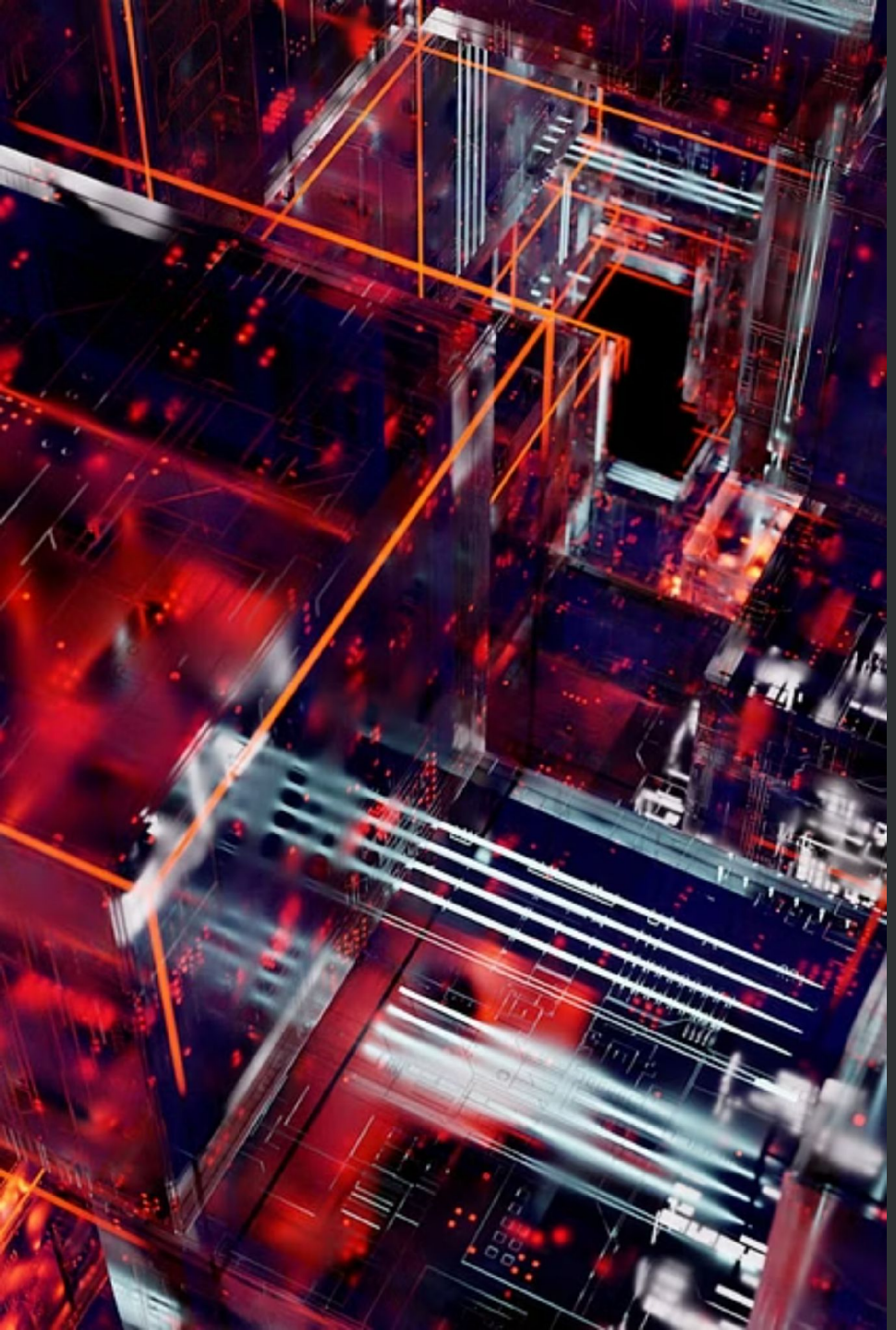


Beyond Algorithms: The Age of Agentic Intelligence and Quantum Disruption

Presenter: Ellis Wong, Head of Infrastructure Engineering and Chief Information Security Officer, JST Capital

Event: Chief AI Officer Summit — New York | June 9, 2026 | 1:30–2:00 PM ET

About Me

20+ years leading global Engineering and Security organizations

Career began building PKI and cryptographic solutions for networking & telecom equipment

9+ years as CISO and Head of Product Security

20+ years in Data and AI

Member, AI-Native Quantum Computing Academy

Member, AI Security Council

A Tuesday Morning in 2031

The Scenario

A trading firm wakes up to news that a sealed-bid M&A archive from 2026 has been retroactively decrypted.

The Cryptography

The cryptography was state-of-the-art. The data was encrypted.

