].

4.2. TLS, Service Mesh mTLS, and Internet-Facing Channels

TLS 1.3 underpins most enterprise transport security. Under Shor's algorithm, both authentication (certificate signatures) and key exchange (ECDHE) are threatened: recorded TLS sessions may become decryptable, and future active interception becomes plausible if authentication chains can be forged [17]. Hybrid TLS design at the IETF explicitly targets a transition period where multiple key exchanges are combined to maintain security if at least one component remains secure [18]. As of 2025, over 60% of human-generated TLS traffic to Cloudflare uses hybrid ML-KEM key exchange [42].

4.3. VPNs, Remote Access, and Site-to-Site IPsec

IKEv2 governs key establishment for most IPsec VPN deployments. Quantum risk mirrors TLS: recorded VPN traffic may become decryptable later; authentication may become forgeable. The IETF is actively standardizing post-quantum and hybrid approaches for IKEv2, including an ML-KEM-based hybrid key exchange draft that cites practical concerns like packet fragmentation due to large post-quantum key exchange payloads [22]. A practical interim mitigation for long-lived VPN confidentiality is to mix pre-shared key material into IKEv2 key derivation (RFC 8784) [24].

4.4. Code Signing, Software Supply Chain, and Firmware Integrity

If signature schemes are broken, attackers can produce malicious updates that appear legitimate, enabling persistent compromise at scale. NSA's CNSA 2.0 transition guidance includes explicit timelines for software/firmware signing: transition to PQC by 2030 [26]. The Software Development Lifecycle (NIST SP 800-218/SSDF) provides a governance anchor for why enterprises should treat code signing migration and verification pipelines as critical security infrastructure [25].

4.5. Cloud Data at Rest, In Transit, and Backups/Archives

Post-quantum risk is often dominated by retention: backups and archives with long confidentiality horizons are prime harvest-now targets because encrypted objects can be stolen once and decrypted decades later when CRQC capability exists [27]. Even if at-rest encryption remains symmetric (e.g., AES), public-key cryptography is used for key exchange, key wrapping, and identities, and those layers become weak. Disciplined key management—cryptoperiods, rotation, and destruction per NIST SP 800-57 becomes

amplified in importance during migration, particularly for re-encrypting archives and rotating wrapping keys [29].

4.6. Identity Systems and Authentication Fabrics

SSO stacks (OIDC/OAuth, SAML, Kerberos-adjacent systems) rely on TLS for channel security and often signatures for tokens and assertions. A quantum break threatens token and assertion integrity (forgery), certificate-based mutual authentication inside service meshes, and long-lived MFA device certificate ecosystems. NIST transition guidance explicitly frames digital signature algorithms and ECC/RSA as quantum-vulnerable under Shor's algorithm [28].

4.7. IoT, OT, Embedded, and Long-Lived Infrastructure

IoT and embedded systems present unique challenges: long service lives (10–30+ years), constrained CPU/memory budgets, infrequent patching, and hard-coded crypto or certificate pinning. The size and performance characteristics of PQC (larger keys/signatures) often cause significant redesign pressure. UK guidance explicitly identifies long-lived hardware roots of trust as a migration planning item requiring identification by 2028 [30].

4.8. Blockchain and Digital Asset Systems

Many blockchain systems rely on ECDSA/EdDSA-style signatures for ownership and transaction authorization. A quantum attacker able to perform Shor-style attacks against ECC could forge signatures and steal assets from exposed keys, creating systemic trust failures. Approximately 74 of the top 100 cryptocurrencies use ECDSA with secp256k1, directly vulnerable to Shor's algorithm. Approximately 25% of Bitcoin's value (~1.72 million BTC in P2PK addresses) has publicly exposed keys and would be immediately vulnerable [26][31].

5. Sector-Specific Risk Analysis

5.1. Financial Services and Banking

The financial sector's cryptographic dependencies are pervasive. A single cross-border payment 'can touch dozens of distinct quantum-vulnerable cryptographic operations, each managed by a different entity with its own upgrade cycle' [23]. TARGET2, the Eurosystem's real-time gross settlement system, moves over €2 trillion daily. SWIFT's interbank messaging uses multi-layered PKI for authentication across 11,000+ member banks, with SwiftNet 8.0 targeting PQC enablement by 2027 [23].

