Deloitte.

德勤

The Quantum Clock is Ticking: Ensure your data is secure

Deloitte Cyber

May 2026

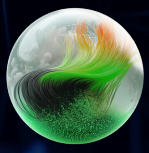
The “Quantum Apocalypse” is not a future IT problem—it is a strategic mandate for the modern boardroom

The bedrock of the global economy is formed by a single, often invisible assumption: that our digital communications are confidential. For decades, this assumption has held true, providing the necessary security for business execution, sensitive intellectual property, and the privacy of billions. However, we are now approaching a “cryptographic cliff” with the advent of Cryptographically Relevant Quantum Computing (QRQC), an incumbent disruption which renders our current defensive measures transparent. This is not a distant theoretical concern—it is a systemic risk to data integrity and the fiduciary responsibilities of the C-suite.

As they navigate this transition, leadership must address the immediate business reality. The “Harvest Now, Decrypt Later” (HNDL) threat which endangers today’s long-term assets requires a multi-year, top-down strategic transformation. Executives and boards require a roadmap outlining the necessity of “Cryptographic Agility” and the urgent need to move to a quantum-ready posture. In the new era of cybersecurity, it is no longer a question of whether the locks will be broken, but how quickly your organization can replace them.

The Deloitte Quantum Advantage

The complexity of the post-quantum landscape requires deep technical expertise and a proven framework for large-scale transformation. We leverage our global insights and specialized heritage to help organizations navigate this transition precisely and proactively.



Deloitte co-authored the "Quantum Readiness Toolkit" in collaboration with the World Economic Forum (WEF)

We are supporting different countries and government entities across the globe on their post quantum journey

Making an impact globally, we bring post quantum and quantum tech solutions from Deloitte centers of excellence worldwide

HNDL: The Delayed Fuse

Harvest Now, Decrypt Later: The Breach Has Already Happened

The most dangerous misconception in cybersecurity today is the belief that quantum threats are a distant concern. The danger is already present: adversaries are intercepting and archiving encrypted, high-value data, stockpiling encrypted transmissions to unlock these the moment a cryptographically capable quantum computer becomes viable.

The HNDL paradigm fundamentally changes your risk profile. If your organization holds data which must remain secret for 10 years or more, such as long-term financial contracts, M&A strategies, trade secrets, or patient records, that data may already be harvested and susceptible to compromise in the next few years.

- Hard Truth: The encryption protecting your "forever data" is effectively a paper shield against a future storm. The adversary may have stolen the key already; they just have not had the strength to turn it yet.
- The Question for the Board: Does your organization have data which must remain confidential until 2036? If the data has already been harvested, then you are merely waiting for the impact to be felt.

Bedrock of Trust (Regulatory Shift)

From Optional Evolution to Mandatory Compliance

Cryptography is undergoing a foundational industry-level change. As the National Institute of Standards and Technology (NIST) in the U.S. finalizes the first set of Post-Quantum Cryptography (PQC) standards (such as FIPS 203 and 204), we are moving toward a world where quantum resilience is no longer a "future-proof" luxury, but a baseline requirement for regulatory compliance.

- The "Skeleton Key" Analogy: Just as SSL 3.0 and early TLS versions were deprecated and deemed non-compliant under PCI-DSS and other frameworks, classical RSA and ECC are approaching their "end of life." Continuing to support them as a primary defense will eventually result in a failure to meet "reasonable security" standards.
- A Shift in Global Governance: NIST has already issued directives for federal agencies to begin the transition, and global financial regulators are following suit. The trend is clear: industry-level protocols like TLS will be fundamentally disrupted. Being prepared now means avoiding the chaotic, high-cost rush of a forced migration when these regulations officially take effect.

The Operational Roadmap

By using a risk-based discovery process, we ensure that your budget is laser-focused on protecting high-value assets first. This targeted approach prevents over-spending on low-risk systems, allowing for a phased migration which spreads costs over time without compromising overall security.

DEFINE → **IDENTIFY** → **PLAN** → **EXECUTE**

Establishing the Foundation

- Organizational Alignment
- Resilience Objectives
- Cryptographic Bill of Materials

Assessing the Catalyst Factors

- Regulatory Compliance
- Operational Demands
- External Factors

Architecting the Path

- Capability Development
- Governance Framework
- Technical Infrastructure
- Resource Prioritization

Sustained Operational Success

- Industry Collaboration
- Continuous Innovation
- Strategic Investment

The Invisible Supply Chain

The Hidden Vulnerability

Organizations often overlook the importance of maintaining a proper Cryptographic Bill of Materials (CBOM): a comprehensive inventory of where encryption is used within operations, especially within third-party vendor software, cloud services, supply chains:

- *Vendor Risk:* If a critical partner such as a cloud provider, payment processor, or logistics firm-fails to upgrade encryption to become quantum resistant, your organization remains vulnerable regardless of your internal efforts.
- *The Endpoint Dilemma:* You can harden your servers, but you cannot control the cryptographic health of an end-user's device, such as a retail banking customer's laptop or a partner's mobile device. This creates a "trust gap" where your secure backend can still be accessed via an insecure frontend.
- *The Action*: Conduct a Cryptographic Discovery immediately. Map encryption usage across all internal apps and third-party dependencies to reveal hidden systemic vulnerabilities. You must know which of your critical vendors are still using obsolete locks and identify workarounds to mitigate risk.

Building Resilience

From Panic to Process: The Strategic Migration

Upgrading an entire enterprise to be quantum-safe overnight is an impossible task which leads to budget exhaustion and operational failure. Success requires a phrased, risk-based approach that balances immediate threats with long-term resilience.

- *Crypto-Agility:* The current selection of PQC algorithms is the best defense we have, but sometimes even the strongest ciphers can eventually be found insecure. You must move away from static security toward a "pluggable" model. Crypto-agility is the ability to swap out algorithms without rebuilding the entire infrastructure, allowing agility in a world full of advancements every day.
- *Strategic Triage:* Apply the "Crown Jewel" principle. You cannot protect everything at once and must decide which assets are most critical to operations (e.g., IP, long-term debt) and which can wait.
- *Culture over Code:* Transitioning to quantum-safe standards requires a fundamental shift in how IT teams manage security, often leading to "change fatigue." Leadership must frame this as a vital evolution of professional competence rather than just another burdensome IT task.

Preserving Strategic Capital

Navigating the Quantum Transition through Capital Preservation

Our methodology focuses on institutional resilience through an informed lens of capital efficiency, ensuring security modernization acts as a catalyst for reducing technical debt rather than as a standalone cost center.

- *Strategic Value Alignment:* By prioritizing high-value assets and aligning with existing infrastructure cycles, we ensure capital is allocated with precision, avoiding the inefficiencies of a generic, broad spectrum approach.
- *Proactive Cost Mitigation:* Early engagement mitigates the risk of late-stage "Digital Y2K" premiums, where talent shortages and market demand for quantum-ready solutions can exponentially inflate implementation costs.
- *Modular Architecture Deployment:* By implementing update-in-place solutions, we prevent the future financial burden of hardware "rip-and-replace" cycles, ensuring long-term budget stability.

The quantum threat is the new Y2K, a multi-year strategic transformation requiring a top-down mandate to combat the immediate HNDL risk.

Reach out to us for focused consultation to evaluate your organization's cryptographic profile and risk exposure.

Contact Us

Eileen CHENG
Cyber – Technology & Transformation
Partner
Tel: +852 2238 7119
eicheng@deloitte.com.hk

Harry WANG
Cyber – Technology & Transformation
Partner
Tel: +852 2238 7908
harrywang@deloitte.com.hk

Paul SIN
Hong Kong Technology and Transformation Banking Lead Partner
paulsin-c@deloitte.com.hk

Tak Chi LIN
Strategy & Innovation Asia Pacific Office
Director
Tel: +852 2238 7762
tclin@deloitte.com.hk

Philip MOK
Cyber – Technology & Transformation
Director
Tel: +852 2740 8829
phmok@deloitte.com.hk