Transformativ IP

Harvest Now,Decrypt Later

An Executive Introductory Primer

For CEOs, CTOs, and CISOs of Mid-Tier Companies and Healthcare Facilities

Understanding the quantum data threat — in 20 minutes

An educational briefing • Not a sales document

How to Read This Document

This primer is built for executives who don't have time to wade through a 40-page technical paper but need to understand the Harvest Now, Decrypt Later (HNDL) threat well enough to make sound decisions. It is educational, not promotional. The goal is to give you a clean, accurate, working understanding of the threat — what it is, why it's real, how it affects mid-tier companies specifically, and what a reasonable response looks like.

If you are…	Read in this order	Estimated time
The CEO	Sections 1, 2, 6, 8	10 minutes
The CTO	Sections 1–4, 6–8	20 minutes
The CISO	All sections — use Section 7 as your working roadmap	25 minutes
Pressed for time	Read only the orange Bottom Line boxes at the end of each section	5 minutes

Four You Need to Know

1. HNDL is not a future problem. The data theft happens now and so does your regulatory liability; the decryption happens later. Adversaries are already stockpiling encrypted data. That's right, your legal liability begins when the data theft takes place not when the encryption is broken.
2. According to Google, IBM and Microsoft Q-Day is projected to be in 2029 Q-Day is the day that 95% of the world's encryption breaks and becomes readable to China, Russia, Iran and cybercriminals.
3. The window for safe migration is shorter than the window for migration itself. A mid-tier company with most PQC solutions requires a few years to fully migrate because hardware is involved and expensive-rip-and-replace. A solution that is 100% software does not have this issue and you can also get a free trialware version that is the full version to run your internal tests. Our preferred solution takes only 90 days for a full installation, and it has the lowest latency and only requires 2 lines of software code.AND is fully certified.
4. The right first step is not buying technology. It is understanding what cryptography you depend on and which of your data has a long shelf life.

Table of Contents

1. What HNDL Actually Is

Harvest Now, Decrypt Later — sometimes called Store Now, Decrypt Later (SNDL) — is a simple, patient attack strategy. It works like this:

Phase	What happens	When
1. Harvest	Adversaries intercept and copy encrypted data using familiar methods: tapping network traffic, compromising servers, hijacking internet routing. They make no attempt to decrypt it yet.	Happening now
2. Store	The stolen ciphertext is archived on cheap, durable storage. Storage costs are negligible. Detection is rare because nothing is being actively attacked.	Ongoing
3. Decrypt	Once a quantum computer powerful enough to break RSA and ECC encryption is operational, the stockpile is processed and the original data is exposed.	Late 2020s to mid-2030s (estimated)

The Core Idea: Data Lifespan Risk

The most useful concept in this whole topic is data lifespan risk. It comes down to a single comparison:

The two timelines	Plain definition
Required secrecy lifetime	How long the data must remain confidential. For a contract, maybe 7 years. For a customer's health record, decades. For genomic data, a lifetime.
Effective encryption lifetime	How long the encryption protecting that data can be expected to hold up. With current RSA and ECC, it depends on when quantum decryption becomes practical.

If the required secrecy lifetime is longer than the effective encryption lifetime, the data is effectively already compromised — even if no one can read it today. The breach has happened; the unlock is just on a delay.

The useful analogy

Imagine a thief who steals a sealed, locked safe from your office. They cannot open it with anything they own today. But they take it home, put it in their garage, and wait. They know that within a few years a tool will exist that can open it. The loss of control over the safe — and everything inside it — happened the day it was taken, not the day it's finally opened.

Bottom line

HNDL decouples the moment of theft from the moment of compromise. The breach is silent, the decryption is deferred, and the damage is retroactive once it arrives. Standard incident response — rotate keys, patch, notify — cannot fix data that was already stolen years ago.

2. Why Quantum Computers Break Today's Encryption

You don't need to be a physicist to understand this. Three short ideas are enough.

Idea 1: Quantum Computers Process Possibilities Differently

Classical computers — every laptop, server, and smartphone you've ever used — work with bits. A bit is either a 0 or a 1. Quantum computers use qubits, which can represent 0, 1, or a combination of both at the same time. This is called superposition.