BIS Project Leap Phase 2 (December 2025) tested PQC in TARGET2 and found PQC signature verification averaged 209.9ms versus 28.1ms for RSA a 7.5× slowdown with PQC signatures nearly 10× larger than predecessors [24]. The Hudson Institute estimates the cost of a single quantum attack on the Fedwire Funds Service at $730 billion to $1.95 trillion, with cascading GDP effects of 10–17% annual decline [25]. Approximately 25% of Bitcoin's value has publicly exposed keys that would be immediately vulnerable to quantum attack [26].

No explicit PQC mandate exists for banking, but the OCC (December 2022) issued the first federal banking guidance. MAS Singapore issued Circular MAS/TCRS/2024/01 (February 2024) directing all financial institution CEOs to maintain cryptographic asset inventories [29]. The Bank of Israel (January 2025) mandated banking corporations to assess quantum risks within one year, and EU member states jointly recommended PKI migration by end of 2030.

5.2. Healthcare and Life Sciences

The U.S. has 96% hospital EHR adoption. EHR systems employ AES-256 for data at rest and TLS for transit, but asymmetric key exchange components within TLS remain quantum-vulnerable. In 2024, 276 million patient records were compromised (64% increase from 2023), with healthcare breach costs averaging $9.77 million—the highest of any sector for 14 consecutive years [30]. Health records trade at up to $250 per record on the black market compared to $5.40 for payment cards, because medical identity theft never expires.

HIPAA's retention mandates 6 years minimum, with OSHA requiring 30-year retention for certain records create extended HNDL vulnerability windows. Legal analysis by IAPP scholars suggests 'there is a plausible argument to show that quantum-safe encryption practices are now relevant given the present threat of post-hoc decryption attacks' [31]. HIPAA does not currently explicitly address quantum threats, though proposed updates include quantum computing considerations.

Connected medical devices with 10–15+ year field lifespans rely on embedded cryptography that cannot be easily upgraded. FDA's 2023 Premarket Cybersecurity Guidance gives FDA legal authority to refuse device submissions lacking cybersecurity protections [32]. CISA's October 2024 guidance identifies OT medical systems as likely 'the last remaining platforms to achieve post-quantum cryptographic standards' due to strict change procedures and verification requirements [33]. Device replacement costs may reach $2 million per device for FDA-approved equipment.

5.3. Critical Infrastructure: Energy and Telecom

Many SCADA protocols (DNP3, Modbus, EtherCAT) were designed without integrated authentication or encryption, often operating in cleartext. Equipment operates for 20–30+ years, and CISA warns that APT actors are 'already harvesting encrypted OT traffic' for future quantum exploitation [33]. RAND Corporation assessed all 55 national critical functions for quantum vulnerability, identifying certificate signing, roots of trust, and privileged user authentication as highest-risk elements [34].

BGP relies on RPKI using RSA signatures for Route Origin Validation. Research warns that using ROV with quantum-vulnerable cryptography can make BGP less secure than not using ROV at all, potentially forcing operators to disable ROV entirely [35]. The 5G-AKA authentication

protocol uses symmetric shared secrets for its core, but the broader 5G infrastructure contains extensive quantum-vulnerable asymmetric operations including eSIM bootstrap, TLS-based Service-Based Architecture interfaces, and N32 SEPP-to-SEPP connections [36]. Thales demonstrated (March 2026) the world's first remote deployment of PQC on SIM/eSIM cards in a live 5G network without device replacement [37].

6. Quantum Vulnerability Analysis of Cryptographic Primitives

NIST's transition documentation identifies discrete-log and factoring-based schemes (RSA, ECDSA, EdDSA, etc.) as quantum-vulnerable, while standardized PQC schemes (ML-KEM, ML-DSA, SLH-DSA) are intended to be resistant to quantum attacks under current knowledge [32]. The following table summarizes enterprise-relevant primitives and recommended migration directions:

Table 2. Enterprise Cryptographic Primitive Quantum Vulnerability Mapping

Primitive	Enterprise Use	Quantum Impact	Enterprise Consequence	Migration Direction
RSA (enc/sig)	TLS certs, code signing, VPN auth	Broken by Shor	Future decryption; forged signatures	Replace with ML-DSA or SLH-DSA
ECDH/ECDHE (X25519)	TLS 1.3 key establishment, mTLS	Broken by Shor	Recorded sessions decryptable later	Hybrid KEX then PQ KEX (ML-KEM)
ECDSA / EdDSA	PKI chains, tokens, code signing	Broken by Shor	Authentication & integrity collapse	PQ signatures (ML-DSA); SLH-DSA backup
AES-128	Bulk encryption	Grover reduces margin	Long-horizon confidentiality risk	Prefer AES-256 for multi-decade needs
SHA-256 / SHA-3	Signatures, integrity, KDF	Grover affects preimage	Some security-margin reduction	Follow NIST guidance on sizes
Diffie-Hellman	Legacy VPN, key exchange	Broken by Shor	Session decryption risk	Replace with ML-KEM based KEX

