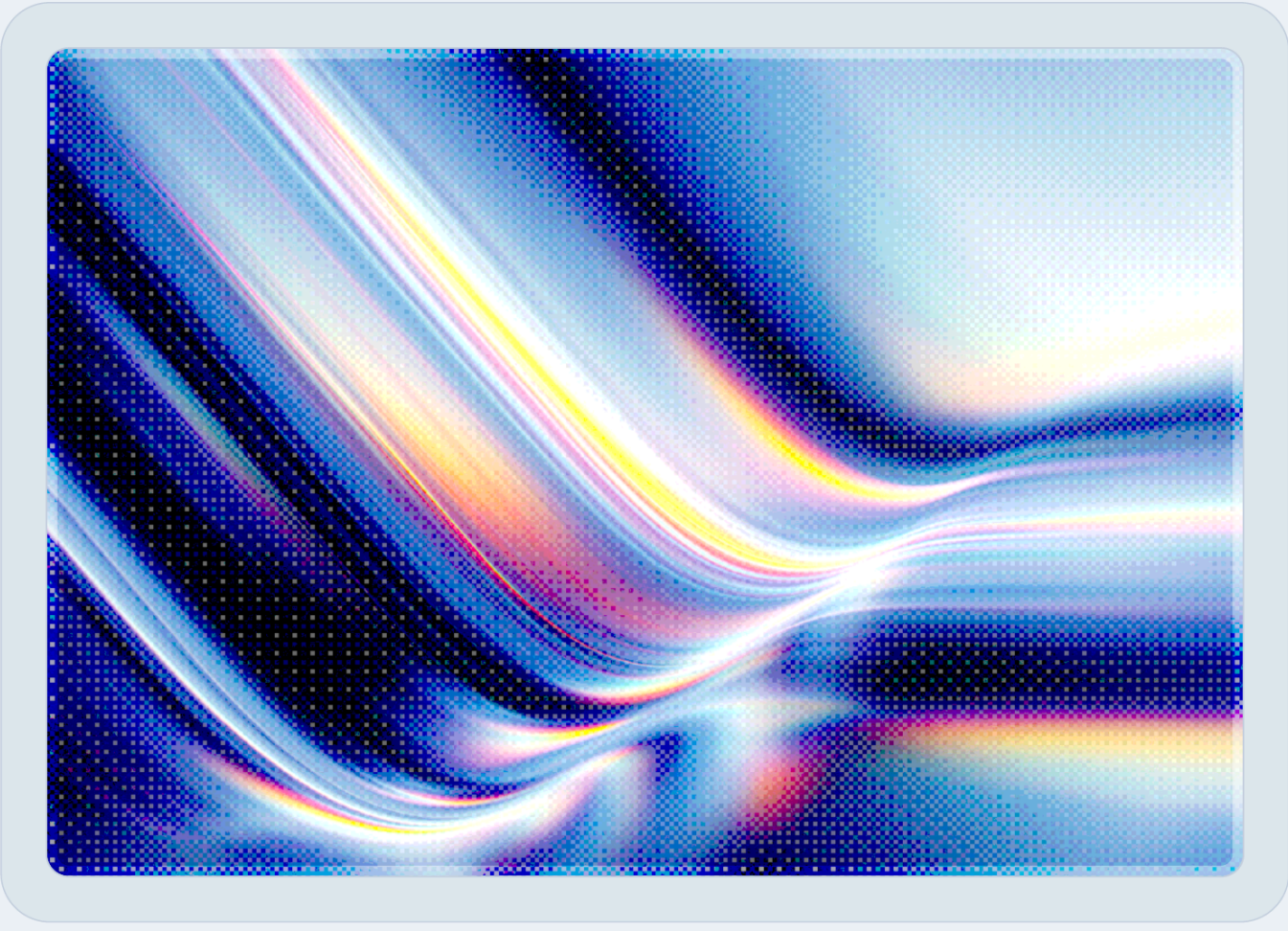
CSAI Foundation | Cloud Security Alliance

