AN EXECUTIVE BRIEFING FROM TRANSFORMATIV IP

Your Worst Problem and How PQC+ Uniquely Solves it

Why Google, IBM, and Microsoft Are Telling You to Migrate Now — and Why PQC+ Is the Only 90-Day Path That Closes Your Personal Liability Gap.

Written for the CEOs, CTOs, and CISOs of mid-tier enterprises whose risk tolerance has collapsed and whose deployment window has shrunk.

The Short Version

Three things have happened simultaneously, and most boards have not connected them. First, Google, IBM, and Microsoft — the companies actually building quantum computers — have publicly converged on a 2029 "Q-Day" timeline, the moment classical RSA and ECC encryption stop protecting your data. Second, adversaries are already harvesting your encrypted data today with the explicit intent to decrypt it the moment quantum capability arrives. Third, U.S. federal and state regulators have responded by criminalizing executive inaction — not at the corporate level, but at **your** level, personally.

The intersection of these three forces is what we call **the Mother of All Regulatory Nightmares**: a world in which a single breach, three years from now, exposes criminal liability in dozens of states because the data was harvested today using cryptography you knew was failing. This briefing makes the case that the prudent, defensible response is to deploy NIST-certified post-quantum cryptography **before** the breach — and that PQC+ is the only software-based path we are aware of that can do it in 90 days, on free trialware, without rip-and-replace.

Part 1 — The Builders Have Spoken. Q-Day Is 2029.

For most of the last decade, quantum risk lived in the footnotes of cybersecurity strategy. That changed in December 2024, when Google's Willow chip **solved the underlying physics problem** of scalable quantum error correction — demonstrating, in the world's most prestigious peer-reviewed scientific journal, that adding qubits could *reduce* error rates rather than increase them. The remaining work is no longer scientific discovery. It is engineering scale. And engineering scale is precisely what the world's best-funded technology companies are organized to deliver.

What follows is not a fringe view. These are the public statements of the executives directly accountable for the hardware:

> *"Google's Willow chip completed a benchmark calculation in under five minutes that would take a leading supercomputer an estimated 10 septillion years, vastly exceeding the age of the universe."*
>
> — Sundar Pichai, CEO of Alphabet & Google — RBC Thought Leadership, December 2024

> *"As we advance quantum capabilities, we must accelerate the transition to post-quantum cryptography to ensure the world's data remains secure against future threats."*
>
> — Satya Nadella, CEO of Microsoft — Official Statement on Quantum Advancement, February 2025

> *"Quantum computing is a double-edged sword. It will solve the world's hardest problems, but it also renders RSA and ECC obsolete. Our security posture must evolve faster than the hardware."*
>
> — Charlie Bell, Executive VP of Microsoft Security — Microsoft Security Blog, February 2025

> *"The transition to quantum-safe cryptography is the largest and most complex migration in the history of computing. We are moving from a world where math was our shield to one where we need new math."*
>
> — Dario Gil, SVP and Director of IBM Research — MIT Technology Review, October 2024

> *"You have the building block in hand, almost ready to scale up to the large machines."*
>
> — Dr. Hartmut Neven, Founder & Director, Google Quantum AI Lab — on the Willow chip breakthrough

Why "2029" Is Not One Person's Guess

The 2029 date is the convergence of **five independent evidence streams**, which is what makes it analytically different from the prior quantum timelines you may have learned to dismiss:

- **Hardware acceleration.** Neven's Law describes quantum capability growing at a doubly exponential rate — a sequence of 4, 16, 256, 65,536, 4.3 billion, 18 quintillion. By the time the trajectory becomes obvious to a board, it is already too late to migrate.
- **Error correction solved.** Willow's below-threshold demonstration in *Nature* eliminated the single most critical prerequisite for a cryptographically relevant quantum computer.
- **Algorithmic optimization.** The number of qubits required to break RSA-2048 has collapsed by 99.9% in a single decade. In May 2025, Google researcher Craig Gidney showed it can be done with fewer than one million noisy qubits in under a week of compute time — a 20× reduction from his own earlier estimate.
- **Expert consensus.** Google, IBM, Microsoft, Gartner, the NSA, NIST, CISA, the Federal Reserve, and the World Economic Forum all project the 2029–2030 window.
- **Government urgency.** NIST finalized FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) in 2024. The NSA mandates quantum-safe acquisitions by January 2027. The EU mandates the transition for critical

infrastructure by 2030. Regulators do not move this fast unless classified intelligence has confirmed the risk.