6.1. PQC Parameter Sizes: Enterprise Engineering Impact

PQC changes payload sizes and computational profiles, affecting MTU constraints, handshake latency, certificate chains, and storage. From FIPS 203, ML-KEM key and ciphertext sizes include: ML-KEM-512 (800/768 bytes), ML-KEM-768 (1184/1088 bytes), ML-KEM-1024 (1568/1568 bytes) [4]. From FIPS 204, ML-DSA key and signature sizes include: ML-DSA-44 (public key 1312, signature 2420 bytes), ML-DSA-65 (1952/3309 bytes), ML-DSA-87 (2592/4627 bytes) [37]. SLH-DSA public keys are small (32–64 bytes) but signatures are large (7,856 to 49,856 bytes) [38].

These sizes explain why enterprises tend to adopt lattice-based PQ signatures first (moderate signature sizes), keep hash-based signatures as a diversity backup rather than the default, and use hybrid handshakes to manage transition risk while engineering ecosystem compatibility [39].

7. PQC Standards and Migration Frameworks

7.1. NIST PQC Standards: Finalized August 2024

NIST published three post-quantum cryptographic standards on August 13, 2024 the culmination of an eight-year standardization process making near-term enterprise migration feasible in controlled stages [3][80]:

- FIPS 203 (ML-KEM): Module-Lattice-Based Key-Encapsulation Mechanism derived from CRYSTALS-Kyber. Offers parameter sets at security Levels 1/3/5 with ~1.5 KB keys and ciphertexts for ML-KEM-768. Security based on the Module Learning With Errors (MLWE) problem [39].
- FIPS 204 (ML-DSA): Module-Lattice-Based Digital Signature Algorithm derived from CRYSTALS-Dilithium. Parameter sets ML-DSA-44/65/87 for authentication, integrity, and non-repudiation [40].
- FIPS 205 (SLH-DSA): Stateless Hash-Based Digital Signature Algorithm derived from SPHINCS+. Conservative hash-based security assumptions but larger signatures (up to ~40 KB) [41].

Additional standards in progress include FIPS 206 (FN-DSA/FALCON) for NTRU lattice signatures and HQC, selected March 2025 as a code-based backup KEM to diversify mathematical assumptions beyond module-lattice designs [12][60].

7.2. NIST IR 8547 Deprecation Timeline

NIST IR 8547 (Initial Public Draft, November 2024) establishes the transition framework: 112-bit security algorithms (RSA-2048, ECC-256) deprecated after 2030 and disallowed after 2035 [8]. For key establishment, application-specific guidance may require earlier migration to mitigate HNDL risks. NSA's CNSA 2.0 sets more aggressive deadlines: software/firmware signing with PQC by 2030, web/cloud exclusive PQC use by 2033, complete NSS transition by 2035 [7].

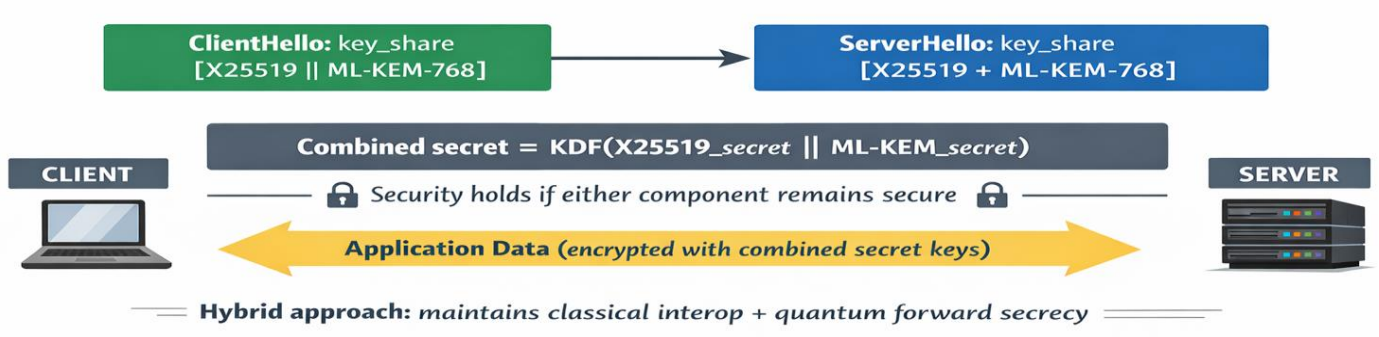

Figure 1. Conceptual Hybrid TLS 1.3 Handshake Combining X25519 (Classical) and ML-KEM-768 (PQC). Security Holds if Either Component Remains Unbroken