Harvest Now, Decrypt Later: Enterprise PQC Migration Gap

Systemic Risk from Deferred Post-Quantum Cryptography Transition

2026-05-31

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- Harvest now, decrypt later (HNDL) attacks are not a future hypothetical. A joint advisory from CISA, NSA, and NIST has explicitly warned that adversaries may already be collecting and storing encrypted data with long-term strategic value for eventual quantum decryption [57], a position shared by the UK NCSC and the Australian Cyber Security Centre [1][13]. China's Salt Typhoon campaign, which compromised at least nine U.S. telecommunications providers and reached over 600 organizations across more than 80 countries, demonstrates the mass-interception infrastructure that makes HNDL viable at scale [2][3].
- The quantum threat window is compressing faster than migration timelines are advancing. Three academic papers published between May 2025 and March 2026 cut the estimated physical-qubit count to break RSA-2048 from roughly 20 million to potentially fewer than 100,000, prompting Google, Cloudflare, and several governments to pull migration deadlines forward toward 2029-2030 [11][20]. IonQ has projected achieving the logical qubit threshold to challenge RSA-2048 in the 2028–2029 window [35], though analysts note this represents a hardware milestone rather than a Q-Day assertion.
- A measurable "migration gap" constitutes a systemic risk in its own right. Large enterprises require an estimated 12-15 years to fully migrate, yet only about 5% have a formal quantum transition plan despite 62% expressing concern [12][58]. If cryptographically relevant quantum computers arrive in 2028-2030 and migration takes 12-15 years, organizations beginning now face an estimated 3-5 year vulnerability window — a range that narrows or widens with revised Q-Day estimates [23].
- AI assets represent a high-value target class for HNDL operations, given that model weights and training corpora are encrypted under the same quantum-vulnerable schemes Shor's algorithm breaks. Adversaries have been reported targeting encrypted model weights, training data, and fine-tuning logs, while agentic AI traffic over the Model Context Protocol (MCP) still rides classical RSA/ECC-based TLS as of mid-2026, absent explicit PQC configuration [29][32]. Long-lived credentials compound the exposure: roughly 64% of secrets confirmed valid in 2022 remained valid in January 2026 [38].
- Crypto-agility, not one-time algorithm replacement, is the durable objective. CSA's Quantum-Safe Security Working Group, NIST's NCCoE migration project, and an IBM/CSA survey of 750 executives (average readiness score of 25 out of 100) all converge on the same

prescription: inventory cryptographic assets now, prioritize long-lived data, and design systems that can swap algorithms without architectural rework [40][48].

Background

Harvest now, decrypt later describes a strategy in which an adversary intercepts and stores encrypted data today with no immediate ability to read it, intending to decrypt it once a cryptographically relevant quantum computer becomes available. The premise is straightforward: data that must remain confidential for ten, twenty, or fifty years is already exposed if it travels or rests under RSA, elliptic-curve, or Diffie-Hellman protection, because those public-key algorithms are vulnerable to Shor's algorithm running on a sufficiently large fault-tolerant quantum machine. A joint advisory from CISA, NSA, and NIST warns that adversaries may already be collecting and storing encrypted data with long-term strategic value for eventual quantum decryption [57], and the UK NCSC has characterized state-actor data theft as long-term collection "for exploitation in years to come" [1][50]. A peer-reviewed analysis frames the defining property of the attack precisely: it "leaves no trace, triggers no alerts, and appears in no security logs," which means an organization cannot detect that it is a victim and cannot remediate after the fact [8].

The reason this matters now, rather than at some indefinite future Q-Day, is that the cost of harvesting has collapsed while the cost of eventual decryption has become the only open variable. A March 2026 arXiv paper reframes HNDL as an economic problem and concludes that retaining intercepted traffic across TLS 1.2, TLS 1.3, QUIC, and SSH is "economically trivial" for nation-state actors, shifting the defensive question "from whether an adversary can archive to how much decryption will cost" [7]. The mass-collection capability is also demonstrably real. China's Salt Typhoon intrusion compromised major U.S. carriers including AT&T, Verizon, T-Mobile, and Lumen, reaching the lawful-intercept infrastructure and enabling real-time tracking, call recording, and message reading at scale [2]; the FBI notified at least 600 organizations across more than 80 nations that they were of interest in the campaign [3]. While Salt Typhoon has not been publicly confirmed as an HNDL operation, it supplies exactly the bulk-traffic interception substrate that an HNDL strategy depends on.