The practical consequence: for certain narrow classes of math problems, a quantum computer can explore many candidate solutions in parallel instead of one at a time. That parallelism doesn't help with most computing tasks, but it happens to be devastating for the specific math problems behind today's public-key encryption.

Idea 2: Most Internet Security Relies on Two Math Problems

Modern digital trust — banking, e-commerce, login, software updates, secure messaging — is built on public-key cryptography. Two algorithms do nearly all the heavy lifting:

Algorithm	What it does	Underlying math problem
RSA	Encrypts messages and verifies digital signatures across most websites and email systems.	Factoring very large numbers into primes.
ECC (Elliptic Curve Cryptography)	A more efficient alternative used in TLS, blockchains, and mobile devices.	Solving discrete logarithms on elliptic curves.

Both problems are currently considered effectively unsolvable in a useful timeframe by classical computers. Estimates put the time to break RSA-2048 on a classical supercomputer at roughly 300 trillion years.

Idea 3: A Specific Algorithm Changes the Game

In 1994, mathematician Peter Shor published an algorithm — now called Shor's algorithm — that solves both factoring and discrete logarithms efficiently on a sufficiently powerful quantum computer. Estimates suggest that a fault-tolerant quantum computer with around 4,000 stable qubits could break RSA-2048 in roughly 10 seconds.

Computer type	Time to break RSA-2048
Today's most powerful classical supercomputer	~300 trillion years
A sufficiently powerful fault-tolerant quantum computer	~10 seconds

Important nuance: a quantum computer powerful enough to do this does not exist today. The question is when one will, and how soon the migration to quantum-resistant cryptography has to be complete.

Bottom line

The threat is mathematical, not magical. A specific algorithm running on a specific kind of hardware breaks the specific math that protects most of the internet. The hardware doesn't exist at scale yet, but it's being built openly, with public roadmaps and substantial investment.

3. The Timeline — What's Known, What's Estimated

There is a converging set of public roadmaps and expert estimates. They have been moving earlier, not later nd they have settled on 2029. Largely as a result of Google's Willow Chips error correction capabilities and roadmap. Previously, it was a physics problem, and it is now a scalable engineering problem.

Public Industry Roadmaps

These are stated targets from the companies most actively building quantum hardware. They are goals, not guarantees — but they shape what a prudent risk posture should assume.

Source	Stated target	Year
IBM	A 200-logical-qubit fault-tolerant quantum computer	2029
Microsoft	A cryptographically relevant trapped-ion quantum computer	2029
Google	A useful, error-corrected quantum computer	2029
General expert consensus	Aggressive, credible projections place the CRQC capability	2028–2030
Earlier consensus (pre-2023)	Original mainstream projections (pre-Google Willow Chip)	2035

Expert Probability Estimates

More cautious researchers express the timeline as a probability. One widely cited assessment estimates a 17–34% probability that a quantum computer capable of breaking RSA-2048 will exist by 2034.

For risk management purposes, the exact date matters less than the range. A 20% probability of catastrophic cryptographic failure within ten years is, by any reasonable framework, a risk that deserves a planned response.

The Critical Mismatch: Threat Timeline vs. Migration Timeline

Here is where most executives experience the first uncomfortable moment. The migration to post-quantum cryptography is not a software update. It is a multi-year process of inventory, planning, vendor coordination, and phased replacement.

Organization profile	Typical full PQC migration time
Large enterprise with global operations and complex legacy systems	12–15+ years
Mid-tier enterprise with hybrid infrastructure	8–12 years
Small businesses are primarily dependent on SaaS and cloud vendors	5–7 years

Compare those numbers to the threat timeline above. For a mid-tier company starting today, full migration completes around 2034–2038. CRQC capability may emerge as early as 2028–2030. There is a real gap. The data flowing across your network in that gap is the data most at risk of being harvested.

Bottom line

The honest answer to “when is Q-Day?” is “probably between 2028 and 2035, with informed people split on which end of that range is more likely.” For decision-making, the date is less important than the migration math: if your migration takes 8–12 years and the threat emerges in 3–7 years, every year of delay widens an unrecoverable exposure window.

