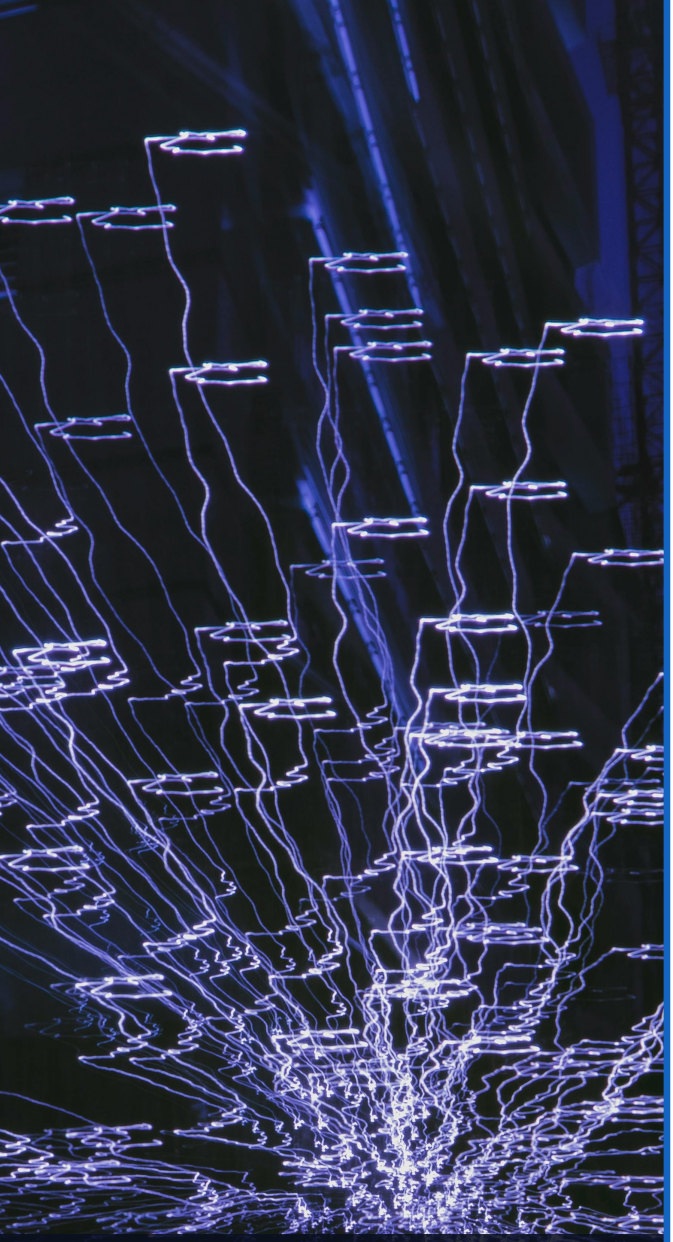

WHITE PAPER

Post-Quantum Cryptography: Developing a Q-Day Readiness Roadmap

How to prepare your organisation for the cryptographic disruption that quantum computing will deliver - and why the time to act is now

A Digital Resilience Strategic Advisory Report

Digital Resilience | www.digitalresilience.co.za | April 2025

Target Audience: Cryptographers, Data Protection Officers, IT Strategic Planners

Digital Resilience

EXECUTIVE SUMMARY

Quantum computing is approaching a threshold that will render the cryptographic foundations of modern digital security obsolete. RSA, the algorithm that secures the majority of internet traffic, financial transactions, and government communications, is mathematically broken by a sufficiently powerful quantum computer. So is Elliptic Curve Cryptography (ECC), which secures VPNs, digital signatures, and mobile communications. The event at which this becomes operationally possible - informally known as Q-Day - is not a distant science fiction scenario. Expert consensus places it between 2030 and 2040, with credible early-case scenarios as soon as 2028.

The critical insight that makes this an immediate concern rather than a future one is the **harvest now, decrypt later (HNDL)** strategy. Nation-state adversaries are collecting encrypted data today - government communications, medical records, financial transactions, intellectual property - with the explicit intention of decrypting it once quantum capability matures. Data encrypted with RSA or ECC today is already compromised in a probabilistic sense if it must remain confidential for a decade or more. The window for retroactive protection has already closed for some categories of sensitive data.