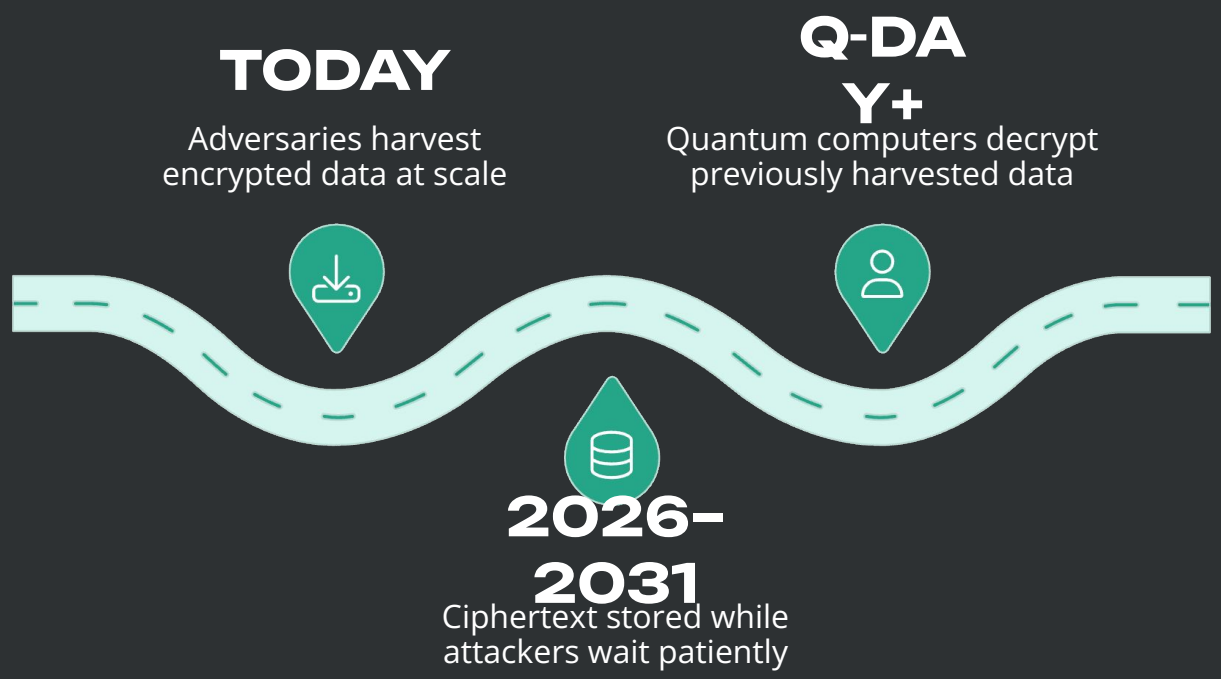
The Breach

The breach was not the failure of encryption. It was the **success of patience**.

"If a cryptographically relevant quantum computer emerged in 2031 — what would we wish we had done differently in 2026? And are we doing those things now?"

HARVEST NOW · DECRYPT LATER

The Adversary Does Not Need to Break Encryption Today



Who Treats HNDL as a Present-Day Risk

Storage is cheap. Patience is free. The payoff is asymmetric.

NSA/OMB
Memorandum M-23-02

Federal Reserve
FEDS 2025-093

BIS
Project Leap Phase 2

NCSC/GCHQ
Active advisory

G7 Cyber Expert Group
Critical finance focus

Sources: NSA M-23-02 · Federal Reserve FEDS 2025-093 (Dec 2025) · BIS Project Leap Phase 2 (Jun 2025) · NCSC advisory

CONVERGENCE

Two Transitions. One Five-Year Window

Agentic AI Timeline

2024
Multi-agent frameworks in production

2025
80%+ of enterprises testing or running agents

2026
Autonomous trading, risk & compliance agent pipelines

2028+
Agent networks with full delegated autonomy at scale

Quantum Hardware Timeline

Aug 2024
NIST FIPS 203–205 published

May 2025
Gidney: RSA-2048 breakable with <1M qubits — 20× reduction

Jan 2027
CNSA 2.0 procurement gate — binding for US supply chains

2029
IBM Starling: 200 logical qubits (publicly committed roadmap)

Sources: Gidney, Google Quantum AI (May 2025) · NIST FIPS 203–205 (Aug 2024) · IBM Quantum roadmap · GRI Quantum Threat Timeline (Mar 2026)

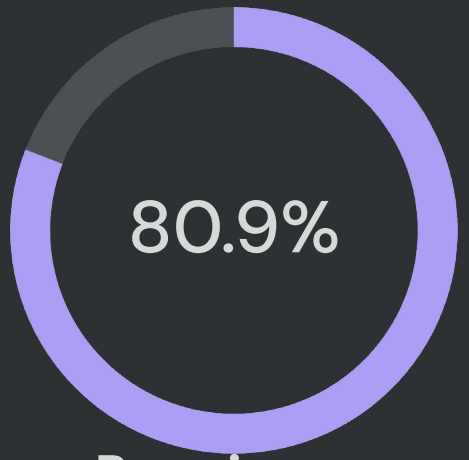
PART I

The Automated Enterprise and Its Unguarded Doors

How agentic AI is transforming organizations — and what that means for your attack surface

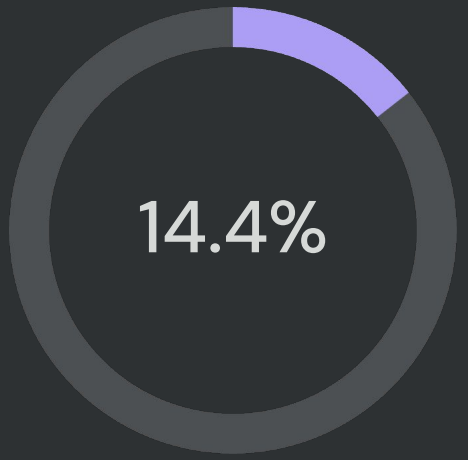
PART I · AGENTIC AI TODAY

Agentic AI Is Not the Future. It Is the Present.



Running or Testing

Agentic AI systems in production or evaluation



Full Approval

Went live with full security and IT approval

Exposed MCP Servers

Publicly exposed as of Feb 2026

Sources: Trend Micro (Feb 2026) · CSA / Strata Identity Survey (2025) · Cyata CVE-2025-68143/144/145

We Treat Human Identities Rigorously. Agent Identities, We Don't.

Human Identity — What We Do

- MFA + Hardware Token
- Scoped Access
- Full Audit Trail
- Cert-Based Auth
- IAM Provisioning

Agent Identity Today — What We Actually Do

- Shared API Keys
- Inherited Permissions
- No Audit Logging
- Unsigned Tool Calls
- No Provisioning

Source: CSA / Strata Identity Survey, 2025 · OpenClaw incident: 1,184 malicious skills published into a public agent ecosystem