7.3. Hybrid Cryptography and Crypto-Agility

Hybrid approaches combine classical algorithms (X25519/ECDH) with PQC (ML-KEM) so an attacker must break both to compromise a connection. Hybrid cryptography reduces the risk of betting early on a single new primitive, supports interoperability while standards and codepoints stabilize, and preserves confidentiality against harvest-now attacks even before certificate ecosystems fully migrate [18]. The IETF hybrid TLS design draft defines hybrid key exchange in TLS 1.3 as using multiple key exchange algorithms and combining results so security holds if at least one component remains secure [13].

NIST published CSWP 39 (December 2025) on crypto-agility, defined as 'the ability to replace cryptographic algorithms in protocols, applications, and infrastructure without disrupting system operations.' The document introduces a crypto-agility maturity model and emphasizes modular system design, algorithm negotiation, and automated cryptographic discovery [43]. Cloudflare has already deployed PQ-protected Zero Trust products providing end-to-end quantum safety for HTTPS corporate applications.

7.4. Enterprise Migration Challenges

PQC migration represents what NIST characterizes as 'the most significant cryptographic upgrade in digital security history.' Key challenges include:

- Performance overhead: SLH-DSA signatures reach ~40 KB; Classic McEliece public keys are ~268 KB. BIS Project Leap measured 7.5× signature verification slowdown in payment systems [24].
- Legacy system compatibility: IoT devices on 8/32-bit microcontrollers may not support PQC. Chrome rolled back hybrid PQC due to widespread enterprise TLS handshake failures from middlebox incompatibility.
- Talent shortage: The Entrust/Ponemon 2024 study found 43% of organizations cite insufficient skills as a barrier and 51% reported lack of clear ownership [44]. McKinsey reports only one qualified quantum candidate for every three quantum jobs globally.
- Migration timelines: Estimates range from 5–7 years for small enterprises, 8–12 for medium, and 12–15+ years for large enterprises to complete PQC migration [45].

8. Enterprise Readiness Gap

8.1. Survey Data: Dramatic Awareness-Action Deficit

The ISACA 2025 Quantum Computing Pulse Poll (2,685 respondents) found 62% of technology professionals worried that quantum computing will break encryption before PQC deployment, yet only 5% of organizations have a defined quantum computing strategy meaning 95% lack formal quantum transition plans. Additionally, 55% have taken no preparatory steps, 44% have never heard of NIST's PQC standards, and 56% cite HNDL as a concern [46].

KPMG's 2024 survey of 250 large US and Canadian corporations found 73% of US respondents believe 'it's only a matter of time' before quantum-enabled cybercriminals breach current protocols, while 81% admit they need to better evaluate their current cryptographic capabilities [47]. DigiCert's May 2025 study confirmed that only 5% of organizations have implemented quantum-safe encryption despite 69% recognizing the risk [48]. The Entrust/Ponemon 2024 study found only 41% are actively preparing, with the US showing the highest preparedness at 48% [44].

8.2. Cost Estimates and Economic Projections

The White House OMB estimates the total cost for migrating prioritized federal information systems to PQC at approximately $7.1 billion between 2025 and 2035 (excluding national security systems) [49]. McKinsey projects the quantum communication market will grow to $10.5–$14.9 billion by 2035, with PQC holding the largest share at $2.4–$3.4 billion [50]. BCG forecasts quantum computing will create $450–$850 billion in economic value globally by 2040 [5].

8.3. Global Regulatory Landscape

A coordinated global regulatory framework is emerging across five major jurisdictions: the United States (NSM-10, CNSA 2.0, OMB M-23-02, CISA EO 14306), the European Union (Commission Recommendation 2024/1101, Coordinated Implementation Roadmap June 2025 with milestones of 2026/2030/2035) [51], the United Kingdom (NCSC three-phase timeline: discovery by 2028, high-priority upgrades by 2031, complete migration by 2035) [52], Singapore (MAS Circular MAS/TCRS/2024/01

directing financial institution CEOs to inventory cryptographic assets) [29], and ENISA (Updated Agreed Cryptographic Mechanisms to include ML-KEM, ML-DSA, SLH-DSA for the first time in May 2025) [53].