> *"I prefer security to not be contingent on progress being slow."*
>
> — Craig Gidney, Google Quantum AI — arXiv preprint, May 2025

> *"The threat to our national security from quantum computing is real. Every organization must start the inventory of their vulnerable public-key systems today."*
>
> — Jen Easterly, Director of CISA — White House Cyber Policy Briefing, 2024

The takeaway for the C-suite

The physics problem is solved. The engineering race is underway. The adversaries are already harvesting your data. The regulators are already setting enforcement timelines. The personal liability framework is already in place. "Wait and see" is no longer an analytical posture — it is a documented decision that prosecutors and plaintiffs' attorneys will later read into a transcript.

Part 2 — The Breach Is Already Happening

If you remember nothing else from this briefing, remember this: **the data your adversary will decrypt in 2029 was stolen this quarter.** Nation-state actors and organized cybercriminals are running "Harvest Now, Decrypt Later" (HNDL) operations at scale right now, vacuuming up RSA- and ECC-encrypted traffic and storing it against the day the math breaks.

> *"The 'Store Now, Decrypt Later' attack is the most pressing cybersecurity threat of our time. Nations and hackers are already vacuuming up RSA-encrypted data waiting for Q-day to unlock it."*
>
> — Jack Hidary, CEO of SandboxAQ — World Economic Forum, January 2025

> *"Encrypted data remains at risk because of the 'harvest now, decrypt later' threat... starting the transition to post-quantum cryptography now is critical to preventing these future breaches."*
>
> — NIST, Transition to Post-Quantum Cryptography Standards (IR 8547), November 2024

Your Data Has an Expiration Date

Here is the calculus that should reframe every cybersecurity budget conversation you have in 2026. If your enterprise needs **X years** to migrate to PQC, and your data must remain confidential for **Y years**, then you are exposed any time a quantum computer arrives in fewer than **X + Y years**.

Apply that math to a regional hospital system or a mid-tier bank. Patient records, genomic data, M&A files, and personnel data routinely carry 30- to 50-year confidentiality requirements. Even a three-year migration window means your current cryptography has to hold for 33 to 53 years. Against a quantum capability arriving in 2029, **the records you encrypted last Tuesday are already on borrowed time.** The breach window did not start when the quantum computer is turned on. It started years ago.

Quantified financial exposure

A January 2026 report from the Citi Institute titled "Quantum Threat: The Trillion-Dollar Security Race Is On" estimates that a single-day quantum attack on a top-five U.S. bank's Fedwire access could cost the U.S. economy between $2.0 and $3.3 trillion — a 10% to 17% GDP decline. The Federal Reserve's own research paper (FEDS 2025-093) frames the HNDL threat as "present, active, and in some circumstances unavoidable."

Part 3 — Three Regulatory Storms Are Converging

Most enterprises are still organized around the assumption that healthcare compliance, AI governance, and privacy law are three separate problems handled by three separate teams. They are not. They are converging into a single, indivisible obligation — and they are converging at the level of the data itself.

1. Healthcare Data (HIPAA + 50 state overlays)

HIPAA is the federal floor. State law is the ceiling, and the ceiling now includes **imprisonment as a criminal penalty in 39 states**. Mid-tier hospitals, regional health systems, PBMs, telehealth platforms, and connected medical devices all face overlapping and sometimes conflicting state mandates.

2. AI Governance (EU AI Act + 37 U.S. states)

AI regulation arrived faster than almost any compliance team forecast. Colorado, California, New York, Texas, and 33 other states have moved to impose obligations on automated decision-making — many with criminal penalties for negligent deployment, undisclosed model use, or biased outcomes in healthcare, hiring, and finance.

3. Privacy (State Comprehensive Privacy Laws + Sectoral Statutes)

Twenty-one states now criminalize specific categories of privacy violations: unauthorized disclosure of biometric data, sale of sensitive personal information without consent, and willful failure to honor consumer rights requests. The patchwork is no longer manageable through policy alone.

What this means in plain terms

• Jurisdiction is determined not by where your headquarters is, but by where your patients or clients live. Odds are you have to comply with all 50 states' regulations.

• Fewer than five states offer a grace period for first-time offenders.

• A single breach can move from regulatory inquiry to criminal indictment, and the easiest way for a state regulator to meet a quota is to subpoena businesses already convicted in other states with similar regulations.

• Compliance can no longer be enforced at the policy layer or the perimeter layer. It must be enforced at the data layer itself — because that is the only layer that travels with the obligation.