PART I · BLAST RADIUS

A Single Compromised Primitive Poisons the Entire Agent Network

- Data Feed
- Research Agent
- Execution Agent
- Risk & Compliance

Supply Chain: Prompt Injection → RCE

OpenClaw Incident
1,184 malicious skills

Cyata CVE-2025-68143
RCE via prompt injection

The Post-Quantum Multiplier

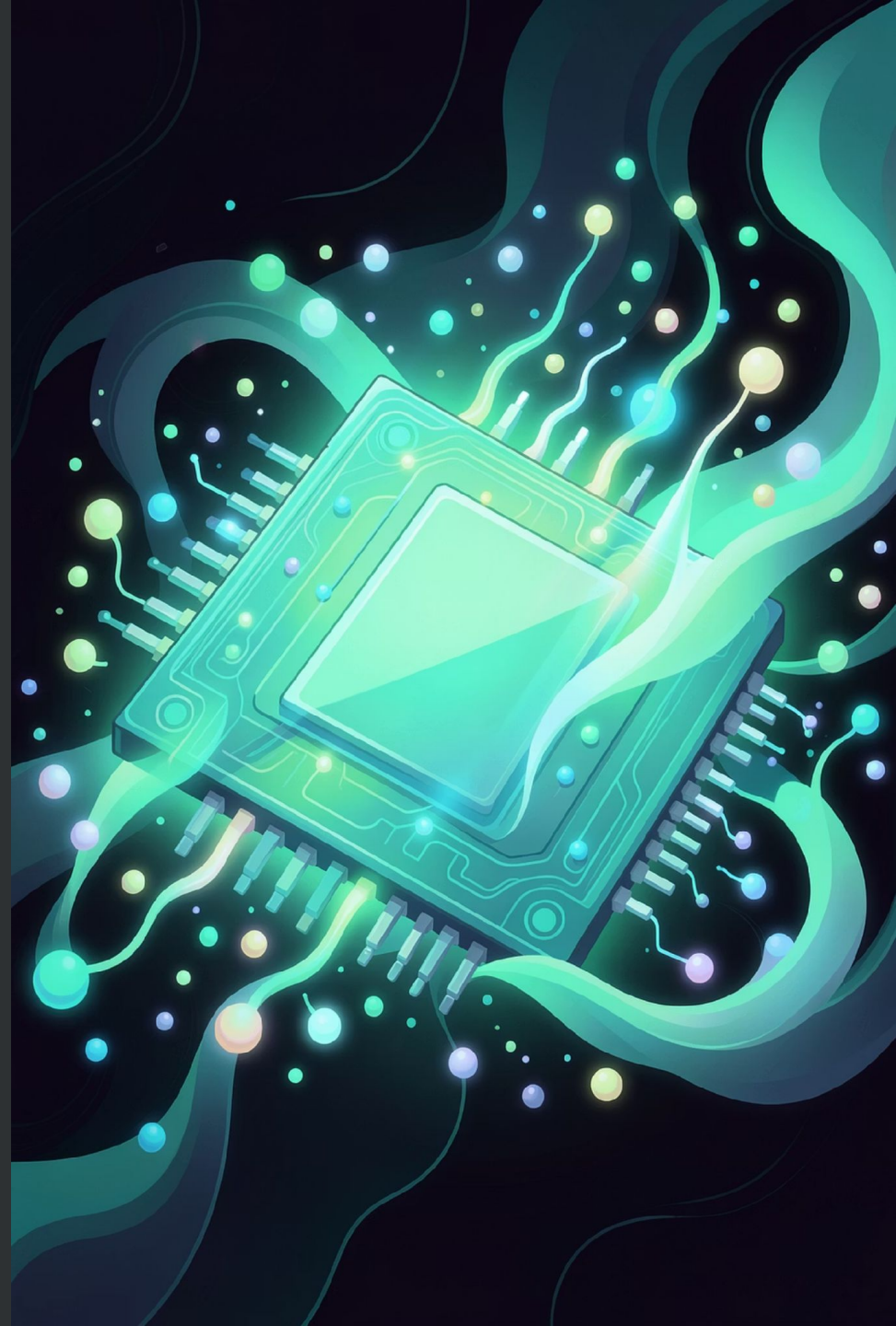
The agents don't protect each other. The cryptography does — and it's on a depreciation schedule.

Sources: Cyata CVE-2025-68143/144/145 · OpenClaw incident, 2026 · Trend Micro MCP exposure analysis (Feb 2026)

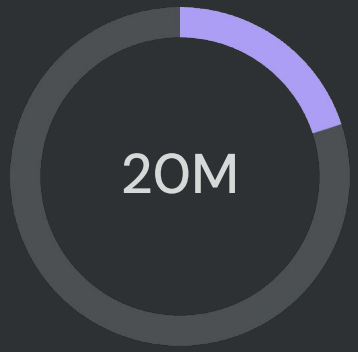
PART II

The Quantum Inflection Point

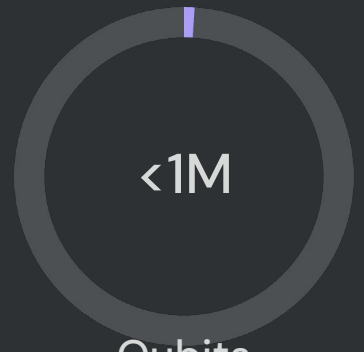
Why the engineering trajectory has changed the planning calculus — even before Q-Day arrives



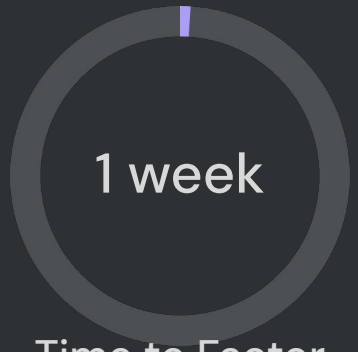
The Cost of Breaking RSA-2048 Has Dropped 20× in Five Years



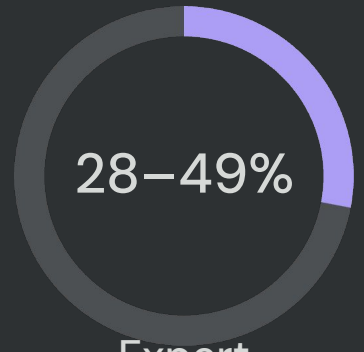
Qubits (2019)