The timeline that governs how long harvested data stays safe is shrinking. NIST finalized its first three post-quantum standards on August 13, 2024 — FIPS 203 (ML-KEM) for key encapsulation, FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) for digital signatures — and added HQC as a backup key-encapsulation mechanism in March 2025 [9][14]. Against that standards backdrop, hardware estimates have moved sharply. Between May 2025 and March 2026, three papers reduced the qubit count needed to break RSA-2048 by roughly a factor of twenty: Google's Craig Gidney brought the 2019 estimate of 20 million qubits below one million; subsequent architectural work pushed estimates lower still, with one

March 2026 result suggesting fewer than 100,000 physical qubits and under 500,000 for the elliptic-curve cryptography protecting most digital signatures and cryptocurrencies [11]. The consensus official estimate for a cryptographically relevant quantum computer remains 2030-2035, but IonQ has projected achieving the logical qubit threshold to challenge RSA-2048 in the 2028–2029 window [35], and current hardware already reaches into the low thousands of physical qubits. The combination of confirmed harvesting, trivial storage economics, and an accelerating hardware curve is what elevates HNDL from a theoretical concern to a present-tense risk.

Security Analysis

The active harvesting threat now reflects a multilateral consensus among major Western signals intelligence and cybersecurity agencies rather than the position of any single organization, and the highest-value targets are precisely the data classes whose sensitivity outlives any plausible decryption timeline. Government, diplomatic, intelligence, and military communications retain value for decades; financial transaction histories, trading algorithms, and regulatory filings remain exploitable for years; and healthcare and biometric records stay sensitive across a patient's lifetime [6]. The Federal Reserve's September 2025 working paper makes the irreversibility explicit for one important case: post-quantum cryptography can protect future transactions, but "no existing method can retroactively safeguard data already recorded on public distributed ledgers," meaning previously recorded financial and blockchain transactions are permanently exposed [5]. A November 2025 House Homeland Security Committee report sharpened the picture further, describing an AI-assisted, partially autonomous PRC cyber operation and warning that adversaries conducting AI-enabled intrusions today "may seek to pair these techniques with future quantum decryption capabilities" against government, defense-industrial, and critical-infrastructure data [4].

Against this active threat sits an enterprise migration gap that is itself a systemic risk. ISACA's 2025 survey of more than 2,600 professionals found that 62% are concerned quantum computing will compromise current encryption, yet only about 5% have a defined transition strategy [58], and a vendor survey found that 75% of businesses worry about HNDL while only 23% have a strategy to address it (per SafeLogic, a provider of FIPS-validated cryptographic modules) [16]. Realistic timelines explain why the gap is so dangerous: modeling cited by ISC2 projects 5-7 years for small organizations, 8-12 years for medium enterprises, and 12-15-plus years for large enterprises under optimistic assumptions [12], and Moody's independently estimates 10-15 years for transitions across all affected devices [12]. When those durations are set against quantum arrival in 2028-2030, organizations starting now confront an estimated 3-5 year window in which significant portions of their infrastructure remain exposed — a range that narrows or widens depending on how both Q-Day estimates and migration timelines evolve [23]. The barriers are structural rather than merely budgetary — incomplete cryptographic inventories, hard-

coded classical algorithms in production code, manual certificate lifecycle management, vendor-imposed limitations, and a talent shortfall in which fewer than 15,000 practitioners worldwide have demonstrated PQC implementation competency against demand projected in the hundreds of thousands by 2030 [15]. The picture is complicated further by TLS certificate lifetimes shrinking from 398 days toward 47 days by 2029, forcing teams to master accelerating certificate churn at the same moment they re-platform onto new algorithms [15].

Critical infrastructure and financial services concentrate this exposure because their migration is both harder and more consequential. The Bank for International Settlements urged financial institutions to "start migrating to post-quantum cryptography now" [17], and Project Leap Phase 2 proved in December 2025 that PQC-signed transfers function in the Eurosystem's TARGET2 system, while simultaneously exposing performance and packet-size failures requiring substantial redevelopment before production use [18]. A hardware blocker compounds the problem: as of early 2026 no HSM vendor had completed a FIPS 140-3 Level 3 validation with PQC algorithms inside the validated boundary, which stalls SWIFT-compliant deployment for most institutions [19][47]. Protocol-level constraints are equally stubborn — ML-DSA signatures (2,420–4,627 bytes) and SLH-DSA signatures (up to roughly 49,856 bytes) far exceed the 512-byte DNS UDP limit, making DNSSEC and BGP the most structurally resistant protocols to migrate [26][28][59][60]. Asynchronous migration is itself a failure mode: a May 2026 Monte Carlo study of Australia's real-time payment platform found transaction-failure rates spiking when 40-60% of participants had migrated and the rest had not [30], and in written public comments submitted to the SEC, one financial security researcher flagged a $317 billion stablecoin market, $36 billion in tokenized real-world assets, and $33 trillion in annual stablecoin transaction volume as systemically exposed if sector actors fail to migrate in coordination [29]. Healthcare carries a parallel burden, where HIPAA's 50-plus year retention requirements and medical devices with 5-25 year service lives mean equipment implanted today will remain in patients past both the 2030 and 2035 deadlines, leaving an estimated 98-100% of healthcare records encrypted today exposed to retroactive decryption [21][22].

For the AI Safety Initiative, the most consequential intersection is that AI assets represent a high-value target class for HNDL operations, and AI infrastructure is among the least protected layers of the stack. Security researchers have assessed that adversaries may be collecting and storing large volumes of encrypted AI training data, model checkpoints, and proprietary weights for deferred decryption once cryptographically relevant quantum computers arrive [31]. Because model weights and training corpora are encrypted under the same RSA and ECC schemes Shor's algorithm breaks, archived models and datasets inherit the full HNDL exposure, and quantum-accelerated model-inversion attacks could later reconstruct anonymized training data faster than classical methods allow [33][34]. The agentic layer is especially fragile: AI agents communicating over MCP authenticate and exchange tool calls across classical TLS, so inter-agent and agent-to-tool channels are directly harvestable, and shadow AI agents — unsanctioned AI tools operating outside organizational governance — connecting to external APIs and vector databases over outdated handshakes face identity-spoofing risk once quantum capability lands

[32]. This quantum exposure rides on top of an acute secrets-management crisis that exists independently of quantum: GitGuardian recorded approximately 29 million secrets exposed in public GitHub during 2025, a 34% year-over-year increase, with AI-service credential leaks up 81% and 24,008 secrets found in MCP configuration files [36][37]. Credential persistence compounds this risk: roughly 64% of credentials confirmed valid in 2022 were still valid in January 2026 [38] — which means a secret harvested today can remain exploitable well into the quantum threat window even before any cryptography is broken. It is worth being precise about what AI does and does not change in cryptanalysis: large language models remain weak at direct decryption, with the best model scoring only 45.14% on the CipherBank benchmark [56], so the near-term AI risk is augmentation of side-channel and hybrid quantum-classical attacks rather than LLMs independently breaking ciphers [34].

Recommendations

Immediate Actions (next 30-90 days)

Enterprises should begin cryptographic discovery and inventory immediately, treating it as the prerequisite that gates every subsequent migration decision. NIST's NCCoE migration project and NIST IR 8547 both emphasize that organizations without complete asset visibility cannot prioritize or sequence migration and face the highest risk of missing the 2031 deprecation milestone [14][25]. A thorough inventory must explicitly include AI infrastructure components — model-weight storage, training-data pipelines, KMS-managed keys, and MCP and agent authentication paths — because most established cryptographic inventory frameworks predate widespread AI infrastructure deployment and may not address these components by default [39]. CISA's product categories guidance and its broader PQC initiative provide practical reference taxonomies for scoping these inventories [27][51].

Alongside inventory, organizations should classify and rank data by confidentiality lifetime rather than by current sensitivity alone. The operative test is whether a given dataset needs to remain confidential past the expected arrival of a cryptographically relevant quantum computer. Government communications, financial transaction records, healthcare data, and proprietary AI assets all carry decade-plus value that places them in the first migration wave [6][22].

Where vendors already ship post-quantum protections, enabling them is a low-effort, low-risk step that provides immediate insurance against ongoing harvesting. AWS KMS, ACM, S3, and Secrets Manager support ML-KEM hybrid TLS [41][42]; Azure Key Vault and Google Cloud KMS support ML-KEM-based key operations [44][48]; OpenSSL 3.5.0 defaults to hybrid keyshares [43]; and Microsoft made ML-KEM

and ML-DSA generally available across Windows Server 2025, Windows 11, and .NET 10 in November 2025 [39][52]. Turning these protections on for in-transit data is low-friction, low-disruption insurance against the harvesting occurring now.

Short-Term Mitigations (6-18 months)

Establishing crypto-agility as an architectural requirement is the single most durable investment an organization can make in this space. Only about 37% of organizations have implemented cryptographic agility frameworks, and 62% report critical systems that cannot support PQC without hardware replacement [46]; designing for algorithm substitution now avoids costly retrofits when standards or threat estimates shift. The objective is not a one-time migration but a posture that can accommodate future algorithm changes without architectural rework — a distinction that becomes important as the field continues to evolve.

Long-lived AI assets warrant explicit prioritization in migration planning. Model weights should be signed with ML-DSA at the moment they leave training clusters, creating an immutable chain of custody that protects against both supply-chain injection and future quantum forgery; core LLM weights belong in the first migration wave [39]. Hybrid encryption should be adopted for MCP and agent-to-tool channels, where the latency overhead is negligible relative to LLM inference time [39].

Secrets management and coordinated migration deserve parallel attention. The secrets-sprawl exposure documented in the Security Analysis does not require quantum computers to be dangerous — harvested credentials can be exploited immediately. AI-assisted development pipelines require explicit secret-detection tooling; GitGuardian's State of Secrets Sprawl 2026 report found that Claude Code-assisted commits exposed secrets at 3.2% versus a 1.5% baseline for non-AI-assisted commits [36], and AI-service credential leaks grew 81% during 2025 alone [36][37]. Long-lived credentials should be rotated aggressively, and agent secrets should be routed through managed services rather than configuration files [37][38][39]. Because asynchronous migration produces transient interoperability failures when 40-60% of network participants have migrated [30], financial services and critical-infrastructure operators should sequence migration with counterparties and align to the BIS and G7 phased roadmaps [17][24].

Strategic Considerations (2-5 year horizon)

The 2030–2031 period represents a hard inflection in the regulatory landscape, and migration programs should be structured with that deadline as the anchor. NSA CNSA 2.0 stops approving RSA, Diffie-Hellman, and ECC for new National Security Systems as of 2025, requires CNSA 2.0 support in new NSS acquisitions by January 1, 2027, and phases out legacy equipment by December 31, 2030 [9]; NIST

deprecates 112-bit classical algorithms by 2031 and disallows them by 2035 [14]; the EU requires high-risk sectors to migrate by end of 2030 [12]; and the UK NCSC sets discovery by 2028, high-priority migration by 2031, and full migration by 2035 [50]. Federal civilian migration alone is estimated at $7.1 billion through 2035 [54], a useful scale anchor for enterprise budgeting.

HSM, PKI, and protocol maturity are multi-year dependencies that must be tracked rather than assumed. No public PQC X.509 certificates are expected to be broadly trusted before 2027 [45], HSM vendors are delivering PQC capability via firmware ahead of full re-certification [47], and DNSSEC and BGP require IETF working-group action not yet finalized [28]. Sequencing cloud KMS key migration ahead of cloud CA migration, as CSA's April 2026 guidance recommends, reduces dependency risk in cloud-native deployments [49].

The core strategic objective is not to complete migration before Q-Day but to shrink the interval during which long-lived, high-value data remains under quantum-vulnerable protection while adversaries are already harvesting it. The gap window is the risk, and every year of delayed migration extends the exposure of data collected today.

CSA Resource Alignment

CSA's Quantum-Safe Security Working Group has produced the practitioner-facing guidance most directly applicable to closing this gap. "A Practitioner's Guide to Post-Quantum Cryptography" (November 2025) offers a roadmap for assessing vulnerable cryptographic components, evaluating store-now-decrypt-later threats, and mapping mitigations for data in transit and at rest, with steps tailored to enterprises lacking in-house cryptographic expertise [40]. For governance, "Quantum-Safe Security Governance with the Cloud Controls Matrix" aligns specific CCM controls to NIST FIPS 203, 204, and 205, giving organizations a control-level vocabulary for quantum readiness [55]. The IBM/CSA Quantum-Safe Readiness Index, drawn from 750 executives, supplies the sobering baseline — an average score of 25 out of 100 and a 36% skills shortfall — that quantifies how far most organizations remain from where these controls expect them to be [48].

These resources connect to CSA's broader assurance and architecture frameworks. The Cloud Controls Matrix v4.1, released November 6, 2025 with 207 controls and mandatory for new STAR assessments beginning July 2027, is the vehicle through which quantum-aligned cryptographic requirements will propagate into third-party assurance; STAR assessments will inherit those expectations as v4.1 becomes mandatory [53]. Because PQC migration is fundamentally about validating algorithms, key lifetimes, and trust hierarchies, it is also a Zero Trust concern: every authentication, key exchange, and signature in a

zero-trust architecture must eventually be quantum-resistant, and CSA's April 2026 guidance recommends migrating cloud KMS keys ahead of cloud certificate authorities in cloud-native zero-trust deployments [49].

For AI systems specifically, the CSA MAESTRO threat-modeling framework provides the lens through which HNDL should be evaluated across the agentic stack. HNDL exposure maps onto MAESTRO's concern for the data layer (harvested training data and model weights), the foundation and deployment layers (model checkpoints encrypted under quantum-vulnerable schemes), and the agent and ecosystem layers (MCP and agent-to-tool channels riding classical TLS, plus the credential-sprawl exposure across agentic pipelines). Modeling these flows with MAESTRO surfaces precisely the AI-specific cryptographic dependencies that generic PQC inventories tend to miss, and it reframes post-quantum readiness not as an isolated cryptography project but as an integral requirement of trustworthy AI deployment.

References

[1] Palo Alto Networks. "Harvest Now, Decrypt Later (HNDL)." Cyberpedia, 2025.

[2] U.S. Senate Commerce Committee. "Experts Agree U.S. Communications Networks Remain Vulnerable Following Salt Typhoon Hack." December 2025.

[3] Nextgov/FCW. "Salt Typhoon hackers targeted over 80 countries, FBI says." August 2025.

[4] U.S. House Committee on Homeland Security. "Homeland Republicans Request Testimony Following Report of AI-Assisted PRC Cyber Operation." November 26, 2025.

[5] Federal Reserve Board. "'Harvest Now Decrypt Later': Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks (FEDS 2025-093)." September 2025.

[6] ISC2. "Harvest Now, Decrypt Later." ISC2 Insights, May 2026.

[7] arXiv. "On the Practical Feasibility of Harvest-Now, Decrypt-Later Attacks (arXiv:2603.01091)." March 2026.

[8] MDPI. "Harvest-Now, Decrypt-Later: A Temporal Cybersecurity Risk in the Quantum Transition." 2025.

[9] NSA. "CNSA 2.0 Algorithms Cybersecurity Advisory." May 30, 2025.

[10] Palo Alto Networks. "Post-Quantum Cryptography Standards." 2025.

[11] The Quantum Insider. "Q-Day Just Got Closer: Three Papers in Three Months Are Rewriting the Quantum Threat Timeline." March 31, 2026.

[12] The Quantum Insider. "Post-Quantum Migration Timelines: Government and Industry Impact." May 8, 2026.

[13] HashiCorp. "Harvest now, decrypt later: Why today's encrypted data isn't safe forever." 2025.

[14] NIST. "NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards." November 12, 2024.

[15] Keyfactor. "What is Crypto Agility and How to Prepare for Post-Quantum Migration." 2025.

[16] SafeLogic. "Harvest Now, Decrypt Later Quantum Threat." 2025.

[17] Bank for International Settlements. "Quantum-readiness for the financial system: a roadmap (BIS Papers No. 158)." July 7, 2025.

[18] Bank for International Settlements. "Project Leap Phase 2: quantum-proofing payment systems." December 2025.

[19] NIST. "Cryptographic Module Validation Program: Modules In Process List." NIST CSRC, 2026.

[20] NIST. "Post-Quantum Cryptography (CSRC)." March 2025.

[21] GovInfoSecurity. "Medical Device Concerns for a Post-Quantum World." 2025.

[22] eMudhra. "Harvest Now, Decrypt Later: NIST PQC and HIPAA Readiness." 2025.

[23] MDPI. "Enterprise Migration to Post-Quantum Cryptography: Timeline Analysis and Strategic Frameworks." 2025.

[24] Europol. "Prioritising post-quantum cryptography migration activities in financial services." January 2026.

[25] NIST NCCoE. "Migration to Post-Quantum Cryptography." September 2025.

[26] IETF. "Post-Quantum Cryptography Strategy for DNSSEC (draft-sheth-pqc-dnssec-strategy)." 2025.

[27] CISA. "Post-Quantum Cryptography Initiative." 2026.

[28] arXiv. "Study of Post-Quantum Status of Widely Used Protocols (arXiv:2603.28728)." March 2025.

[29] U.S. Securities and Exchange Commission. "Post-Quantum Financial Infrastructure Framework (PQFIF) — Written Input." September 3, 2025.

[30] arXiv. "Post-Quantum Cryptography Migration in Australian Real-Time Payment Infrastructure (arXiv:2605.02276)." May 2026.

[31] Gopher Security. "Why Is Quantum-Resistant Encryption Critical for AI Infrastructure Security?." 2026.

[32] Gopher Security. "2026 Guide to Post-Quantum AI Infrastructure Security: Protecting MCP." 2026.

[33] Exabeam. "Quantum Threats to Machine Learning: The Next Security Reckoning." December 30, 2025.

[34] arXiv. "Securing Cryptography in the Age of Quantum Computing and AI (arXiv:2603.06969)." March 7, 2026.

[35] PostQuantum.com. "IonQ Claims Q-Day by 2029 — Here's What They Actually Said." 2025.

[36] GitGuardian. "The State of Secrets Sprawl 2026." March 2026.

[37] Help Net Security. "29 Million Leaked Secrets in 2025: AI Agents' Credentials Are Out of Control." April 14, 2026.

[38] GitGuardian. "The State of Secrets Sprawl 2026 — Credential Validity Findings." March 2026.

[39] Gopher Security. "Implementing Quantum-Resistant Cryptography in AI Environments: A 2026 Strategy." 2026.

[40] Cloud Security Alliance. "A Practitioner's Guide to Post-Quantum Cryptography." November 10, 2025.

[41] AWS Security Blog. "ML-KEM post-quantum TLS now supported in AWS KMS, ACM, and Secrets Manager." April 7, 2025.

[42] AWS. "Amazon S3 post-quantum TLS key exchange endpoints." November 2025.

[43] Help Net Security. "OpenSSL prepares for a quantum future with 3.5.0 release." April 9, 2025.

[44] Google Cloud Blog. "Announcing Quantum-Safe Key Encapsulation Mechanisms in Cloud KMS." October 7, 2025.

[45] Cloudflare Blog. "The State of the Post-Quantum Internet in 2025." October 2025.

[46] IoT Security Institute. "Quantum Cryptography: Security Challenges in the Post-Quantum Era." 2025.

[47] PQShield. "Trust Starts in the Hardware: Inside the HSM Strategy for Post-Quantum Security (RSA 2025)." May 2025.

[48] IBM Institute for Business Value / Cloud Security Alliance. "2025 Quantum-Safe Readiness Index." 2025.

[49] Cloud Security Alliance. "Post-Quantum Cryptographic Migration for Cloud-Native Zero-Trust Architectures: What CSA Members Need to Deploy Now." April 6, 2026.

[50] UK National Cyber Security Centre. "Timelines for migration to post-quantum cryptography." 2025.

[51] CISA. "Product Categories for Technologies That Use Post-Quantum Cryptography Standards." January 23, 2026.

[52] Microsoft. "Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms." November 2025.

[53] Cloud Security Alliance. "Cloud Controls Matrix v4.1." November 6, 2025.

[54] Preprints.org. "Estimating Migration Timelines for Enterprises Transitioning to Post-Quantum Cryptography." November 2025.

[55] Cloud Security Alliance. "Quantum-Safe Security Governance with the Cloud Controls Matrix." 2025.

[56] arXiv. "CipherBank: A Cryptographic Benchmark for Large Language Models (arXiv:2504.19093)." April 2025.

[57] CISA/NSA/NIST. "Quantum-Readiness: Migration to Post-Quantum Cryptography (PQC)." August 21, 2023.

[58] ISACA. "Organizations Lack a Quantum Computing Roadmap, ISACA Finds." 2025.

[59] NIST. "FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)." August 13, 2024.

[60] NIST. "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)." August 13, 2024.