This white paper provides the strategic and practical framework for Post-Quantum Cryptography (PQC) readiness: understanding the threat, assessing cryptographic vulnerability, implementing quantum-safe algorithms, and executing a multi-year migration that is sequenced, measurable, and proportionate to your organisation's risk profile.

2030–2040 Expert consensus range for Q-Day - when quantum computers break RSA	**4+ hrs** Time for a cryptographically relevant quantum computer to break RSA-2048
USD 3T+ Value of global financial transactions secured by vulnerable cryptography daily	**2024** Year NIST finalised the first four Post-Quantum Cryptography standards

> *"The organisations that will be most exposed on Q-Day are not those that ignored quantum computing - they are those that assumed they had more time than they did. The migration to quantum-safe cryptography is a decade-long programme that must begin now."*
>
> **- Yaron Assabi**

THE QUANTUM THREAT – UNDERSTANDING THE STAKES

To understand why quantum computing threatens current cryptography, it is necessary to understand why that cryptography works in the first place. RSA and ECC derive their security from mathematical problems that are computationally intractable for classical computers - problems so hard that solving them would take longer than the age of the universe with current hardware. Quantum computers change this fundamental equation.

What Quantum Computers Actually Break

Shor's Algorithm, developed in 1994, demonstrates that a sufficiently powerful quantum computer can solve the integer factorisation problem (the basis of RSA) and the discrete logarithm problem (the basis of ECC and Diffie-Hellman key exchange) in polynomial time. This is not a marginal improvement in computing speed - it is a categorical change. An algorithm that would take a classical computer millions of years to execute would be completed by a large-scale quantum computer in hours.

Algorithm	Current Security Basis	Quantum Threat	Status on Q-Day
RSA-2048/4096	Integer factorisation hardness	Shor's Algorithm	Completely broken
ECDSA / ECDH	Elliptic curve discrete logarithm	Shor's Algorithm	Completely broken
Diffie-Hellman	Discrete logarithm problem	Shor's Algorithm	Completely broken
AES-128	Symmetric key exhaustion	Grover's Algorithm	Security halved - upgrade to AES-256
AES-256	Symmetric key exhaustion	Grover's Algorithm (weakened)	Remains acceptable
SHA-256	Hash collision resistance	Grover's Algorithm (weakened)	Marginal reduction - SHA-384+ preferred

The Breadth of What Breaks

The scope of cryptographic exposure on Q-Day is not limited to a few niche applications. Every system that relies on public-key cryptography for key exchange, authentication, or digital signatures is affected. This encompasses the entire fabric of modern digital trust:

- **TLS/HTTPS** - the protocol securing all web traffic, online banking, e-commerce, and API communications relies on RSA or ECC for key exchange.
- **Digital signatures** - code signing certificates that verify software authenticity, document signing, and email signing (S/MIME, PGP) all use vulnerable algorithms.
- **VPNs and SSH** - remote access and server management protocols use Diffie-Hellman or ECDH for session key establishment.
- **Public Key Infrastructure (PKI)** - the certificate authority system that underpins identity verification across the internet is built on RSA and ECC.
- **Blockchain and digital assets** - cryptocurrency wallets use ECDSA for transaction signing; funds in wallets with exposed public keys would be at risk of theft.
- **Hardware Security Modules (HSMs)** - many HSMs cannot be software-updated to support new algorithms and will require hardware replacement.

The Harvest Now, Decrypt Later Threat

The HNDL threat transforms quantum computing from a future risk into a present one. Adversaries do not need quantum computers today to exploit quantum vulnerability today. They simply need to collect and store encrypted data now, and wait for quantum capability to arrive.

This strategy is rational and well-documented. Signals intelligence agencies have historically retained encrypted communications they could not decrypt in hope of future capability. The same logic applies to quantum. Any data encrypted today that must remain confidential for 10 or more years - national security communications, long-term R&D;, medical records, financial agreements, legal documents - should be considered potentially compromised under the HNDL model.

> **Classifying Data by Sensitivity Horizon**
> Not all data carries the same quantum risk. The key variable is how long confidentiality must be maintained. Data that needs 2-year protection (short-term business communications) carries minimal quantum risk. Data requiring 10-year protection (R&D; roadmaps, product designs) is at moderate risk. Data requiring 20+ year protection (national security, long-term contracts, health records, infrastructure design documents) should be treated as already exposed under the HNDL model and prioritised for immediate re-encryption with quantum-safe algorithms.

ASSESSING YOUR CRYPTOGRAPHIC VULNERABILITY

Before any migration can begin, organisations must understand what they have. Cryptographic assets are embedded throughout enterprise infrastructure in ways that are rarely documented, frequently forgotten, and deeply interconnected. The discovery and risk assessment phase is the foundation of the entire PQC readiness programme - and it is the phase most organisations systematically underinvest in.

Building a Cryptographic Bill of Materials (CBOM)

The Cryptographic Bill of Materials is the foundational inventory artefact of PQC migration - a comprehensive catalogue of every cryptographic algorithm, key, certificate, and library in use across the organisation's estate. Analogous to the Software Bill of Materials (SBOM) that has become standard practice in supply chain security, the CBOM makes the cryptographic attack surface visible and manageable.

A complete CBOM requires inputs from multiple discovery methods used in combination:

- **Network traffic inspection** - analysing TLS handshakes to identify cipher suites and key exchange mechanisms in active use across internal and external communications.
- **Certificate inventory** - cataloguing all X.509 certificates issued by internal CAs or public CAs, including their algorithm, key size, expiry, and the systems they protect.
- **Code analysis** - static and dynamic analysis of application codebases to identify cryptographic library calls, hardcoded algorithms, and deprecated function usage.
- **Configuration scanning** - reviewing server, network device, and cloud service configurations for cryptographic settings.
- **Vendor questionnaires** - systematic engagement with all technology vendors to understand their PQC roadmaps and the algorithms embedded in their products.

Vulnerability Classification and Prioritisation

Category	Examples	Quantum Risk	Migration Priority
Critical	RSA key exchange in TLS, ECDH in VPN, ECDSA in code signing	Completely broken on Q-Day	Immediate - Phase 1
High	Hybrid TLS (vulnerable key exchange + AES payload)	Key exchange broken; payload safe	Near-term - Phase 2

Category	Examples	Quantum Risk	Migration Priority
Medium	AES-128 symmetric encryption	Security halved by Grover	Planned - Phase 3
Lower	SHA-256 hashing	Marginally weakened	Opportunistic - Phase 4
Monitor	AES-256, SHA-384/512	Acceptable margin remains	Track standards evolution

The Legacy System Challenge

The most intractable challenge in PQC migration is the long tail of legacy systems that cannot be updated to support new algorithms without hardware replacement. Industrial control systems, SCADA infrastructure, embedded medical devices, HSMs, and older network equipment often have cryptographic capabilities baked into firmware or hardware that cannot be patched.

Hardware refresh cycles for these systems are measured in decades, not years. A SCADA system installed in 2015 with a 25-year operational lifecycle will still be running in 2040 - on the far side of the expected Q-Day window. Organisations with significant OT or embedded system estates must begin hardware lifecycle planning for PQC compatibility now, as part of standard capital expenditure cycles, even if algorithm migration is not yet possible.

POST-QUANTUM ALGORITHMS AND QUANTUM KEY DISTRIBUTION

In 2024, the National Institute of Standards and Technology (NIST) completed its multi-year Post-Quantum Cryptography Standardisation process, finalising the first four quantum-resistant algorithm standards. These standards provide the algorithmic foundation for PQC migration and should be the basis of all new cryptographic implementations.

The NIST PQC Standards

Standard	Former Name	Type	Security Basis	Primary Use Case
ML-KEM	CRYSTALS-Kyber	Key Encapsulation	Module Learning With Errors (MLWE)	Replacing RSA/ECDH for key exchange
ML-DSA	CRYSTALS-Dilithium	Digital Signature	Module Learning With Errors (MLWE)	Primary signature standard

Standard	Former Name	Type	Security Basis	Primary Use Case
SLH-DSA	SPHINCS+	Digital Signature	Hash function security only	Conservative fallback signature scheme
FN-DSA	FALCON	Digital Signature	NTRU lattice problem	Compact signatures for constrained environments

The lattice-based algorithms (ML-KEM, ML-DSA, FN-DSA) offer strong performance characteristics and are the recommended primary choice for most enterprise use cases. SLH-DSA, based purely on hash function security, offers a conservative option for applications where long-term confidence in the underlying mathematical assumption is paramount, at the cost of larger signature sizes.

The Hybrid Migration Strategy

Migrating directly to PQC algorithms without a hybrid transition period carries its own risk. The NIST standards, while rigorous, are significantly less battle-tested than RSA and ECC, which have survived decades of intensive cryptanalytic scrutiny. A cryptanalytic breakthrough against a lattice-based algorithm - while considered unlikely - cannot be ruled out.

The recommended approach during the transition period is **hybrid cryptography**: combining a classical algorithm (ECDH) with a post-quantum algorithm (ML-KEM) in a single key exchange, so that security is maintained as long as either algorithm remains unbroken. This approach is already being deployed in production by Google, Cloudflare, and major browser vendors in TLS 1.3 hybrid key exchange, providing forward-looking protection without abandoning proven classical security.

> **Cryptoagility: The Most Important Design Principle**
> Cryptoagility - the ability to swap cryptographic algorithms without re-engineering the systems that use them - is the single most valuable property an organisation can build into its cryptographic infrastructure today. Systems designed with cryptoagility can migrate algorithms as standards evolve, as new vulnerabilities are discovered, and as quantum computing capability advances - without the expensive, disruptive re-architecture that inflexible systems require. Every new system built or procured today should have cryptoagility as a non-negotiable requirement.

Quantum Key Distribution (QKD)

Quantum Key Distribution is a physics-based approach to key exchange that uses quantum mechanical properties - specifically the observer effect - to make eavesdropping on key exchange physically detectable. Unlike PQC, which is a software-based algorithmic approach, QKD requires dedicated quantum communication channels: specialised optical fibre or satellite links.

QKD and PQC are complementary rather than competing technologies. QKD is appropriate for specific high-security, point-to-point links where the infrastructure investment is justified: government networks, financial institution interconnects, and critical national infrastructure. It is not a general-purpose replacement for PQC in enterprise environments - it cannot scale to internet-wide communications, does not address authentication (classical or post-quantum authentication is still required), and carries significant cost and operational complexity.

> *"Quantum Key Distribution solves one problem very well. Post-Quantum Cryptography solves the broader enterprise problem. Organisations that conflate the two risk misallocating their migration budget significantly."*
>
> **- Yaron Assabi**

69 Candidate algorithms evaluated in the NIST PQC competition (2016-2024)	**4** Final standards published by NIST in 2024 - the new quantum-safe baseline
3x–10x Larger key and signature sizes in PQC vs. classical algorithms - plan for overhead	**2028** Earliest credible Q-Day scenario based on current quantum hardware trajectories

THE Q-DAY READINESS ROADMAP – A MULTI-YEAR MIGRATION PLAN

PQC migration is not a single project with a defined end date. It is a continuous programme that spans discovery, prioritisation, piloting, systematic migration, and ongoing adaptation as standards evolve and quantum hardware capability advances. The following five-phase roadmap provides a structured framework for organisations at any current maturity level.

Phase 1 - Awareness and Governance (0-6 Months)

- **Executive briefing:** Frame the quantum risk in business terms - regulatory exposure, HNDL threat, insurance and liability implications, and competitive risk. Boards and executive teams must understand that this is a capital planning issue, not merely a technical one.

- **Establish a PQC Working Group:** Assemble cryptographers, IT architects, legal and compliance leads, procurement representatives, and business unit heads. Assign a named executive sponsor with budget authority.
- **Regulatory landscape review:** Map applicable mandates. NIST standards adoption timelines, NSA CNSA 2.0 suite requirements, EU NIS2 and forthcoming quantum security guidance, PCI-DSS future versions, and sector-specific requirements (DORA for financial services, FDA for medical devices).
- **Immediate no-cost actions:** Download and review NIST PQC standards. Add PQC readiness questions to all new vendor RFPs and contract renewals. Identify internal staff with cryptography expertise and assess whether external specialist support is required.

Phase 2 - Discovery and Risk Assessment (6-18 Months)

- **Execute the CBOM:** Conduct the cryptographic inventory using the multi-method approach described in Section 2. Prioritise internet-facing systems, systems handling long-horizon sensitive data, and systems with known hardware upgrade constraints.
- **Vendor engagement programme:** Issue PQC readiness questionnaires to all technology vendors. Track their published migration timelines. Flag vendors with no PQC roadmap as high-risk supply chain dependencies.
- **Identify cryptoagile systems vs. legacy constraints:** Categorise every system in the CBOM as cryptoagile (algorithm can be swapped via configuration or software update), software-updatable (requires development work), or hardware-bound (requires physical replacement).
- **Data sensitivity mapping:** Overlay the cryptographic inventory with a data sensitivity and retention analysis. Systems protecting long-horizon sensitive data with vulnerable cryptography are the highest priority.

Phase 3 - Pilot and Proof of Concept (12-24 Months)

- **Select 2-3 high-priority pilot systems:** Choose internet-facing, high-sensitivity systems with cryptoagile architecture. External TLS endpoints are the ideal starting point - hybrid TLS 1.3 with ML-KEM can be deployed with minimal application changes.
- **Performance benchmarking:** PQC algorithms have larger key and signature sizes than classical algorithms (ML-KEM keys are approximately 3x larger than RSA-2048 equivalents). Benchmark latency, throughput, and storage impact in production-representative environments.
- **Certificate Authority migration planning:** Design the PQC PKI hierarchy that will replace RSA-based certificate chains. Plan HSM firmware updates or hardware replacement timelines.
- **Developer education:** Update internal cryptography guidelines to mandate use of PQC-safe libraries in all new development. Introduce cryptoagility requirements into architecture review processes.

Phase 4 - Systematic Migration (2-5 Years)

The systematic migration phase executes the full estate migration in priority order, working outward from the highest-risk systems identified in Phase 2. Progress is tracked against the CBOM, with quarterly reporting to executive sponsors and annual third-party audit.

Priority Tier	System Type	Target Timeline	Migration Approach
Tier 1	Internet-facing, long-horizon sensitive data	Year 1-2	Hybrid TLS, PQC digital signatures
Tier 2	Internal systems, privileged access, PKI infrastructure	Year 2-3	PQC certificate chains, secrets re-encryption
Tier 3	SaaS and cloud services - vendor-dependent	Year 2-4	Vendor engagement, contractual PQC requirements
Tier 4	Legacy and OT systems - hardware constrained	Year 3-5+	Hardware replacement planning, compensating controls
Tier 5	Symmetric cryptography uplift	Year 3-5	AES-128 to AES-256 migration, SHA-256 to SHA-384+

Phase 5 - Validation and Continuous Improvement (Ongoing)

- **Third-party cryptographic audits:** Annual audits by specialist PQC firms to validate migration completeness and identify gaps.
- **Standards monitoring:** NIST may standardise additional algorithms; cryptanalytic advances may require algorithm retirement. A dedicated function must track the standards landscape continuously.
- **Incident response planning:** Define the response playbook for the scenario where a classical cryptographic break occurs before migration is complete - who is notified, what is the emergency re-encryption priority, and which compensating controls can be applied immediately.
- **Cryptoagility validation:** Periodically test that cryptoagile systems can actually execute an algorithm swap within the target timeframe. A cryptoagility claim that has never been tested is a compliance fiction.

STRATEGIC RECOMMENDATIONS FOR SECURITY AND IT LEADERS

The following actions are sequenced by urgency and addressable without waiting for a complete CBOM or executive-sponsored programme. Every organisation can begin some of these today.

Actions Requiring No Budget (Start Immediately)

- Download NIST FIPS 203 (ML-KEM), 204 (ML-DSA), and 205 (SLH-DSA) and distribute to your cryptography and architecture teams.
- Add a PQC readiness question to every vendor assessment, RFP, and contract renewal process: 'What is your published timeline for migrating your products to NIST-standardised PQC algorithms?'
- Identify which of your technology vendors have published PQC roadmaps and which have not. Vendors with no roadmap are a supply chain risk.
- Brief your board and executive team. Frame the risk in business language: regulatory exposure, insurance implications, and the HNDL threat to data that must remain confidential for 10+ years.

Near-Term Investments (6-18 Months)

- **Fund and execute the CBOM.** This is the most important investment in the programme. Without it, you are migrating blind.
- **Deploy hybrid TLS on internet-facing endpoints.** This is available in current versions of nginx, Apache, and major cloud load balancers. It provides immediate HNDL protection for data in transit at minimal cost.
- **Engage your HSM vendor.** Hardware Security Modules are a long-lead item for PQC migration. Understand whether your current HSMs support PQC via firmware update or require hardware replacement, and plan accordingly.
- **Re-encrypt your highest-sensitivity stored data** with AES-256 if currently using AES-128. This addresses the Grover's Algorithm exposure for symmetric encryption and can be done independently of the broader PQC programme.

The Business Case for the Board

PQC migration must be framed as a capital investment with a measurable risk reduction return, not as an IT cost. The business case has three components: regulatory compliance (NIS2, DORA, and sector-specific mandates increasingly reference cryptographic standards that will require PQC

compliance), cyber insurance (underwriters are beginning to assess quantum exposure; early movers will benefit from more favourable terms), and competitive differentiation (demonstrating quantum-safe security to enterprise customers, government counterparties, and regulated sector partners will become a procurement requirement within this decade).

The cost of inaction compounds over time. Every year of delay compresses the migration timeline, increases the probability that a Q-Day event occurs mid-migration, and expands the HNDL exposure surface for long-horizon sensitive data. The organisations that begin now will migrate at manageable cost and pace. Those that wait will face emergency programmes at crisis cost.

SOURCES AND REFERENCES

1. **NIST**. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (2024).* https://csrc.nist.gov/pubs/fips/203/final

2. **NIST**. *FIPS 204: Module-Lattice-Based Digital Signature Standard (2024).* https://csrc.nist.gov/pubs/fips/204/final

3. **NIST**. *FIPS 205: Stateless Hash-Based Digital Signature Standard (2024).* https://csrc.nist.gov/pubs/fips/205/final

4. **NSA**. *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).* https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

5. **ETSI**. *Quantum Safe Cryptography - Technical Reports and Standards.* https://www.etsi.org/technologies/quantum-safe-cryptography

6. **BSI**. *Migration Guide to Post-Quantum Cryptography*. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie/post-quanten-kryptografie_node.html

7. **IBM**. *IBM Quantum Development Roadmap 2024*. https://www.ibm.com/quantum/roadmap

8. **CISA/NSA/NIST**. *Quantum Readiness: Migration to Post-Quantum Cryptography*. https://www.cisa.gov/quantum-readiness

9. **European Commission**. *EU NIS2 Directive and Quantum Security Guidance.* https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

10. **Cloud Security Alliance**. *Post-Quantum Cryptography for Dummies.* https://cloudsecurityalliance.org/research/topics/post-quantum-cryptography

Partner with Digital Resilience

Digital Resilience provides specialist advisory services to help organisations design and execute their Post-Quantum Cryptography readiness programme. Our services span quantum risk assessment, Cryptographic Bill of Materials development, PQC migration roadmap design, hybrid cryptography deployment, cryptoagility architecture review, and board-level quantum risk briefings.

Our practitioners combine deep cryptographic expertise with practical enterprise architecture experience, helping organisations move from awareness to action in a programme that is sequenced, proportionate, and measurable - whether you are at the beginning of your quantum readiness journey or accelerating an existing programme.

Protecting your Business Ecosystem

yaron@digitalresilience.co.za | www.digitalresilience.co.za