Qubits Needed Now



Time to Factor RSA-2048



Expert Probability

Sources: Gidney, Google Quantum AI (May 2025) · Gidney & Ekerå (2019) · Global Risk Institute Quantum Threat Timeline (Mar 2026, authors: Mosca & Piani)

PART II · COMPLIANCE

The Compliance Path Arrives Before the Quantum Threat Does

Aug 2024
NIST FIPS 203–205

2028
UK NCSC Phase 1

2030–2032
G7 Critical Infrastructure Migration

Jan 2027
CNSA 2.0 Gate

2030
EU & Australia

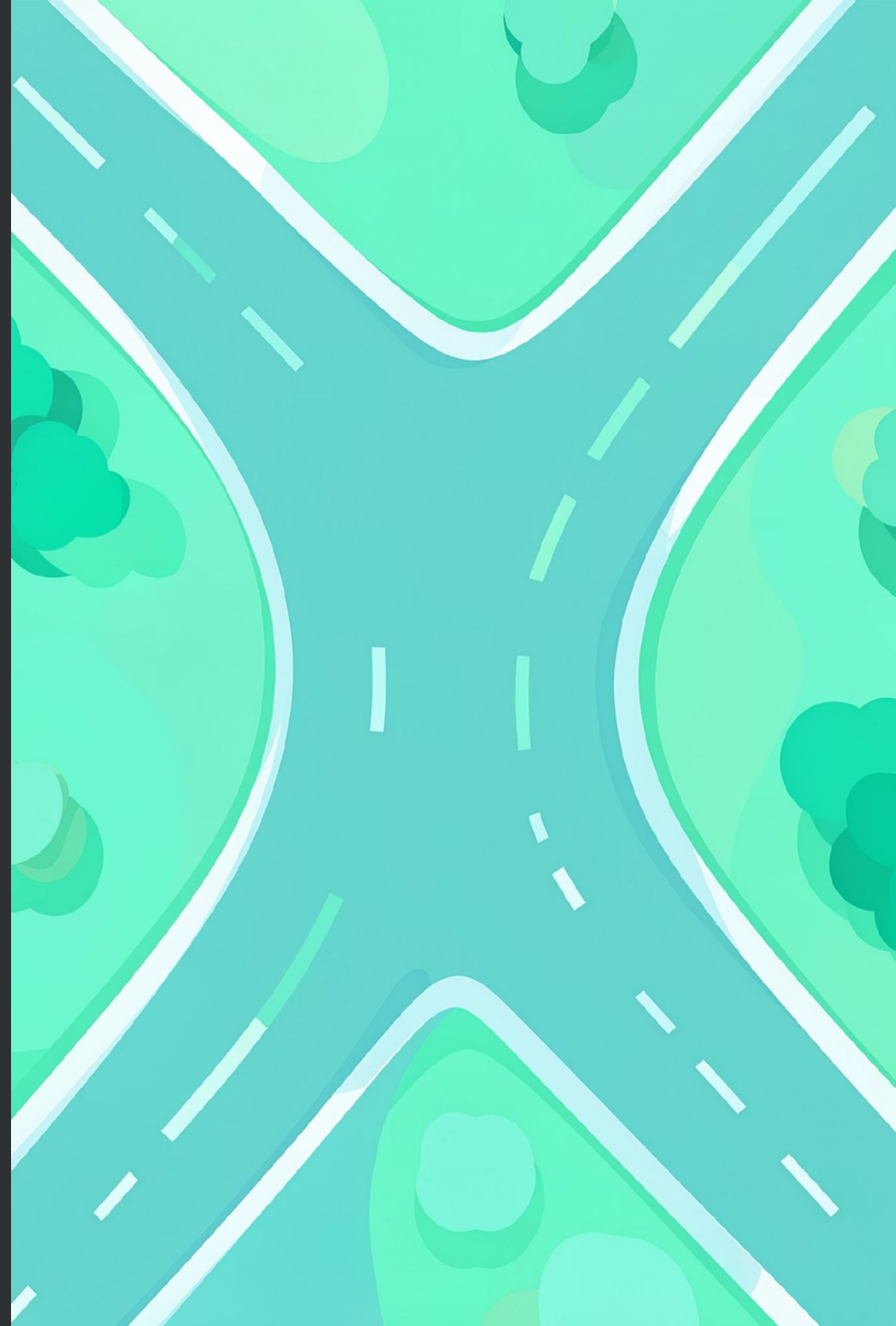
2035
Full Phase-Out

Sources: NIST FIPS 203–205 (Aug 13, 2024) · NSA CNSA 2.0 · UK NCSC Phase 1 guidance · EU NIS2 / DORA · ASD post-quantum advisory · G7 Cyber Expert Group

PART III

The Intersection

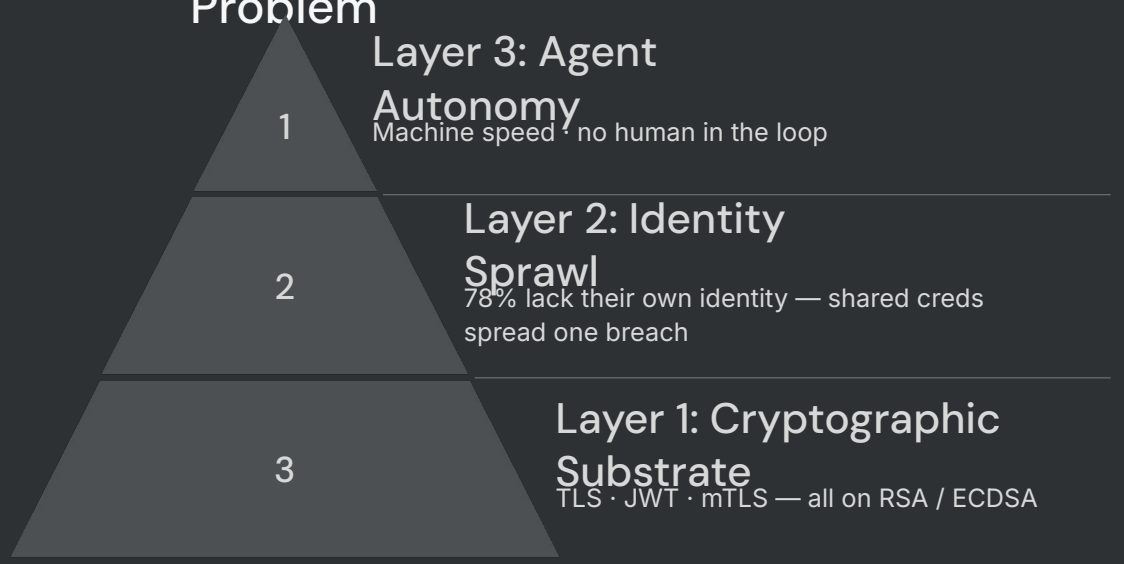
Where agentic AI and quantum disruption converge — and what the path forward looks like