Table 3. Key Quantitative Findings

Metric	Value	Source
CRQC probability within 10 years	~34%	Global Risk Institute, 2024 [4]
Organizations with quantum strategy	Only 5%	ISACA, 2025 [46]
Organizations implementing quantum-safe encryption	Only 5%	DigiCert, 2025 [48]
US enterprises believing quantum breach inevitable	73%	KPMG, 2024 [47]
Healthcare records at HNDL risk	98–100%	MDPI Telecom, 2025 [14]
Federal PQC migration cost (2025–2035)	~$7.1 billion	OMB Report, 2024 [49]
Cost of single Fedwire quantum attack	$730B–$1.95T	Hudson Institute, 2023 [25]
Bitcoin value with exposed public keys	~25% (~1.72M BTC)	Ledger Donjon [26]
Physical qubits for RSA-2048 (2025 est.)	<1 million	Gidney, 2025 [13]
PQC signature verification slowdown	7.5×	BIS Project Leap, 2025 [24]

9. Mitigation Frameworks and Best Practices

9.1. Quantum Risk Assessment and Cryptographic Inventory

Cryptographic inventory discovery is the essential first step in PQC migration. NIST SP 1800-38B demonstrates automated discovery methodologies [54], while OMB Memo M-23-02 requires federal agencies to submit prioritized inventories. CISA's September 2024 strategy supports Automated Cryptography Discovery and Inventory (ACDI) tools for federal civilian agencies [55]. Tools like IBM Quantum Safe Explorer, CipherInsights (recognized by NIST NCCoE), and InfoSec Global's AgileSec Analytics enable passive network monitoring, SBOM analysis, and agent-based scanning to catalog quantum-vulnerable algorithms.

The Cryptographic Bill of Materials (CBOM), developed by IBM Research and standardized through OWASP CycloneDX, extends the SBOM concept to cryptographic assets—cataloging algorithms, certificates, keys, protocols, and their dependencies in a machine-readable format enabling automated compliance checking [56]. This enables organizations to scope PQC pilots, track rollout progress, and conduct supply chain cryptographic audits.

9.2. Migration Roadmap with Prioritization Logic

A practical enterprise roadmap can be structured into four stages:

- Discovery and classification (now–2028): Inventory cryptographic use across endpoints, applications, CI/CD, cloud services, and third-party products; classify by confidentiality horizon, integrity criticality, and blast radius. Communicate needs to suppliers [30].
- Priority controls (2026–2031): Focus on hybrid TLS for internet-facing traffic and internal mTLS, VPN protections for high-value links, and code signing root modernization. Enable best-practice PFS everywhere; identify long-retention archives [47].
- Scale migration (2029–2033): Expand PQC/hybrid across service mesh, API gateways, and managed endpoints; rotate long-lived keys and re-encrypt archives; track vendor roadmaps and protocol standards convergence [48].
- Completion and deprecation (2033–2035): Move from hybrid to PQ-only where the ecosystem permits; retire quantum-vulnerable algorithms per regulatory/partner expectations.

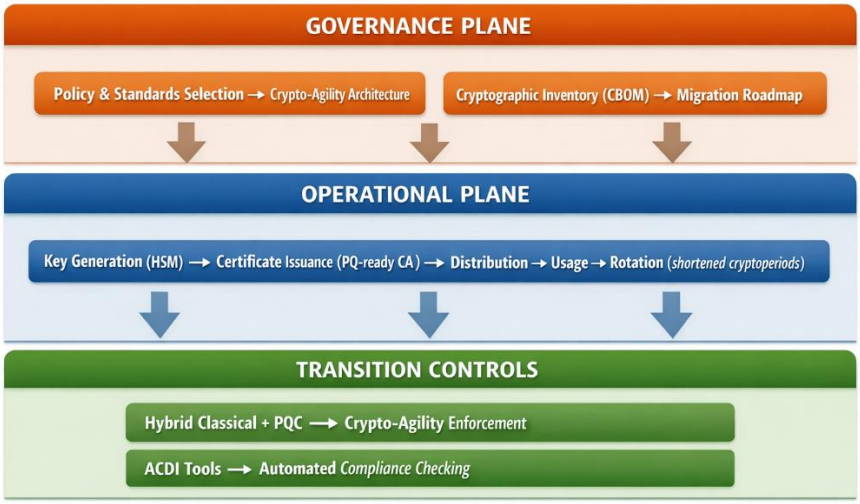

Figure 2. Enterprise Cryptographic Key Lifecycle with Crypto-Agility Control Plane. Governance Feeds Operational Steps across the Full Key Lifecycle

