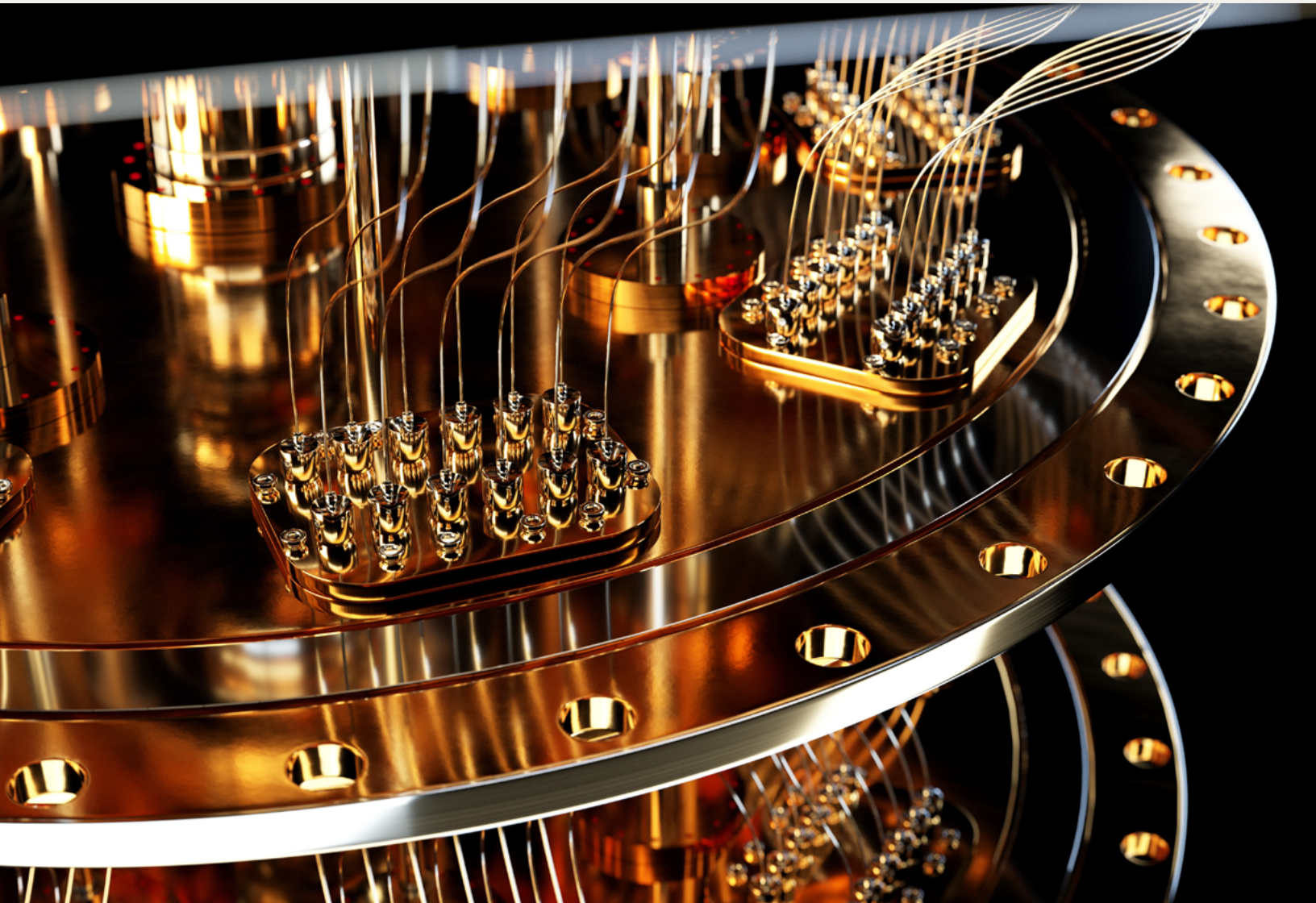
kyndryl

A CIO's guide to the quantum threat

Why your most secure data has an expiration date

by Kris Lovejoy

Global Security and Resiliency Practice Leader, Kyndryl



Introduction

For years, cybersecurity has been defined by the pursuit of resilience — building systems that can withstand disruption rather than simply repel it. Yet the advent of fault-tolerant quantum computing introduces a threat unlike any before it, one that could unravel the cryptographic foundations underpinning the world's digital economy.

This is no longer a theoretical discussion. The global cost of cybercrime is projected to stretch into the trillions of dollars by 2030, and the quantum threat will act as a significant accelerant. For CIOs, this is not merely another technical risk to manage; it is a strategic challenge demanding immediate attention at the executive level. Understanding and preparing for the Post-Quantum Cryptography (PQC) era is the new mandate for building true, long-term enterprise resilience.

The cryptographic time bomb: "Harvest now, decrypt later"

The most insidious aspect of the quantum threat? Its damage has already begun.

Nation-state adversaries and sophisticated criminal syndicates are actively engaged in "Harvest now, decrypt later" attacks. They are siphoning and storing vast quantities of our most sensitive encrypted data — long-term financial records, intellectual property, customers' personally identifiable information, and strategic plans. While this data is secure today, protected by industry-standard encryption like RSA and ECC, its protection has a known, albeit uncertain, expiration date.

The moment a cryptographically relevant quantum computer comes online, it will be capable of breaking this encryption. Every piece of data harvested today is a future liability. For a CIO, this means that data thought to be protected for decades could become suddenly exposed, creating unprecedented regulatory, financial, and reputational risk.

The Y2Q global deadline

This threat is not being ignored by world governments. The U.S. Government's National Security Memorandum 10 has set a hard 2035 deadline for federal agencies to migrate to quantum-resistant standards, effectively firing the starting gun on a global migration effort often called Y2Q — Years to Quantum. The 2035 deadline will create a ripple effect across the private sector, setting the pace for regulators, supply chain partners, and customer expectations worldwide.

This global migration will dwarf the scale of Y2K. Organizations must identify and replace cryptographic protocols embedded deep within legacy software, hardware, and digital certificates across the entire enterprise. Waiting for the quantum threat to fully materialize is not an option; organizations that fail to prepare now will be exposed to a new degree of vulnerability in data security.

The CIO's playbook: Three non-negotiable imperatives

Navigating this transition requires moving beyond awareness to action. For a CIO, the strategic plan can be distilled into three immediate, non-negotiable imperatives:

01 Achieve cryptographic agility: Charter a task force

As a foundational goal, organizations must achieve crypto-agility. This means designing systems so that cryptographic algorithms can be replaced or updated easily, without requiring a complete overhaul of every application. The first step to achieving crypto-agility is to charter a formal post-quantum preparedness task force, sponsored at the executive level, to lead this multi-year effort. This cannot be a side project for the IT department; it must be a recognized strategic initiative.

02 Conduct a crypto census now: Know your risk

The task force's first mandate is to conduct a crypto census — a complete inventory of all public-key cryptography across the enterprise. This effort will identify every application, system, and vendor that relies on vulnerable encryption, creating the foundational blueprint for any migration plan. Because invisible risks cannot be managed, this is a critical due-diligence step that must be funded and prioritized.

03 Plan and budget for migration: Make it a formal initiative

Based on the inventory, the task force must develop a prioritized migration roadmap for transitioning to PQC algorithms approved by the National Institute of Standards and Technology (NIST). Most importantly, migration must be established as a formal, funded line item in future technology and security budgets. Migration is a multi-year, strategic program essential for the long-term resilience of the organization. Treating it as a routine IT upgrade will ensure failure.

Comparing encryption algorithm security: Traditional vs. quantum

A crucial part of a Post-Quantum Cryptography (PQC) strategy is understanding which cryptographic systems are vulnerable, how vulnerable they are, and when that vulnerability might be exploited. The nature of the threat is dramatically different for symmetric and asymmetric encryption.

Here are some common algorithms and the estimated time and resources required to break them with both traditional and quantum computers:

Algorithm	Type	Primary use case / What it encrypts	Time to break (traditional computer)	Time to break (quantum computer)	Quantum resources required
SYMMETRIC ENCRYPTION (SIngle shared key)					
AES-256	Symmetric	Data at rest and in transit. Modern global standard for encrypting files, databases, and network traffic.	Infeasible. Billions of times the age of the universe.	Infeasible. Still thousands of years or more.	Millions of stable physical qubits. Considered quantum-resistant.
3DES / TDEA	Symmetric	Legacy financial and payment systems. Used for ATM transactions and older financial applications.	Feasible. Can be broken in a matter of months or less with dedicated hardware.	Minutes to hours.	A few thousand qubits. The classical threat is more immediate.
DES	Symmetric	Obsolete systems. The original mainframe encryption standard.	Trivial. Can be broken in hours or days with readily available resources.	Seconds.	A minimal quantum computer. It is completely insecure.
ASYMMETRIC ENCRYPTION (Public/private key pair)					
RSA-2048	Asymmetric	Digital signatures and key exchange. Securing web traffic (HTTPS) and verifying software/document authenticity.	Infeasible. Trillions of years.	Hours.	~20 million physical qubits (or ~4,000 stable logical qubits).
ECC	Asymmetric	Digital signatures and key exchange. A modern, efficient alternative to RSA, common in mobile and IoT.	Infeasible. Trillions of years.	Hours.	~300,000 physical qubits (or ~2,500 stable logical qubits).
Diffie-Hellman	Asymmetric	Key agreement. Establishing a shared secret key for protocols like TLS and VPNs.	Infeasible. Trillions of years.	Hours.	Similar resources to RSA/ECC, depending on the key size.

One key takeaway is that asymmetric encryption is urgently threatened. Data clearly shows that a future quantum computer primarily threatens public-key cryptography like RSA and ECC. The ability to break these algorithms in hours renders all data protected by them vulnerable — and fuels "Harvest now, decrypt later" attacks.

Legacy symmetric encryption, on the other hand, is a classical threat. The most critical risk for algorithms like DES and 3DES, often found on mainframes, comes from today's traditional computers. They are already considered broken or deprecated and represent an immediate security vulnerability that should be remediated regardless of the quantum threat.

For all new symmetric encryption needs, AES-256 is the recommended standard for quantum resistance. Grover's algorithm — a quantum algorithm that can accelerate the time required to break encryption — theoretically weakens AES-256. However, the practical requirements to break AES-256 are so immense that it remains secure against all known quantum and classical attacks.

The era of viewing cryptography as a static, solved problem is definitively over. The CIO's role is expanding to manage this new class of foundational risk. By taking decisive action now, leaders can steer their organizations through this historic inflection point. They will need to do more than defend — ensuring they are resilient, adaptive, and intelligent in the face of a new digital reality.

kyndryl