PART III · CONVERGENCE

The Security Ceiling of Your Agent Network Is the Cryptography Underneath It

The Layered Problem



What a Quantum-Safe Stack Needs

- ☐ PQC-capable trust roots and model provenance
- ☐ Independent agent identities
- ☐ Crypto-agility (swap algorithms)
- ☐ Cryptographic bill of materials (CBOM)

Sources: CSA / Strata Identity Survey (2025) · BIS Project Leap Phase 2 (Jun 2025) · NSA CNSA 2.0

PART III · START PQC MIGRATION

Pilot Hybrid PQC Migration — No Need To Wait

What is Hybrid PQC?

Classical X25519
Elliptic-curve key exchange

Post-Quantum ML-KEM
Lattice-based (Kyber)

▼

Hybrid Key Exchange
Secure if EITHER holds

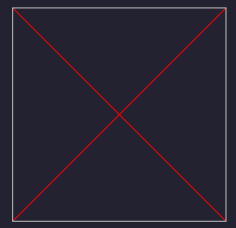
Production-Ready PQC Tools & Libraries

- KeyFactor
- oqs-provider (OpenSSL 3)
- BouncyCastle
- CIRCL · Cloudflare
- pyca/cryptography

Live in TLS & Protocols Today

- TLS 1.3 Hybrid
- Chrome 124+
- AWS KMS / ACM
- OpenSSL 3.5+
- OpenSSH 9+

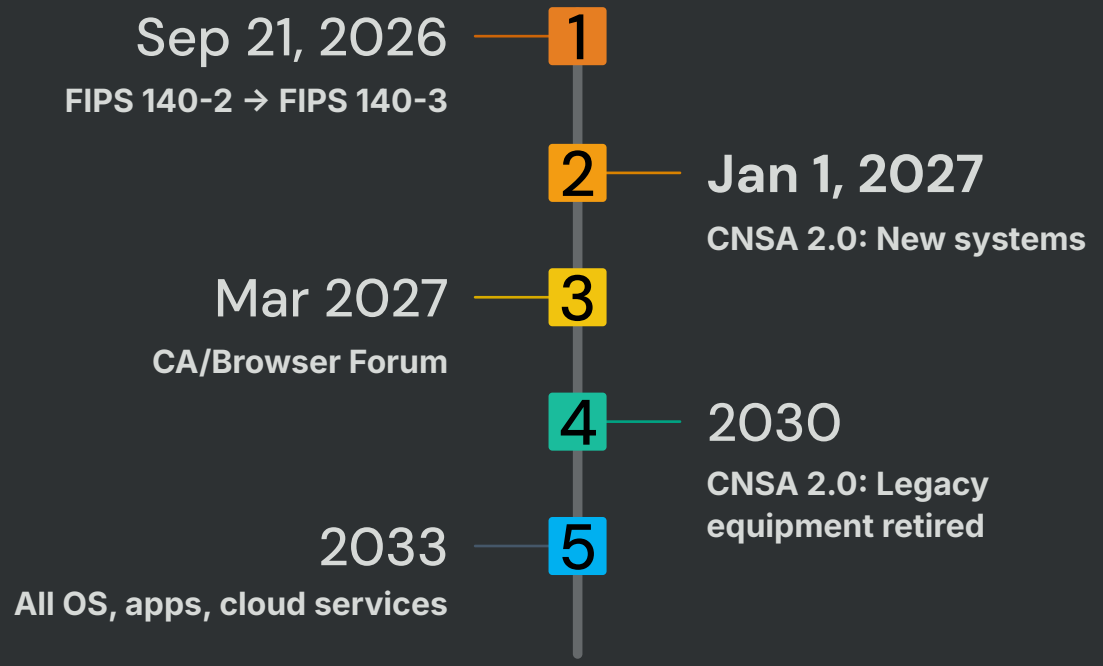
Compliance/Compliance Deadlines Driving PQC Migration Timeline



The clock is already running.

Mandates land before quantum computers do — migration windows are measured in months, not years.

Why Act Now? Key Dates



PART III · INDUSTRY PATHWAYS

Industry Pathways: Where Quantum Value Is Emerging First

Now	2026–28	2027–29	2028–35
Cybersecurity *PQC migration urgency*	Finance & Logistics *Optimization economics*	Telecommunications *Network efficiency*	Healthcare & Life Science Energy & Sustainability

Source: Quantum, AI & Reallocation of Capital Panel (May 27, 2026) · Panelists: Christopher Monroe (IonQ), Bharath Kannan (Quantum@Google), Yudong Cao (Zapata Quantum), Garfield Jones (QuSecure, Ex-DHS), Anthony Lawrence (Light Rider, Ex-NSA), Andrew Hammond (Quantum Answers), Amirhossein Ghods (Mesa Quantum)

CLOSE · ACTION PLAN

The 90-Day List. The Decisions That Separate Ready From Exposed

THIS WEEK

01 Appoint Owner

02 Classify Data

30–60 DAYS

03 Crypto Inventory

04 Agent Identity

60–90 DAYS

05 Vendor Gates

06 PQC Pilot

CLOSE · CALL TO ACTION

The answer to what we wish we had done differently in 2026 — is exactly what we can still do today.

The harvest is already underway. The standards are written. The only variable left is you.