9.3. Prioritized Action Checklist by Asset Criticality

Table 4. Prioritized Action Checklist by Asset Criticality and Budget

Asset	Low Budget (Do No Harm)	Medium Budget (Broad Readiness)	High Budget (Accelerate)
Critical Trust Anchors (PKI, SSO)	Document RSA/ECC usage; shorten cryptoperiods [49]	Pilot PQ signatures for internal PKI; dual/hybrid verification [50]	Build PQ-capable CA infrastructure; require vendor PQ roadmaps contractually [51]
High-Value Data Flows (TLS/VPN)	Enable PFS everywhere; identify long-retention traffic [52]	Deploy hybrid TLS in gateways; implement PQ-aware IKEv2 plans [53]	End-to-end hybrid coverage; optimize MTU controls; safe rollback [54]
Backups and Archives	Tag datasets by confidentiality horizon; adopt AES-256 for long-term [55]	Re-encrypt top-tier archives; rotate wrapping keys; harden KMS/HSM [49]	Continuous re-encryption pipelines; PQ-secure key establishment [56]
Supply Chain and Firmware	Tighten signing controls; enforce verification gates [57]	Introduce PQ signing for high-risk artifacts and firmware [58]	Full PQ-capable signing infrastructure; enforce supplier PQ compliance [59]

9.4. Zero Trust Architecture as Quantum-Resilient Foundation

Zero Trust Architecture (NIST SP 800-207) and PQC are synergistic. Microsegmentation reduces the quantum attack surface by limiting blast radius, while PQC-secured authentication prevents quantum-enabled impersonation. The GSA published a ZTA PQC Buyer's Guide (June 2025) for federal agencies with use cases including Quantum Security-as-a-Service.

9.5. Quantum Key Distribution as Complementary Defense

QKD provides information-theoretic security based on quantum mechanical principles (BB84 protocol), fundamentally different from PQC's computational hardness assumptions. Major networks include China's 2,000+ km Beijing-Shanghai backbone, Europe's EuroQCI initiative, and South Korea's 800 km network connecting 48 government agencies. However, NSA explicitly does not recommend QKD for National Security Systems, citing limitations including partial solution scope, special-purpose equipment requirements, increased infrastructure costs, and denial-of-service risk [57]. The consensus treats QKD as complementary to, not a replacement for, PQC.

9.6. NIST CSF 2.0 Integration with PQC Migration

NIST CSWP 48 (September 2025) systematically maps PQC migration capabilities to CSF 2.0's six functions: Govern (updating governance policies, establishing PQC migration leads), Identify (cryptographic discovery, vulnerability identification), Protect (implementing PQC algorithms, deploying quantum-ready HSMs), Detect (monitoring for deprecated algorithms), Respond (incident response for cryptographic vulnerabilities), and Recover (business continuity with quantum-safe backup encryption) [58].

9.7. Vendor and Supply-Chain Quantum Risk

The PQC transition extends beyond internal systems to the entire software supply chain. OMB M-23-02 requires agencies to assess cryptographic methods in vendor-supplied systems. Organizations should require PQC implementation timelines from suppliers, include quantum readiness requirements in procurement contracts, and evaluate vendor crypto-agility capabilities. CISA maintains and updates lists of PQC-enabled products with version numbers to support procurement decisions.

10. Conclusion

The research synthesized here reveals a threat that is mathematically certain (Shor's algorithm), temporally urgent (Mosca's inequality), and systematically underaddressed (5% organizational readiness). The convergence of three factors HNDL attacks already underway, multi-decade data sensitivity windows in healthcare and critical infrastructure, and 12–15 year enterprise migration timelines means that for most sectors, the migration deadline has already passed.

The finalization of NIST FIPS 203/204/205 in August 2024 removed the last justification for inaction: approved standards now exist, deprecation timelines are codified, and the regulatory apparatus from NSM-10 to the EU Coordinated Roadmap is tightening. What remains is execution at scale a challenge that demands cryptographic inventory as prerequisite, hybrid deployment as bridge, crypto-agility as architecture, and workforce development as enabler.