Part 4 — The Liability Just Became Personal

This is the part of the briefing that most CTOs and CISOs find genuinely uncomfortable, and that most CEOs have not yet been briefed on by counsel. Under the U.S. Department of Justice Data Security Program (DOJ DSP), which went into effect in 2025, the legal framework is explicit: when a data breach occurs and regulators determine that leadership **was aware of an emerging threat but failed to act**, the designation shifts from negligence to "willful violation."

This briefing — along with the public statements of Pichai, Nadella, Krishna, Gil, Easterly, and NIST quoted above — is precisely the kind of "awareness" record that a federal prosecutor will use to make that designation stick.

Consequence	Detail
Personal criminal prosecution	Up to 20 years imprisonment under applicable federal statutes; up to 50 years under the most severe state regulations.
Personal civil penalties	Assessed against individual officers, not just the organization.
Uninsured defense costs	D&O insurance covers the costs of regulatory criminal proceedings. However, if you lose or accept a plea deal, the D&O insurer will claw back what they paid. You are personally on the hook for it, and it cannot be discharged in a bankruptcy. Defense costs for a single DOJ charge often exceed $1 million.
Institutional non-coverage	Employers are not obligated to cover criminal defense costs. If you accept a plea or are convicted, D&O carriers can claw back what they advanced.
Domino enforcement	A single state breach disclosure often triggers parallel investigations by other US states where affected patients or clients reside.
90%+ conviction rates	Federal conviction rates in white-collar regulatory prosecutions exceed 90%. Insufficient public data exists for the state level.
DO Insurance does not cover…	D&O insurance does not cover penalties, restitution, or private lawsuits.

The single sentence the C-suite has to internalize

Your institution may pay for the PQC solution. It will not pay for your criminal defense.

Our own polling indicates that fewer than 10% of executives are aware of the personal exposure they currently carry. The gap between those two numbers is the entire reason this briefing exists.

PQC as Your "Good Faith" Defense

The DOJ DSP framework is equally explicit on the other side of the ledger: implementing NIST-certified post-quantum cryptography is treated as a **good-faith compliance measure**. It does not guarantee immunity. It does fundamentally change how regulators and prosecutors evaluate culpability after an incident especially criminal culpability and imprisonment.

The analogy executives understand intuitively is fire suppression. Two companies suffer a fire. One installed a certified suppression system before the incident; the other did not. They face very different questions about accountability — even when the outcome of the fire is the same.

The question prosecutors and plaintiffs' attorneys are now asking is narrow and answerable:

Did the executive deploy commercially available, NIST-certified post-quantum cryptography when it became available? "We were evaluating it" is no longer a defensible answer when a 90-day deployment path exists.

Part 5 — Why PQC+ Is the Only Path That Closes Both Gaps

Every PQC vendor will tell you they implement FIPS 203 and FIPS 204. That is table stakes. What separates PQC+ from the rest of the market is the combination of three properties that, to our knowledge, no other solution delivers simultaneously:

Rapid Deployment	Certified Security	Proactive Compliance
90 days vs. the 2-year industry standard. 100% software — no rip-and-replace. No new hardware. No procurement cycle measured in fiscal years.	FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA), the NIST-finalized post-quantum standards. Tiered key strength up to 10,240-bit for data that must survive decades. Free trialware available.	Designed to satisfy the strictest jurisdiction by default — including foreign-headquartered entities selling into U.S. markets. Compliance with the strictest regime produces compliance with the rest — including the 39, 37, and 21 criminal-penalty states.

Why 90 Days, Not Two Years

The industry-standard PQC migration timeline assumes *rip-and-replace*: new hardware security modules, new endpoint agents, new key-management infrastructure, lengthy procurement, and per-application integration. PQC+ is delivered as a 100% software overlay. It does not require new hardware. It does not displace your existing cryptographic stack. It does not require a procurement cycle measured in fiscal years.

This matters more than it sounds: **every day between today and your migration completion is a day on which an adversary may be harvesting data that will be readable in 2029.** The math of HNDL does not care whether your CFO has approved the budget yet.