Q & A

Do you have any questions for me?

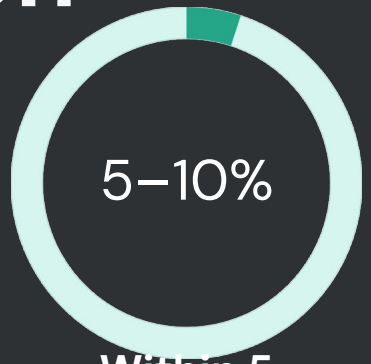
Ellis Wong
Entrepreneurial Technology and InfoSec Executive | MBA | CISSP

APPENDIX

Appendix

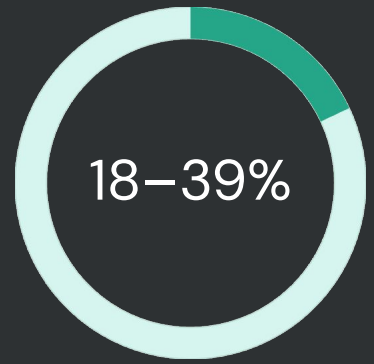
Backup detail and reference material — for Q&A support, not part of the main keynote flow

CRQC Timeline: Uncertain on Date, Certain on Direction



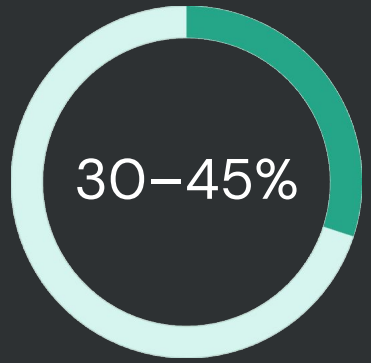
Within 5 Years

Low but non-negligible near-term probability



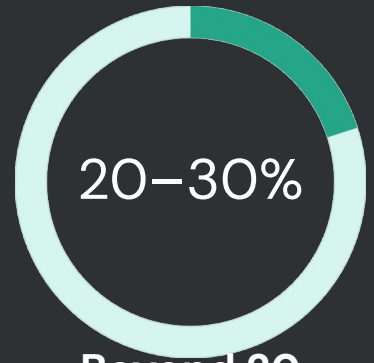
5–10 Years

The primary planning window for most institutions



10–20 Years

Consensus central estimate range



Beyond 20 Years

Long-tail scenario — but migration runway still applies

Source: Global Risk Institute, Quantum Threat Timeline Report (Mar 2026, authors: Mosca & Piani) · 7th consecutive year of expert surveying

BACKUP · WHAT ARE THE STANDARDS?

NIST PQC Standards: What Was Standardized and Why It Matters

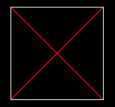
HIGH PRIORITY — MIGRATE FIRST

FIPS 203

HIGH

ML-KEM (CRYSTALS-Kyber)

Key Encapsulation · Lattice (MLWE)



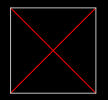
FIPS 204

HIGH

ML-DSA (CRYSTALS-Dilithium)

Digital Signatures · Lattice (MLWE/SIS)

MEDIUM PRIORITY & MONITOR

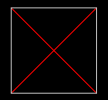


FIPS 205

MEDIUM

SLH-DSA (SPHINCS+)

Hash-Based Sig. · Hash functions

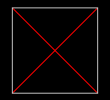


FIPS 206

MEDIUM

FN-DSA (FALCON)

Compact Sig. · NTRU Lattice



HQC (TBD)

MONITOR

Hamming Quasi-Cyclic

Backup KEM · Code-based

Published Aug 13, 2024. FIPS 206 finalized Aug 2025. HQC selected Mar 2025. **Migration can begin now — standards are final.**

Source: NIST PQC Standardization Process, 2024–2025 · FIPS 203/204/205 (Aug 13, 2024) · FIPS 206 (Aug 2025) · HQC selection (Mar 11, 2025)

BACKUP · WHAT IS CRYPO-AGILITY?

Crypto-Agility: The Architecture Property That Determines Survival Cost

> Crypto-agility = the ability to swap cryptographic algorithms, key sizes, and protocols **without invasive application rewrites.**

Cryptographic Abstraction Layer

Applications call a crypto API, not specific algorithm implementations

Centralized KMS / Certificate Lifecycle

Single control plane; supports hybrid classical+PQC during transition

Cryptographic Bill of Materials

Inventory every primitive in every system. EU Cyber Resilience Act: legally required by Dec 2027

Hybrid Mode Support

Run classical + PQC simultaneously (X25519+ML-KEM). Already shipping: Chrome, OpenSSH, Apple iMessage

Sources: NCSC, BSI, ENISA hybrid mode guidance · EU Cyber Resilience Act (Dec 2027) · Chrome/OpenSSH/iMessage implementations

BACKUP · DIGITAL ASSETS / RWA

Quantum-Safe Blockchains: A Uniquely Irreversible Exposure Profile

#1

XRP Ledger

Most Advanced

90% ready

ML-DSA on AlphaNet; four-phase plan targeting full quantum resistance by 2028

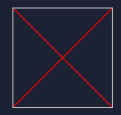
#2

Bitcoin Cash

Live · May 2026

85% ready

Layla Upgrade: Quantumroot PQ wallet storage (OPTN Labs, Paytaca). x402 protocol enables AI agent micropayments; 100–1,000× cheaper than EVM with PQ-signatures



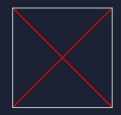
#3

Bitcoin

Merged · Feb 2026

65% ready

BIP-360; P2MR conceals public keys until spend. BTQ testnet v0.3.0 live Mar 2026



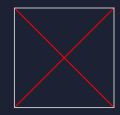
#4

Ethereum

Strawmap · 2026

45% ready

Glamsterdam + Hegoá forks 2026; ZK rollups migrating to STARK/FRI



#5

Solana

In Development

35% ready

Dual Ed25519+Dilithium keypairs; Firedancer client supports multi-signature backends

Sources: Federal Reserve FEDS 2025-093 · BIP-360 (Feb 2026) · Buterin Strawmap (Feb 2026) · XRP Ledger AlphaNet · The Quantum Insider (May 26, 2026) — BCH Layla Upgrade / Quantumroot

Quantum Ecosystem Hardware Architecture Diversity

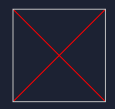
Four active hardware paradigms — not a winner-take-all race:

Superconducting

IBM · Google

✓ **Fastest gate speeds, highest qubit counts**

– Short coherence; needs near absolute zero



Trapped-Ion

IonQ · Quantinuum

✓ **Best coherence, highest gate fidelity**

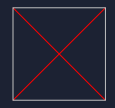
– Slower gate speeds; scaling complexity

Photonic

PsiQuantum · Xanadu

✓ **Room temperature; telecom compatible**

– Low gate efficiency; specialized use



Neutral Atom

QuEra · Pasqal

✓ **Large qubit arrays; flexible connectivity**

– Still early; calibration complexity

Most systems remain in the NISQ era. Quantum-as-a-Service (QaaS) enables experimentation without hardware ownership — **lowering enterprise entry barriers significantly.**

BACKUP · STRATEGIC PLANNING

Three Strategic Scenarios for 2026–2030: Plan Against All Three

P: MED | I: HIGH | 2029–31

Scenario A — Slow Migration / Fast Adversary

Medium probability, High impact. PQC migration at average 5–7 year enterprise pace. A retrospective-decryption incident in 2029–2031 forces emergency regulatory action. Firms with inventories demonstrate due diligence; firms without face enforcement.

YOUR MOVE

Build a crypto inventory now to prove due diligence

P: HIGH | I: MED | 2027–29

Scenario B — Regulator-Forced Migration

High probability, Medium impact. Regulators harden advisory framing into binding requirements 2027–2029. CNSA 2.0 gates cascade through supply chains. DORA, FCA/PRA require cryptographic inventory. **Dominant near-term driver.**

YOUR MOVE

Map CNSA 2.0 / DORA gaps before mandates bind

P: LOW–MED | I: HIGH | 2028–29

Scenario C — Quantum Optimization Edge Arrives Early

Low–Medium probability, High impact. Portfolio rebalancing or execution routing sees credible production quantum advantage in 2028–2029. Early adopters extract alpha; laggards face 12–18 month catch-up in a talent-scarce domain.

YOUR MOVE

Run a quantum-advantage pilot to avoid catch-up

ⓘ All three scenarios reward action in 2026.

Source: Helios Strategic Insights scenario analysis, May 2026

BACKUP · WHAT ABOUT QML?

Quantum Machine Learning: Separating Evidence from Marketing

HYPE — Unsupported Claims

25–45% fraud detection gain from QML

HYPE

Not reproduced under realistic noise. 2024 systematic review: only 16 of 4,915 papers met rigorous standards.

QML delivers hedge-fund alpha by 2028

HYPE

No peer-reviewed evidence; most claimed advantages were later dequantized by classical algorithms.

REAL — Evidence-Backed

Quantum advantage learning physical-system properties

REAL · NARROW

Huang et al. 2024: exponentially fewer queries for quantum systems. Verified — but does NOT extend to financial ML.

Google 'quantum echoes' (Oct 2025): molecular structure

REAL · SPECIFIC

Nature peer-reviewed. Genuine advantage for quantum chemistry — not a finance application.

Sources: 2024 systematic review (4,915 papers, Cornell/MIT Tech Review) · Huang et al., 2024 · Google "quantum echoes," Nature (Oct 2025) · McMahon, MIT Technology Review, 2025

BACKUP · FULL ACTION PLAN

Full Quantum-Readiness Action Checklist — Sequenced by Horizon

NOW — 90 DAYS

- [ ] Single accountable owner appointed (CISO + CDO + CTO co-sponsors)
- [ ] Cryptographic inventory: apps, infra, HSMs, KMS, SaaS, code-signing
- [ ] Data classified by confidentiality lifetime; >10yr RSA/ECC flagged
- [ ] Agent identity program: independent ID + scoped auth per agent

12 – 18 MONTHS

- [ ] CBOM published; vendor PQC-roadmap disclosure at contract renewal
- [ ] Hybrid PQC TLS pilot on non-critical workload: latency, throughput, cert-size
- [ ] Digital asset custody validated vs quantum-safe migration milestones

18 – 36 MONTHS

- [ ] Code-signing migrated to ML-DSA / SLH-DSA or hybrid
- [ ] High-priority TLS endpoints on hybrid PQC; FIPS 140-2 deprecated
- [ ] Quantum-inspired optimization pilot: rebalancing, execution, risk sim
- [ ] Quantum readiness established as quarterly board KPI

Completing the first 90-day actions places your organization ahead of a vast majority of financial firms globally.

Source: Helios Strategic Insights, May 2026 · JST Capital PQC Evaluation Report (Ellis Wong, May 28, 2026)

BACKUP · ECOSYSTEM REALITY

The Quantum Ecosystem Is a Multi-Layer Hybrid Infrastructure

Real-world System Integration over Qubit Counts

- Quantum Core
- Enterprise Systems
- Cloud & HPC
- Operations

Value comes from embedding quantum into real-world workflows — not raw qubit counts.

1. **Layer 5: AI Orchestration**
   Strategic intelligence layer routing workloads
2. **Layer 4: Software Abstraction**
   (largest commercialization bottleneck)
3. **Layer 3: Classical Foundation**
   Cloud, HPC, GPUs, AI Accelerators
4. **Layer 2: Cloud Access**
   IBM Q, AWS, Azure Quantum, IonQ
5. **Layer 1: Quantum Hardware**
   Superconducting, Trapped-ion, Photonic, Neutral-atom

Source: Quantum Computing Ecosystem Webinar (May 21, 2026) · Panelists: QEC Labs, Qubits Ventures, SuperQ Quantum, Quantum.Tech · Moderated by INTLDA

BACKUP · IN PRACTICE — VENDOR SPOTLIGHT

AI-Native Orchestration: The Strategic Intelligence Layer

What AI Does in the Hybrid Ecosystem Today

- **Optimizes & calibrates quantum circuits**
- **Routes workloads — quantum · classical · GPU**
- **Adapts hybrid workflows from feedback**
- **Abstracts quantum complexity from users**

Live Example — SuperQ Quantum

Multi-agent autonomous AI platform integrating:

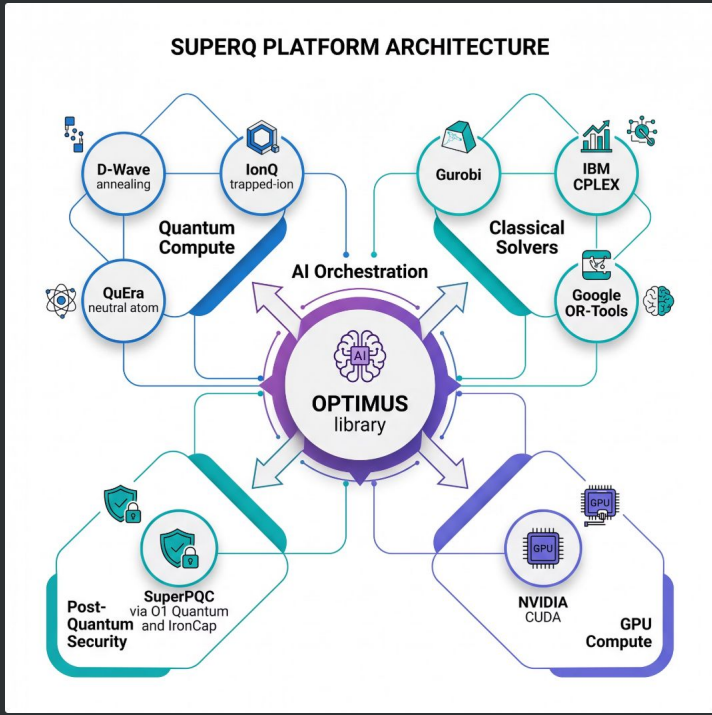
- **Quantum: D-Wave · IonQ · QuEra**
- **Classical: Gurobi · CPLEX · OR-Tools**
- **GPU compute: NVIDIA CUDA**
- **SuperPQC: post-quantum crypto AI**

"Competitive advantage depends not on any single technology, but on how effectively organizations coordinate multiple technologies into operational systems."

BACKUP · IN PRACTICE — VENDOR SPOTLIGHT

SuperQ: A Live Multi-Agent Quantum-Classical-PQC Platform

SuperQ Quantum Computing — "The Gateway to Commercial Quantum Computing"



Why This Matters

One of the only live commercial platforms bridging quantum optimization and post-quantum cryptography within a single agentic orchestration architecture.

- Demonstrates that the hybrid intelligence model described in this talk is **operational today** — not a 2029 roadmap.

Quantum Compute	Classical Solvers	GPU Compute	Post-Quantum Security
D-Wave (annealing) · IonQ (trapped-ion) · QuEra (neutral atom)	Gurobi · IBM CPLEX · Google OR-Tools	NVIDIA CUDA	SuperPQC via 01 Quantum and IronCap

Source: SuperQ Quantum Computing Inc. (www.superq.co) · Quantum Computing Ecosystem Webinar, May 21, 2026 (Alex G. Lee Ph.D. Esq., Executive Director, AI-Native Quantum Computing Academy)

BACKUP · VENDOR SPOTLIGHT

Quantum-Ready AI Infrastructure with Zero Plaintext Exposure using FHE

Run AI on Encrypted Data

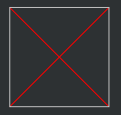
Process encrypted data without exposing plaintext.

Secure Enterprise Collaboration

Share and compute on sensitive data privately.

Eliminate Key Exposure

Keep data encrypted instead of decrypting it.



Critical for Regulated Industries

Built for high-confidentiality, high-HNDL sectors.

Enabling enterprises to deploy AI on sensitive data without compromising privacy or compliance.

Performance vs Cost Tradeoffs

Llama3.1 8B, FP16 precision, Total context and max. output is 16.4K tokens	Encrypted computing on GPU (Nvidia A100) CipherSonic AI	Non-encrypted computing on GPU (Nvidia A100)	Confidential computing on GPU (Nvidia H100)	Confidential computing on CPU (Nvidia A100)
Latency	0.53 s	0.49 s	0.44 s	0.54 s
Throughput	71 t/s	71.43 t/s	80 t/s	68 t/s
Input cost#	$0.02 per Mt	$0.02 per Mt	$0.8 per Mt	$0.021 per Mt
Output cost#	$0.03 per Mt	$0.03 per Mt	$1 per Mt	$0.031 per Mt
Security mechanism	Encrypted Computing	Non-encrypted Computing	Non-encrypted Computing*	Non-encrypted Computing*

#Inference cost to run model

*Protects only input/output, not the GPU memory

CipherSonic

BACKUP · PQC Cipher Performance

PQC Cipher Suite Evaluation: Kyber Scheme — KeyGen, Encrypt, Decrypt

NIST FIPS 203 (ML-KEM / CRYSTALS-Kyber) parameter sets — Key operations: **KeyGen · KEM Encaps (Encrypt) · KEM Decaps (Decrypt)**

Parameter Set	Security Level	Kyber Public Key	Kyber Private Key	AES Key	RSA Public Key	RSA Private Key
ML-KEM-512	Level 1 (~AES-128, RSA-2048)	800B	1,632B	16B	256B	1,216B
ML-KEM-768	Level 3 (~AES-192, RSA-7680)	1,184B	2,400B	24B	960B	4,512B
ML-KEM-1024	Level 5 (~AES-256, RSA-15360)	1,568B	3,168B	**32B**	1,920B	9,024B

Source: NIST FIPS 203, Aug 13, 2024 · JST Capital PQC Evaluation Report (Ellis Wong)