4. Which of Your Data Is Actually at Risk

Not every byte in your company is at risk from HNDL. The threat is real only for data with a long enough shelf life that it remains valuable, sensitive, or legally protected once quantum decryption is practical. The exercise is to find that subset.

The Four Exposure Tiers

A useful way to triage data is by required secrecy lifetime. Most data falls cleanly into one of four tiers.

Tier	Secrecy required	Examples	HNDL risk
Critical	30+ years, often permanent	Genomic data, intelligence identities, blockchain history, child welfare records	Already compromised if harvested today

Tier	Secrecy required	Examples	HNDL risk
High	10–30 years	Patient medical records, mental health histories, M&A documents, source code with long-lived IP value, long-term contracts	Highly likely to be exposed
Moderate	3–10 years	Customer PII, financial statements, business correspondence, internal strategy documents	Likely exposed if harvested early in the window
Low	Under 3 years	Session tokens, one-time passwords, short-lived auth credentials, transient logs	Generally not an HNDL target

By Sector

Some sectors carry a disproportionate share of long-lifespan data. If your business sits in one of these, HNDL exposure is structural rather than incidental.

Sector	Why it's exposed
Healthcare & life sciences	Medical records and genomic data are sensitive throughout the patient's lifetime. Genomic data is also immutable — once decrypted, the loss of privacy is permanent and may affect relatives and descendants.
Financial services	Long-term contracts, customer financial histories, M&A files, and trading models retain value for decades. Payment infrastructure (SWIFT, ACH, card networks) and Hardware Security Modules depend on RSA and ECC.
Government & defense	Diplomatic communications, intelligence, and classified archives often require 50+ years of confidentiality.
Technology & IP-driven manufacturing	Trade secrets, drug formulas, R&D pipelines, and proprietary source code may remain commercially valuable a decade or more after creation.
Cloud and critical infrastructure	Encrypted client data stores, cross-border transfers, and operational technology in energy, water, and telecom carry extended secrecy and safety requirements.
Public blockchains	The entire historical ledger is a permanently public ciphertext. Decryption of historical transactions would expose every counterparty involved over the chain's lifetime.

The Healthcare Exception: Immutability

Healthcare deserves a separate note. You can change a stolen password, a credit card number, or a Social Security number. You cannot change your DNA. Once decrypted, genomic data is a permanent disclosure — not only about the patient but about their biological relatives and any descendants. The breach is, in a meaningful sense, multi-generational.

Healthcare data breaches already average $9.77 million per incident. HNDL adds long-tail liability: lawsuits and regulatory action that could arrive years or decades after the original theft, against data that the organization may no longer even hold.

Bottom line

The fastest way to scope your own exposure is to ask: which datasets in our possession must remain confidential past 2030, and where do they live? Anything past that line is on the HNDL risk surface. Anything that loses sensitivity within a year or two is not.

5. Why Mid-Tier Companies Have a Specific Problem

Most public material on the quantum threat is written for either Fortune 100 enterprises or for general audiences. Mid-tier companies — roughly, organizations large enough to have meaningful regulated data and complex vendor relationships, but without the dedicated cryptography teams of the largest banks and defense contractors — sit in a particular blind spot. The challenges they face are not just smaller versions of the enterprise challenge.

Five Realities for Mid-Tier Companies

Reality	What it means in practice
You depend heavily on vendors for cryptography	Most of the cryptographic decisions affecting your data are made by your SaaS providers, cloud platforms, payment processors, identity providers, and embedded software suppliers. Your migration path is largely their migration path.
You have limited in-house cryptographic expertise	A dedicated quantum-readiness team is rarely justifiable at this scale. The work has to be absorbed by existing security, engineering, and procurement functions — who already have full plates.
You have more legacy than you think	Most mid-tier companies discovered during the SHA-1 deprecation or Log4j cycles that they had cryptography running in places nobody had inventoried. The same will be true here. Industry research suggests 43% of organizations cannot inventory their cryptographic assets.
Your customers may demand readiness before regulators do	If you sell into healthcare, finance, defense, or government supply chains, your customers will start asking for PQC roadmaps as part of procurement — well before you're legally required to have one.
Your migration window is shorter than an enterprise's, but so is your runway	8–12 years to complete versus 12–15+ for an enterprise. That sounds like a relative advantage — until you factor in less staffing and less bargaining power with vendors.

The Practical Implication

Mid-tier companies generally cannot rebuild cryptographic infrastructure from scratch. The realistic strategy looks different from the enterprise version of the same plan:

- **Inventory first, replace second.** You can't plan migration of cryptography you haven't mapped.
- **Vendor pressure matters more than internal engineering.** Procurement is one of the most effective tools you have. Asking vendors for their PQC roadmap is free and creates real urgency.

- **Crypto-agility beats crypto-replacement.** Designing systems to swap algorithms easily is more durable than picking one "right" algorithm now.
- **Prioritize ruthlessly.** Protect what has the longest shelf life first. Most of your daily transactional data is not the issue.

Bottom line

Mid-tier companies don't need to be quantum cryptography experts. They need to know what cryptography they depend on, which data has a long enough lifespan to be exposed by HNDL, and which vendors are on a credible path to delivering post-quantum support.

6. The Regulatory Picture

The regulatory landscape is moving faster than many executives realize, and for a specific reason: governments treat HNDL as a national security issue, not a privacy issue. That distinction matters — it limits the defenses (such as user consent) that normally apply to data handling.

Major Jurisdictions and Deadlines

Jurisdiction	Mandate or guideline	Key dates
United States	National Security Memorandum 10 (NSM-10) — federal agencies must mitigate quantum risk; annual inventories of vulnerable systems are required	Full mitigation: 2035
United States	NIST PQC standards — FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)	Finalized August 2024
United States	NSA CNSA 2.0 — PQC mandatory for newly classified national security systems	New systems: 2027 / Full transition: 2035
European Union	EU Commission Coordinated Roadmap — high-risk systems (finance, utilities, telecom, government) must complete PQC migration	High-risk: end of 2030 / Broader: 2035
European Union	DORA and NIS2 — cryptographic resilience testing and quantum-threat preparedness required of financial and critical infrastructure entities	Active and enforceable
United Kingdom	NCSC three-phase plan	Discovery: 2028 / Full migration: 2035
Canada	Federal government roadmap	Migration plans: April 2026 / High-priority systems: 2031

How This Reaches Mid-Tier Companies

You may not be a federal agency, a Tier-1 bank, or an EU utility. The regulations above still reach you, typically through three channels:

1. **Procurement clauses.** If you sell to any government, large bank, healthcare system, or critical infrastructure operator, expect contractual requirements for PQC readiness during the 2026–2030 window. Your customer is regulated; you become a sub-requirement of their compliance.
2. **Sectoral overlays.** Finance, healthcare, energy, and telecommunications routinely receive sector-specific guidance from their regulators that closely tracks NIST and EU mandates. DORA in the EU already does this for financial entities of essentially any size.
3. **Insurance and liability.** Cyber insurers are beginning to ask about PQC readiness during renewals. Independent of any statute, your premium and your liability picture will move.

Bottom line

You may not face direct PQC mandates yet. But your largest customers, your insurers, and your sector regulators are on trajectories that will. Inventory and planning work begun in 2026 is on a sensible timeline. Work delayed to 2030 is, for most mid-tier companies, work that finishes late.

7. A Reasonable Response — What to Do First

The steps below are sequenced for a mid-tier company that has not yet started. They are deliberately conservative and do not require selecting a vendor or committing budget to new technology in the first phase. Most of the value of starting now comes from understanding your current state — something you control completely.

Step 1: Build a Cryptographic Inventory (Months 1–6)

You cannot plan a migration of cryptography you haven't mapped. The deliverable is sometimes called a Cryptographic Bill of Materials, or CBOM. For a mid-tier company, this is more tractable than it sounds — most of the cryptography lives in a manageable number of places.

What to inventory	What to capture for each
Web-facing systems (TLS certificates, web servers, APIs)	Algorithm, key length, certificate expiry, issuing authority
Internal services and microservices	Authentication mechanisms, signing keys, mutual TLS configurations
VPN and remote access	Key exchange algorithms, certificate chains, device count
Code signing and software supply chain	Signing keys, key custody, build systems involved
Encryption at rest	Database encryption, backup encryption, key management service in use
Third-party vendors and SaaS	What they encrypt for you, what algorithms they use, their stated PQC roadmap
Hardware Security Modules and HSM-backed systems	Vendor, firmware version, upgrade path

What to inventory	What to capture for each
Legacy and embedded systems (OT, IoT, older line-of-business apps)	What can be patched, what cannot, end-of-life dates

Step 2: Identify Your Long-Lifespan Data (Months 3–6, in parallel)

Run a simple classification exercise: which of our data must remain confidential past 2030? Past 2040? Permanently? You don't need a perfect answer — even a rough categorization tells you which systems and which vendors deserve the most attention in later steps. Cross-reference with the four exposure tiers in Section 4.

Step 3: Engage Your Critical Vendors (Months 6–12)

This may be the single highest-leverage activity you do this year. For each vendor handling Critical-tier or High-tier data, ask three questions:

4. What cryptographic algorithms do you currently use to protect our data, in transit and at rest?
5. What is your published roadmap for post-quantum cryptography? Specifically, when will you support the NIST standards (FIPS 203, 204, 205), and when will you offer hybrid options that combine classical and PQC algorithms?
6. How will you handle migration of data we have already entrusted to you? Will historical data be re-encrypted, or is that our responsibility?

Vendors that cannot answer these questions today are not necessarily disqualified — but the gap between vendors who can and vendors who can't will become procurement-relevant quickly.

Step 4: Adopt Crypto-Agility as a Design Principle (Months 12–18)

Crypto-agility means designing systems so that the cryptographic algorithm is a swappable component, not a hardcoded assumption. Practically, this looks like:

- **Algorithm abstraction —** applications call a cryptographic library through an interface, not by directly invoking RSA or ECC.
- **Parameter flexibility —** key sizes, signature formats, and algorithm choices live in configuration, not in code.
- **Protocol negotiation —** systems agree on supported algorithms at connection time, with safeguards against downgrade attacks.

Crypto-agility pays off whether or not the quantum timeline shifts. If a flaw is found in one of the new PQC algorithms — which has happened before during NIST evaluation — a crypto-agile system swaps in a replacement. A non-agile system requires a code release.

Step 5: Plan a Hybrid Migration (Year 2 onward)

NIST and ENISA both recommend hybrid cryptography during the transition period: combine a classical algorithm (like ECC) with a post-quantum algorithm (like ML-KEM) so that an attacker would have to break both to compromise the data. This is widely viewed as the prudent default until PQC algorithms have additional years of cryptanalytic scrutiny.

Be aware of the practical costs. PQC algorithms produce larger keys and signatures — ML-DSA signatures are roughly 50 times larger than ECDSA — which can affect network performance, firewall configurations, and some embedded systems. Plan for this "bandwidth tax" in capacity and infrastructure conversations.

A Realistic First-Year Roadmap

Quarter	Primary focus	Deliverable
Q1	Sponsorship and scoping	Executive sponsor named; scope agreed (which business units, which data categories)
Q2	Cryptographic inventory begins; data classification in parallel	Initial CBOM covering 60–80% of production systems
Q3	Vendor engagement and roadmap requests	Vendor risk register with PQC readiness scores
Q4	Gap analysis and multi-year plan	Board-ready roadmap with budget request for Year 2

Bottom line

The first year of a sensible response is not a technology project. It is an inventory, classification, and vendor management exercise. Technology decisions — which PQC implementations to adopt and where — belong in Year 2, once you actually know what you have.

8. Common Misconceptions, Corrected

These are the most frequent misunderstandings that surface in executive conversations about HNDL. Pushing back on them, calmly and accurately, tends to be the difference between productive planning and another year of inaction.

You may hear…	The accurate response
"Quantum computers don't exist yet, so this is a 2035 problem at the earliest."	The decryption is a future event. The data theft is happening now. If your data must remain confidential past 2030, the migration is effectively retroactive — it must protect data being moved today.
"Our encryption is fine. We use TLS 1.3."	TLS 1.3 relies on classical key exchange (typically ECDHE) that Shor's algorithm breaks. The protocol version is not the issue — the underlying public-key math is.
"We'll just upgrade when the time comes."	A full PQC migration takes 8–12 years for a mid-tier company. By the time "the time comes," the migration window has closed and the harvested data is already vulnerable.
"Our data isn't valuable enough to be a target."	HNDL harvesting is largely passive and indiscriminate. Adversaries collect broadly and sort later. Storage is cheap; sorting is automated. Selectivity is not the attacker's problem.

You may hear…	The accurate response
"NIST published standards in 2024. Doesn't that mean it's solved?"	Standards exist. Implementations, vendor support, hardware acceleration, performance tuning, and enterprise rollout do not yet. The standard is the starting gun, not the finish line.
"We'll buy a product that fixes it."	No single product fixes it. PQC migration is a multi-year, multi-vendor coordination problem. Tools help with specific phases — discovery, key management, certificate lifecycle — but no product replaces the underlying inventory and planning work.
"This sounds like Y2K. We'll handle it the same way."	Y2K had a fixed deadline, finite scope, and ended in months. Q-Day has an uncertain deadline, broader scope (all cryptography, not just date fields), and an ongoing threat (HNDL harvesting is already happening). The lessons of Y2K about executive sponsorship apply; the timeline assumptions do not.

9. Glossary

Plain-English definitions of every term used in this document, in alphabetical order.

Term	Definition
CBOM (Cryptographic Bill of Materials)	An inventory of every place cryptography is used across an organization: which algorithms, which key lengths, which certificates, which vendors.
Crypto-agility	The practice of designing systems so cryptographic algorithms can be swapped easily, without rebuilding the system. Enables fast response when standards change or vulnerabilities are found.
CRQC (Cryptographically Relevant Quantum Computer)	A quantum computer powerful and reliable enough to break current public-key encryption. Does not yet exist; estimates for its arrival range from 2028 to 2035+.
Data lifespan risk	The mismatch between how long data must remain confidential and how long its encryption can be expected to hold. The defining concept behind HNDL.
ECC (Elliptic Curve Cryptography)	A widely used public-key algorithm, more efficient than RSA. Vulnerable to Shor's algorithm on a CRQC.
FTQC (Fault-Tolerant Quantum Computer)	A quantum computer with enough error correction to run long computations reliably. The hardware platform needed to break RSA-2048.
Hybrid cryptography	An interim approach that combines a classical algorithm (like ECC) with a post-quantum algorithm (like ML-KEM). An attacker must break both to compromise the data.
ML-DSA (FIPS 204)	The NIST-standardized post-quantum digital signature algorithm, formerly known as CRYSTALS-Dilithium.
ML-KEM (FIPS 203)	The NIST-standardized post-quantum key encapsulation mechanism, formerly known as CRYSTALS-Kyber. Replaces classical key exchange like ECDHE.

Term	Definition
NIST	U.S. National Institute of Standards and Technology. Ran the multi-year competition that produced the first post-quantum cryptography standards in August 2024.
PQC (Post-Quantum Cryptography)	Cryptographic algorithms designed to remain secure against both classical and quantum computers. The intended replacement for RSA and ECC in long-lifespan applications.
Q-Day	Informal term for the day a CRQC becomes operational and current public-key encryption stops being secure.
RSA	The most widely deployed public-key encryption algorithm. Vulnerable to Shor's algorithm on a CRQC.
Shor's algorithm	A quantum algorithm, published in 1994, that efficiently solves the math problems behind RSA and ECC. The reason quantum computers threaten current encryption.
SLH-DSA (FIPS 205)	A NIST-standardized post-quantum signature algorithm based on hash functions, formerly known as SPHINCS+. A backup option to ML-DSA.
SNDL (Store Now, Decrypt Later)	An alternative name for HNDL. The two acronyms describe the same threat.
Superposition	The quantum mechanical property that allows a qubit to represent multiple values simultaneously. The basis of quantum computational advantage.
Superposition	A quantum property enabling qubits to hold multiple values at once, providing the basis for quantum computational advantage.

This informational primer does not endorse specific technologies. Consult cryptographic and legal counsel for migration advice specific to your sector and jurisdiction.

PQC+™

Transformativ IP

Regulatory Compliance & HNDL Protection
Federal & all 50 States within 90 Days

www.TransformativIP.ai
Info@TransformativIP.ai