The $7.1 billion federal estimate represents merely the public-sector floor of what will be the most consequential cryptographic transition in digital history. Enterprises that frame this as a routine security upgrade misunderstand the scope: this is a structural transformation of the cryptographic infrastructure underpinning every aspect of digital commerce, communications, and governance. The organizations that begin systematic discovery and hybrid deployment today will be positioned to meet regulatory deadlines; those that wait will face emergency transitions at vastly greater cost and risk.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Review, vol. 41, no. 2, pp. 303–332, 1999.

[2] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic

curve discrete logarithms," IACR ePrint Archive, Report 2017/598, 2017. Available: https://eprint.iacr.org/2017/598.pdf
[3] NIST, "On the practical cost of Grover for AES key recovery," presented at Fifth PQC Standardization Conf., 2024.
[4] M. Mosca and M. Piani, "Quantum Threat Timeline Report 2024," Global Risk Institute, Toronto, Dec. 2024. Available: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
[5] Boston Consulting Group, "The long-term forecast for quantum computing still looks bright," BCG, Boston, Jul. 2024. Available: https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright
[6] Gartner, "Top strategic technology trends for 2025: Postquantum cryptography," Gartner, Inc., Stamford, CT, Oct. 2024. Available: https://www.gartner.com/en/documents/5850047
[7] NSA, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Algorithms," Cybersecurity Advisory, ver. 2.1, ay 2025. Available: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
[8] NIST, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547 (Initial Public Draft), Nov. 2024. DOI: https://doi.org/10.6028/NIST.IR.8547.ipd
[9] UK NCSC, "Timelines for migration to post-quantum cryptography," National Cyber Security Centre, Mar. 2025. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
[10] H. Neven, "Meet Willow, our state-of-the-art quantum chip," Google Blog, Dec. 9, 2024. Available: https://blog.google/innovation-and-ai/technology/research/google-willow-quantum-chip/
[11] Microsoft, "Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits," Azure Quantum Blog, Feb. 19, 2025.
[12] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," Quantum, vol. 5, p. 433, Apr. 2021. DOI: 10.22331/q-2021-04-15-433.
[13] C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv preprint, arXiv:2505.15917, May 2025.
[14] MDPI, "Harvest-now, decrypt-later: A temporal cybersecurity risk in the quantum transition," Telecom, vol. 6, no. 4, art. 100, 2025. Available: https://www.mdpi.com/2673-4001/6/4/100
[15] J. Mascelli and M. Rodden, "'Harvest now decrypt later': Examining post-quantum cryptography and the data privacy risks for distributed ledger networks," Finance and Economics Discussion Series 2025-093, Board of Governors of the Federal Reserve System, Washington, DC, 2025.
[16] MDPI, "Towards a unified quantum risk assessment," Electronics, vol. 14, no. 17, art. 3338, 2025.
[17] M. Mosca, "Cybersecurity in a quantum world: Will we be ready?" presented at NIST Workshop on Cybersecurity in a Post-Quantum World, Apr. 3, 2015.
[18] The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10)," May 4, 2022.
[19] NSA, CISA, and NIST, "Quantum-readiness: Migration to post-quantum cryptography," Cybersecurity Information Sheet, Aug. 21, 2023.
[20] Congressional Research Service, "Preparing secrets for a post-quantum world," CRS In Focus IN11921, 2022.
[21] C. C. Demchak and Y. Shavitt, "China's maxim—Leave no access point unexploited: The hidden story of China Telecom's BGP hijacking," Military Cyber Affairs, vol. 3, iss. 1, art. 7, 2018.
[22] Mastercard, "Migration to post-quantum cryptography," Mastercard R&D White Paper, 2025.
[23] M. Ivezic, "Payments and the race to quantum safety," PostQuantum.com, Feb. 23, 2026.
[24] BIS, "Project Leap phase 2: Quantum-proofing payment systems," BIS Innovation Hub, 2025. Available: https://www.bis.org/publ/othp107.htm
[25] A. Butler and A. Herman, "Prosperity at risk: The quantum computer threat to the US financial system," Hudson Institute, Washington, DC, Apr. 2023.
[26] Ledger Donjon, "Quantum computing's threat to blockchain," Ledger Blog, 2025. Available: https://www.ledger.com/blog-quantum-computing-threat-to-blockchain
[27] BIS, "Quantum-proofing the financial system," BIS Paper No. 67, 2022. Available: https://www.bis.org/publ/othp67.pdf
[28] NIST, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547 (IPD), Nov. 2024.
[29] MAS, "Advisory on addressing the cybersecurity risks associated with quantum," Circular No. MAS/TCRS/2024/01, Monetary Authority of Singapore, Feb. 20, 2024.
[30] UK NCSC, "Quantum-safe cryptography: Guidance," National Cyber Security Centre, 2023. Available: https://business.cch.com/CybersecurityPrivacy/ncscquantumguidance.pdf
[31] I. Scanlon and C. Zweifel-Keegan, "A quantum of context: Cybersecurity law after Q-Day," IAPP, 2025.
[32] MedCrypt, "Navigating post-quantum cryptography in medical device cybersecurity," MedCrypt Blog, 2025.
[33] CISA, "Post-quantum considerations for operational technology," DHS/CISA, Oct. 2024. Available: https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20(508).pdf
[34] M. J. D. Vermeer et al., "Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems," RAND Corporation, RR-A2427-1, 2023.
[35] APNIC, "How can RPKI be made quantum-safe?" APNIC Blog, Jul. 2025. Available: https://blog.apnic.net/2025/07/22/how-can-rpki-can-be-made-quantum-safe/