Why Compliance Becomes Provable, Not Asserted

PQC+ shifts protection from the network perimeter to **the data packet itself.** Every piece of regulated data — a patient record, a financial transaction, an AI model output, a consent attestation — carries its own cryptographic envelope. Inside that envelope:

- **Certified post-quantum encryption** (FIPS 203 ML-KEM, FIPS 204 ML-DSA) so the data resists both today's attacks and tomorrow's quantum decryption.
- **Embedded Identity & Privacy Access Control Lists (IP-ACLs)** that enforce who, on which hardware, under which conditions, can decrypt the data — at the moment of access, not at the moment of provisioning.
- **Dynamic consent attributes** so HIPAA, GDPR, state privacy law, and AI training-consent obligations are enforced by the data itself, not by a downstream system that may or may not honor them.
- **Hardware-bound keys** so a stolen password — or even a stolen database — is mathematically useless without the specific authorized device.

In practical terms: when a regulator or prosecutor asks whether your enterprise *prevented* unauthorized access — not whether you intended to, not whether you had a policy that *said* you would, but whether you **mathematically prevented it** — PQC+ produces a cryptographic record that answers the question.

This is the "Holy Grail" shift

Traditional security defends the "pipes" — the networks. PQC+ secures the "water" — the data itself. Once the data is its own self-protecting vault, a breach of the perimeter is no longer the same kind of event. A stolen database becomes millions of individual, quantum-locked files with zero resale value on the dark web. Identity is devalued because keys are hardware-defined. Consent is enforceable because it is cryptographically baked in. The economic model that has driven 20 years of data breaches is, for the first time, no longer appealing to cybercriminals.

Tiered Strength for the Data You Actually Have

Tier	Key Size (Bits)	Intended Protection Level
Commercial	1,024	Standard business operations.
Military	2,048	Sensitive defense and mission-critical data.
Intelligence	5,120	Highly classified intelligence.
Max Strength	10,240	Designed to protect sensitive data for decades — the answer for healthcare genomic records, oil & gas geological data, and any long-tail confidentiality obligation.

Part 6 — The Decision in Front of You

The window is open. It will not stay open. Three things follow from this briefing for any CEO, CTO, or CISO reading it:

1. Document what you did before the breach

The personal liability framework is **retrospective**. Prosecutors will look at what you knew, when you knew it, and what you did about it. The single most powerful evidence in your favor is a documented, dated record of evaluation and deployment of NIST-certified post-quantum cryptography.

2. Treat the 50-state patchwork as a single problem

PQC+ is engineered to satisfy the strictest jurisdiction by default. Compliance with the strictest regime produces compliance with the rest — including the criminal-penalty regimes in the 39 states for healthcare data, the 37 states for AI regulation, and the 21 states for privacy.

3. Use the free trial to establish institutional knowledge

PQC+ offers free trialware. This is not a procurement tactic. It is a **governance tactic.** A documented evaluation, conducted in advance of a board meeting or an audit, is precisely the diligence that distinguishes a defensible executive from a personally liable one. It costs you nothing. It produces a dated artifact that lives in your compliance file.

> *"I think the undeniable reality of this progress puts the ball firmly in the court of those who believe scalable quantum computing can't work. They're the ones who need to articulate where and why the progress will stop."*
>
> — Scott Aaronson, Professor of Computer Science, University of Texas at Austin

The Bottom Line

The regulatory environment has criminalized inaction. The cryptographic environment has shortened the half-life of "good enough." PQC+ is the only path we are aware of that closes both gaps in 90 days, on certified standards, with a documented trail that protects both the enterprise and the individuals who lead it.

The organization that starts its PQC+ migration in 2026 will complete it before the end of the next quarter, well before 2029. The organization that waits for 2028 will be migrating under emergency conditions, at emergency costs, with emergency consequences. Every day of delay is a day of harvested data, of accumulated regulatory exposure, and of personal liability that compounds — not from what you did, but from what you did not do in time.

Next Step — Two Documents, One Trial, No Obligation

Request the materials below. Both are designed to support a single, defensible board-level conversation:

- **The 16-page state-by-state compliance PDF,** documenting the actual levied criminal and civil penalties in all 50 states and at the federal level, with third-party-verifiable Google AI search results saved for 18 months.
- **The 7-page legal synopsis on DOJ sentencing,** including the three-variable formula DOJ attorneys use to calculate sentencing severity — a formula that directly compares your cybersecurity spend to your sales-and-marketing spend.
- **A no-obligation PQC+ trial,** demonstrating 90-day deployment in your environment, on your data, against your existing infrastructure — with no hardware procurement and no rip-and-replace.

Start the 90-day clock today.

Request the compliance dossier and the PQC+ free trial.

Info@TransformativIP.ai • www.TransformativIP.ai