[36] P1 Security, "Post quantum cryptography for mobile networks," P1 Security Blog, 2025.
[37] Thales Group, "Thales sets world first with remote post-quantum 5G SIM upgrade," BusinessWire, Mar. 2, 2026.
[38] Ericsson, "Impact of quantum computing on 5G & 6G security," Ericsson, 2025.
[39] NIST, "Module-lattice-based key-encapsulation mechanism standard," FIPS 203, Aug. 13, 2024. DOI: https://doi.org/10.6028/NIST.FIPS.203
[40] NIST, "Module-lattice-based digital signature standard," FIPS 204, Aug. 13, 2024. DOI: https://doi.org/10.6028/NIST.FIPS.204
[41] NIST, "Stateless hash-based digital signature standard," FIPS 205, Aug. 13, 2024. DOI: https://doi.org/10.6028/NIST.FIPS.205
[42] Cloudflare, "State of the post-quantum Internet in 2025," Cloudflare Blog, 2025. Available: https://blog.cloudflare.com/pq-2025/
[43] NIST, "Considerations for achieving crypto agility: Strategies and practices," NIST CSWP 39, Dec. 2025.
[44] Entrust and Ponemon Institute, "2024 PKI and post-quantum trends study," Entrust, 2024. Available: https://www.entrust.com/resources/reports/ponemon-post-quantum-report
[45] T. D. Le, P. H. Do, et al., "Are enterprises ready for quantum-safe cybersecurity?" arXiv preprint, arXiv:2509.01731, Sep. 2025.
[46] ISACA, "Quantum Computing Pulse Poll 2025," ISACA, Schaumburg, IL, Apr. 28, 2025. Available: https://www.isaca.org/resources/quantum-pulse-poll
[47] KPMG, "Quantum is coming—and bringing new cybersecurity threats with it," KPMG Global, Mar. 2024.
[48] DigiCert, "Quantum readiness gap: A DigiCert study on quantum-safe encryption," DigiCert, May 8, 2025.
[49] Office of Management and Budget, "Report on post-quantum cryptography," The White House, Washington, DC, Jul. 2024.
[50] McKinsey & Company, "Quantum communication growth drivers: Cybersecurity and quantum computing," McKinsey Digital, 2025.
[51] European Commission, "Coordinated implementation roadmap for the transition to post-quantum cryptography," NIS Cooperation Group, Jun. 23, 2025.
[52] UK NCSC, "Timelines for migration to post-quantum cryptography," National Cyber Security Centre, Mar. 2025. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
[53] ENISA, "Post-quantum cryptography: Current state and quantum mitigation," v2, European Union Agency for Cybersecurity, May 2021.
[54] NIST NCCoE, "Migration to post-quantum cryptography," NIST SP 1800-38B (Preliminary Draft), Dec. 2023.
[55] CISA, "Strategy for migrating to automated post-quantum cryptography discovery and inventory tools," CISA, Sep. 2024.
[56] IBM Research, "Cryptographic Bill of Materials (CBOM) speeds quantum safe adoption," IBM Research Blog, 2023.
[57] NSA, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," NSA Cybersecurity, 2021.
[58] NIST, "Mappings of migration to PQC project capabilities to risk framework documents," NIST CSWP 48 (Initial Public Draft), Sep. 2025.
[59] NIST, "Recommendation for stateful hash-based signature schemes," NIST SP 800-208, 2020.
[60] NIST, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," Mar. 2025. Available: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption