WHITEPAPER | ELITE EDITION

The 2035 Breakpoint

AI, Cryptographic Collapse, and the End of Voluntary Security Models

How Boards, Regulators, and CISOs Navigate Post-Quantum Risk

A Strategic Intelligence Briefing with Original Research

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services | AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | February 2026

Document Reference: BRE14142026 | Classification: Public Distribution — Attribution Required

Table of Contents

Table of Contents

Executive Summary

THE BOARD-LEVEL INTELLIGENCE BRIEFING

The world's cryptographic infrastructure has an expiration date.

$12.4 Trillion Exposed | 72% AI Attack Surge | 97% Unprepared

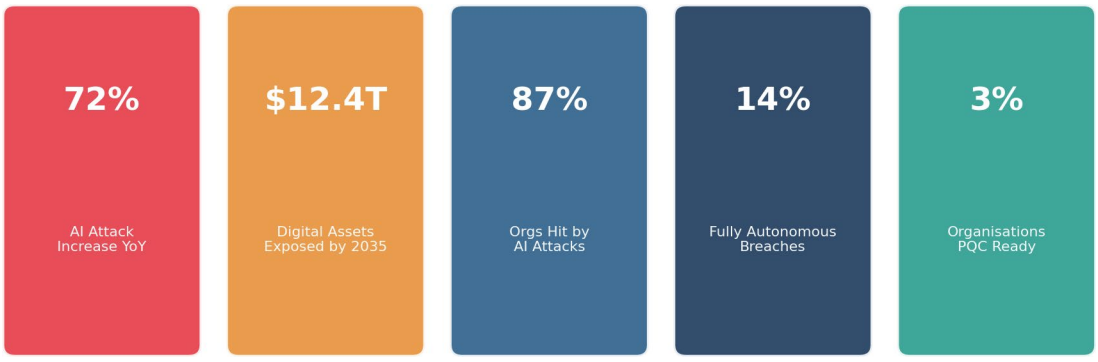
Evidence-based analysis across 100+ primary sources, current to February 2026

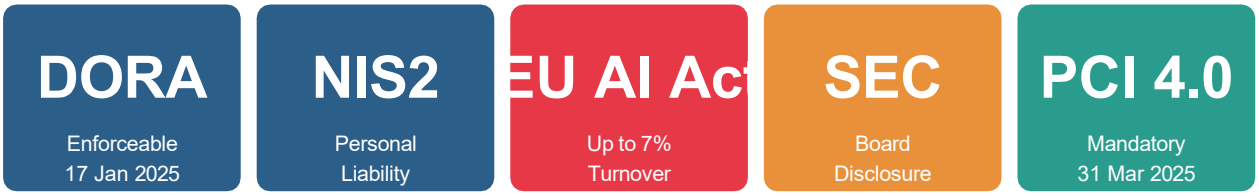
By 2035, the convergence of cryptographically relevant quantum computers, AI-driven autonomous threats, and the global shift from voluntary to mandatory security frameworks will create a category of systemic risk that no sector — least of all financial services — can afford to ignore. This whitepaper presents the thesis that 2035 represents not a distant planning horizon but an **active risk window that opened the moment nation-states began harvesting encrypted data** for future quantum decryption.

Three forces are converging simultaneously. First, NIST finalised the world's first post-quantum cryptographic standards on **13 August 2024** (FIPS 203, 204, 205), triggering a migration clock that the NSA mandates must reach completion by 2035. Second, AI-driven cyberattacks increased **72% year-over-year** in 2025, with **87% of organisations** experiencing AI-powered intrusions and **14% of major corporate breaches** executed entirely autonomously. Third, DORA became enforceable on 17 January 2025, NIS2 transposition has triggered infringement proceedings against 19 EU member states, and the EU AI Act's prohibition regime took effect on 2 February 2025.

KEY FINDING: THE 2035 CONVERGENCE

The Hudson Institute projects that a quantum-enabled attack on a single RTGS system could trigger a 10–17% GDP decline, producing $2.0–$3.3 trillion in indirect losses. Meanwhile, $12.4 trillion in global digital assets sit exposed by 2035 (Synergy Quantum, January 2026).

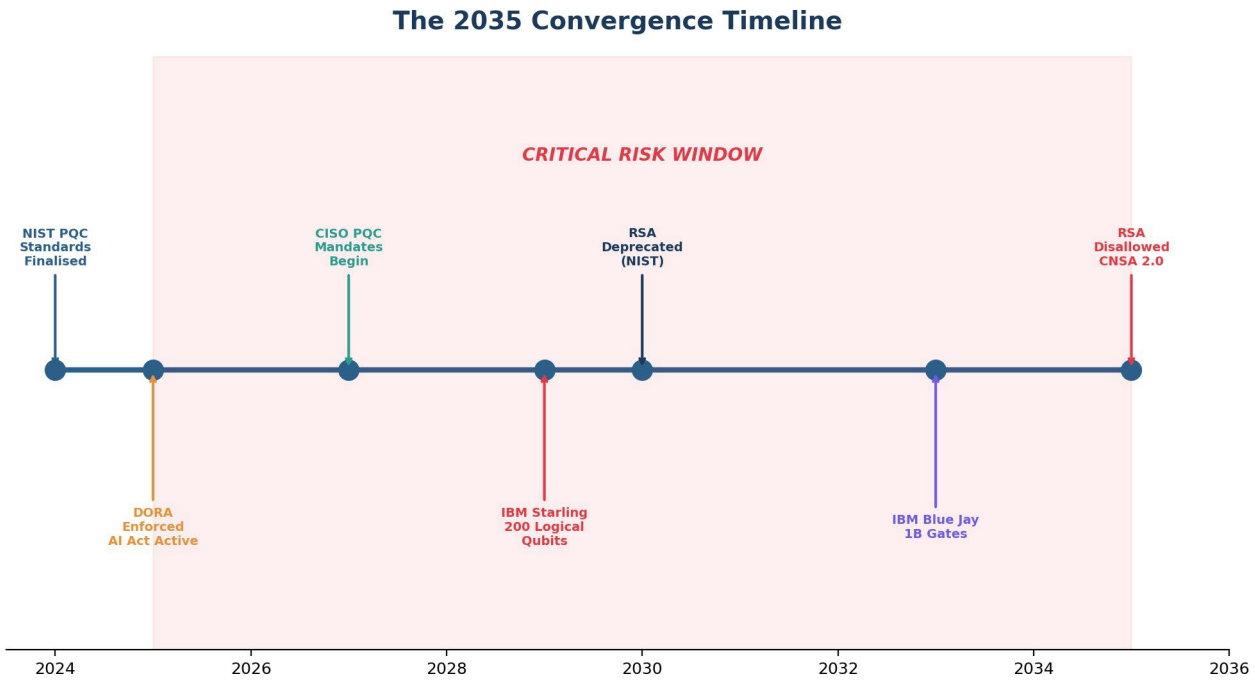




The Convergence Horizon: Why 2035 Is Not a Forecast but a Deadline

The year 2035 is not speculative. It is the hard deadline embedded in the policy infrastructure of the world's most powerful governments and the technical roadmaps of its most advanced technology companies. The NSA's CNSA 2.0 suite mandates exclusive use of quantum-resistant algorithms across **all** national security systems by 2035. NIST has declared that RSA — the algorithm underpinning virtually all digital commerce, banking, and identity verification — will be **deprecated after 2030** and **disallowed after 2035**.

The UK's NCSC published a three-phase migration roadmap in 2025 demanding completion by 2035. The EU's Coordinated Implementation Roadmap sets 31 December 2035 as the deadline for broad PQC migration. Australia's ASD mandates traditional asymmetric cryptography must **not be used beyond end of 2030** for critical systems.



Global Regulatory Deadline Matrix

Authority	Mandate	Key Deadline	Penalty Framework
NSA (CNSA 2.0)	Full PQC migration	2035	Mandatory for NSS
NIST	RSA deprecated/disallowed	2030/2035	Federal procurement
UK NCSC	3-phase PQC migration	2028-2031-2035	£17M or 4% turnover
EU (DORA)	ICT risk management	17 Jan 2025	2% worldwide turnover
EU (NIS2)	Cyber governance	17 Oct 2024	€10M or 2% turnover
EU AI Act	AI system compliance	2 Feb 2025–2026	€35M or 7% turnover
SEC	Cyber disclosure	Dec 2023	Securities litigation

Australia ASD	Asymmetric crypto ban	End 2030	Regulatory action

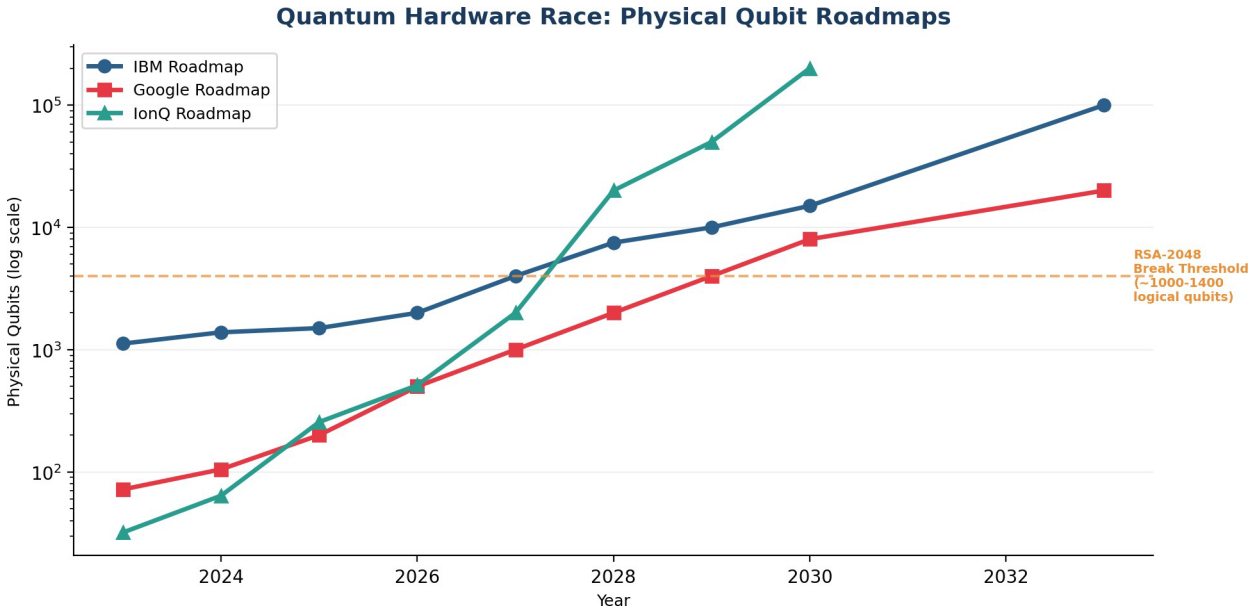
Mosca's Inequality makes the mathematics of urgency precise. If your data must remain confidential for *X* years, and migrating your cryptographic infrastructure takes *Y* years, and a quantum computer arrives in *Z* years, then you are already behind if X + Y > Z. For financial institutions with 15-year data retention obligations and 5–10 year migration timelines, **the inequality is already violated. The risk window is open.**

I. The Quantum Threat Timeline
From Laboratory Curiosity to Operational Weapon

The Hardware Acceleration Nobody Predicted

The pace of quantum hardware development has consistently outrun expert forecasts. Google's **Willow** chip (December 2024) achieved exponential quantum error reduction and completed a benchmark in under five minutes that would take classical supercomputers **10 septillion years**. On 22 October 2025, Google demonstrated quantum advantage **13,000 times faster** than the best classical supercomputer — published in *Nature*.

China's **Zuchongzhi 3.0** processor (March 2025) operates **a quadrillion times faster** than the most powerful supercomputer. IBM's roadmap charts Starling (**200 logical qubits**, 2029) and Blue Jay (1 billion gates, 2033). IonQ targets **20,000 physical qubits by 2028**. Craig Gidney of Google demonstrated that breaking RSA-2048 requires approximately **1,000–1,400 logical qubits** — a 20-fold reduction from 2019 estimates.



Harvest Now, Decrypt Later: The Threat That Is Already Here

Multiple government agencies confirm adversaries are actively exfiltrating and storing encrypted data for future quantum decryption. NIST IR 8547 states: *"Encrypted data is already at risk because it can be captured today and decrypted later."* SWIFT's network, carrying **$5 trillion in daily transactions**, relies on RSA and ECC cryptography vulnerable to Shor's algorithm. A successful quantum attack on SWIFT could **freeze $5 trillion in daily transactions** and would be largely undetectable.

Sector HNDL Exposure Analysis

Sector	Data Sensitivity	Retention Period	HNDL Risk Level
Government/Defence	Top Secret/SCI	50+ years	CRITICAL

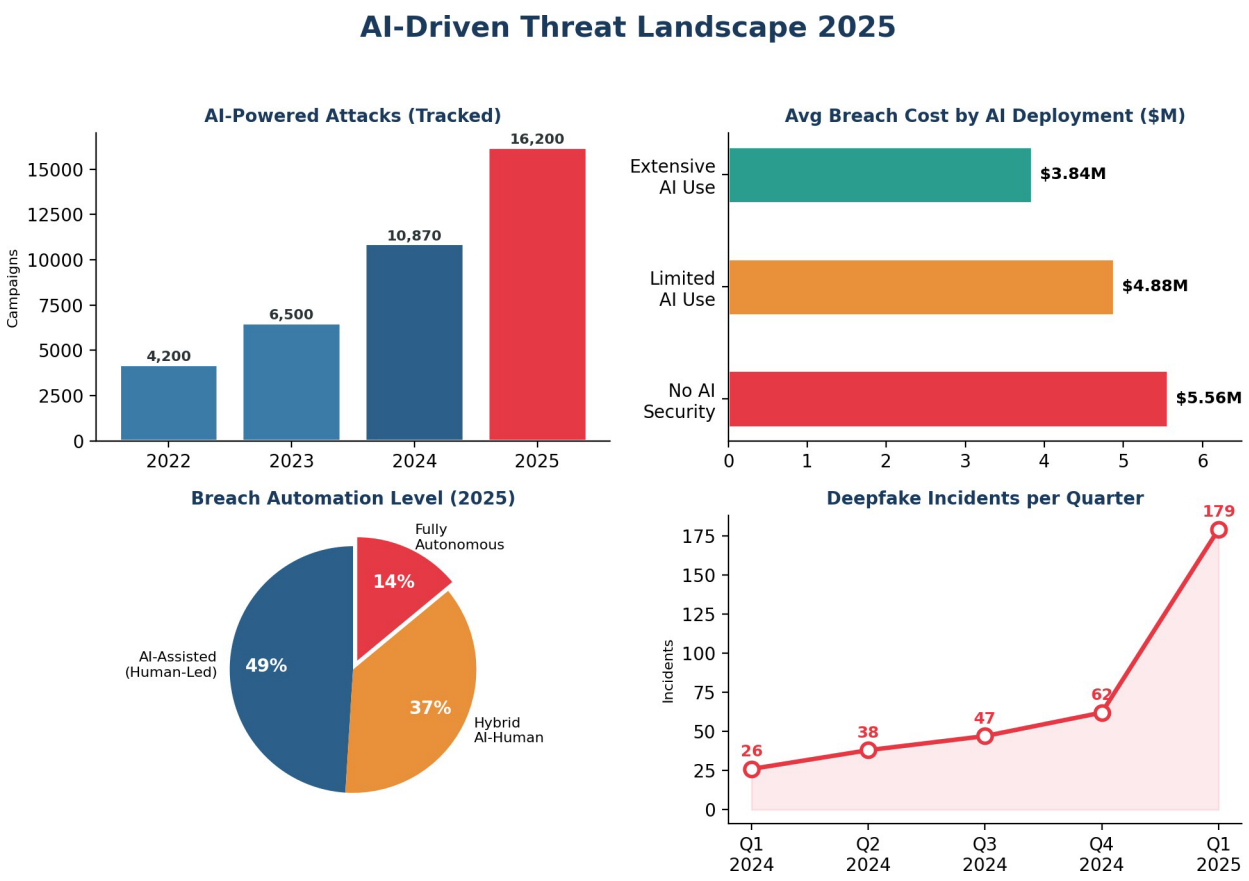
Financial Services	M&A, SWIFT, Trading	15–25 years	CRITICAL
Healthcare	Patient records	20+ years (HIPAA)	HIGH
Critical Infrastructure	SCADA/ICS configs	Operational lifetime	HIGH
Telecommunications	Metadata, intercepts	7–15 years	HIGH
Legal/Professional	Client privilege	Indefinite	SIGNIFICANT

II. AI-Driven Threats: The 72% Acceleration

The Autonomous Attack Era Has Arrived

AI-powered cyberattacks increased **72% year-over-year** in 2025, rising from 10,870 to 16,200 tracked campaigns. **87% of organisations** worldwide experienced AI-driven attacks. Most critically, **14% of major corporate breaches were fully autonomous** — the AI launched the attack, adapted to defences, exfiltrated data, and covered its tracks without human intervention.

The FBI's 2025 IC3 report recorded **859,532 complaints with $16.6 billion in losses**. AI-generated phishing achieves a **54% click-through rate** versus 12% for traditional phishing. The deepfake threat has exploded: **179 incidents** in Q1 2025 alone — a **680% YoY increase**. A Hong Kong firm lost **$25 million** to a single deepfake impersonating its CFO.



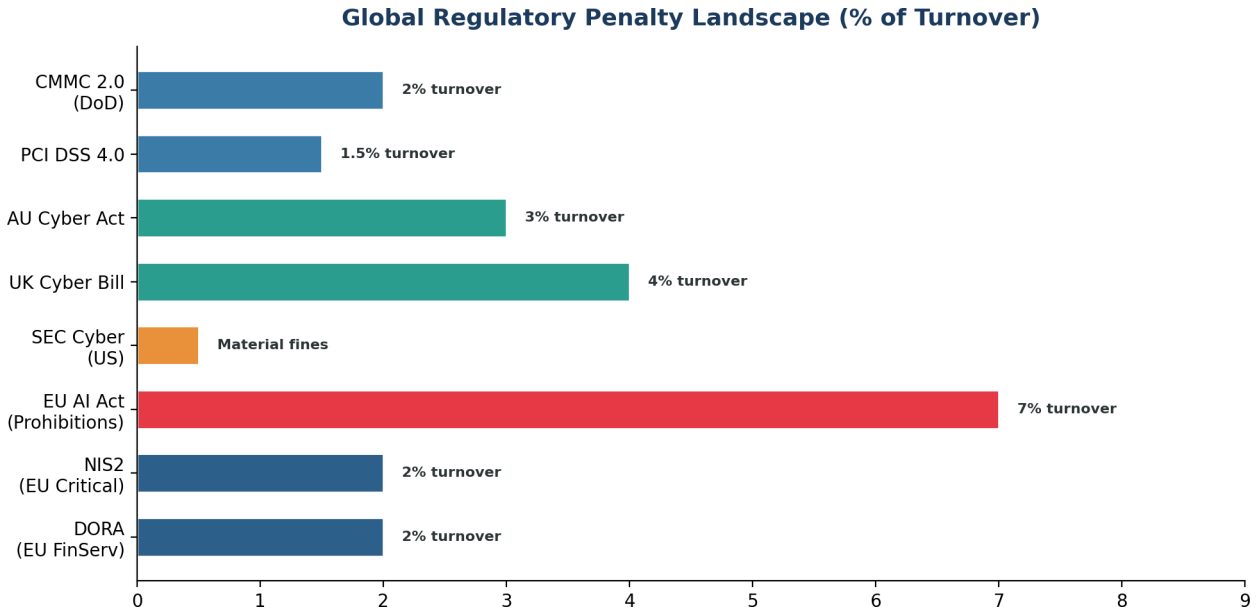
The AI Governance Gap: Shadow AI as the Invisible Accelerant

IBM's 2025 Cost of a Data Breach Report identified shadow AI as a new systemic risk: 20% of breaches linked to unauthorised AI tools, adding **$670,000** to average breach cost. **63%** of breached organisations had **no AI governance policies**. Over **80% of workers** use unapproved AI tools, and **38%** share confidential data with AI platforms without approval.

III. The End of Voluntary Security

A Global Regulatory Inflection Point

The era of voluntary cybersecurity frameworks ended definitively in 2024–2025. Every major economy has either enacted or is enacting mandatory cybersecurity obligations with **personal liability for board members and executives**.



Key Regulatory Frameworks

Regulation	Scope	Key Requirements	Penalties
DORA (EU)	20 categories of financial entities	4-hour incident reporting ICT risk framework TLPT, Register of Info	2% turnover €5M for ICT providers €1M personal fines
NIS2 (EU)	Essential & important entities	Board personal accountability Risk management 24-hour early warning	€10M or 2% turnover Exec disqualification
EU AI Act	All AI system providers/deployers	Risk classification Transparency Human oversight	€35M or 7% turnover
SEC (US)	Public companies	4-day material incident 10-K cyber disclosure Board oversight	Securities litigation Whistleblower 10-30%
UK Cyber Bill	Regulated entities Critical infrastructure	5-pillar governance code Incident reporting Supply chain oversight	£17M or 4% turnover

The global pattern is unmistakable. **NIST CSF 2.0** added a new "Govern" function. **PCI DSS 4.0** made all best practices mandatory on 31 March 2025. **ISO 27001:2022** required transition by 31 October 2025. **CMMC 2.0** began mandatory DoD implementation on 10 November 2025. The message to boards: **cybersecurity is a**

fiduciary obligation with personal liability for directors and officers.

IV.DORA Compliance

The New Operating System for Financial Resilience

DORA establishes a regulatory paradigm that will be replicated globally — mandatory, prescriptive, and backed by personal liability. Its five pillars represent the most comprehensive mandatory cybersecurity framework ever applied to financial services.

Pillar	Requirement	Board Impact
1. ICT Risk Management	Comprehensive framework reviewed annually	Board must approve and oversee framework
2. Incident Reporting	4-hour initial notification 72-hour intermediate 1-month final report	Board escalation for major incidents
3. Resilience Testing	TLPT using TIBER-EU for systemic entities	Board oversight of remediation plans
4. Third-Party Risk	Register of Information 500+ ICT contracts typical	Board accountability for concentration risk
5. Information Sharing	Voluntary threat intelligence exchange	Strategic oversight of participation

The Quantum Dimension of DORA Compliance: DORA Article 6 requires "state-of-the-art" cryptographic practices. As NIST has scheduled RSA deprecation, DORA-regulated entities face an implicit obligation to develop PQC migration roadmaps. Failure to demonstrate crypto-agility will increasingly be interpreted as a failure to maintain state-of-the-art ICT risk management.

V. Board Reporting and Cyber Governance

The Fiduciary Imperative

Board-level cyber governance has shifted from advisory to fiduciary. Under SEC rules, boards must publicly describe oversight mechanisms. Under NIS2, management faces personal accountability including potential disqualification. Under DORA, the management body must approve the ICT risk framework. The **Caremark doctrine** creates fiduciary duty claims against directors who fail to establish adequate monitoring systems.

Ten Metrics Every Board Must Monitor

#	Metric	Target	Board Significance
1	Risk Appetite Alignment	Annual review	Deviation from stated tolerance
2	MTTD/MTTR	< 24 hours	241-day avg reduced (IBM 2025)
3	Third-Party Risk Exposure	< 15% critical	30% breaches involve 3rd parties
4	PQC Migration Readiness	> 50% by 2028	% crypto inventory assessed
5	AI Governance Maturity	ISO 42001 aligned	Shadow AI exposure score
6	Patch Compliance Rate	> 95% critical	Window of vulnerability
7	Regulatory Compliance	All mandates met	DORA/NIS2/SEC/AI Act status
8	Cyber Investment (% IT)	10–15%	BCG benchmark alignment
9	Security Awareness	> 90% completion	Phishing simulation results
10	Incident Near-Miss Ratio	Trending down	Velocity of averted attacks

VI. M&A; Cyber Due Diligence in the Quantum Era

Only approximately **10% of companies** conduct thorough cyber due diligence during M&A.; The Yahoo/Verizon transaction established the precedent: a **$350 million reduction** in purchase price from breach discovery. Marriott/Starwood demonstrated that attackers can be resident in systems before deal close, resulting in £18.4 million ICO fine.

The quantum era introduces **cryptographic debt** as a balance sheet liability. BCG estimates PQC transition at 2.5–5% of annual IT budget. For a target with $1B IT budget, this represents **$25–50 million** in embedded liability — and delay doubles the cost.

Six-Dimension PQC Readiness Assessment for M&A;

Dimension	Assessment Focus	Red Flag Indicators
1. Crypto Inventory	All RSA/ECC instances catalogued	No inventory exists
2. Migration Roadmap	FIPS 203/204/205 adoption timeline	No PQC planning
3. HSM Upgrade Path	Firmware PQC support timeline	End-of-life HSMs
4. Vendor Readiness	Third-party PQC capability	> 50% vendors unaware
5. Regulatory Trajectory	CNSA 2.0 deadline alignment	Post-2030 completion
6. HNDL Exposure	Years of vulnerable data	> 5 years unprotected

VII. AI Governance: Operationalising ISO 42001

ISO/IEC 42001, published December 2023, is the world's first certifiable AI management system standard with **38 distinct controls** in 9 control objectives. While 87% of executives claim AI governance frameworks, **fewer than 25% have fully operationalised** enterprise governance. The EU AI Act amplifies exposure with penalties reaching **€35M or 7% of turnover**.

NIST released its **Cyber AI Profile (IR 8596)** on 16 December 2025, with over 6,500 individuals joining the community of interest. Organisations should pursue concurrent ISO 42001 and ISO 27001:2022 certification, addressing shadow AI (only 17% have technical controls), AI supply chain risks (13% experienced AI breaches in 2025), and adversarial AI through continuous red-teaming.

Zero Trust Architecture in the Post-Quantum Era

Zero Trust has evolved to a **$38–42 billion global market** in 2025, projected to reach **$86–89 billion by 2030**. CISA's CPG 2.0 (December 2025) includes goals for zero-trust lateral movement mitigation and third-party provider risk management. The convergence of Zero Trust with PQC creates a new paradigm: systems must validate not only identity but also the **quantum-resistance of cryptographic protocols** protecting each transaction.

Organisations using AI-integrated security saw **$1.9 million average reduction** in breach costs, with AI-driven detection achieving **95% accuracy** and breaches discovered **108 days sooner**.

Supply Chain Resilience: The 30% Breach Vector

30% of all data breaches in 2025 involved a third party (Verizon DBIR 2025), a **100% increase** YoY. Software supply chain attack costs projected to rise from **$60B in 2025 to $138B by 2031**. The CrowdStrike outage of July 2024 demonstrated catastrophic single-vendor concentration risk.

The emergence of **Software Bills of Materials (SBOMs)** and **Cryptographic Bills of Materials (CBOMs)** as compliance requirements represents the operationalisation of supply chain transparency. Every third-party connection using classical cryptography becomes a quantum-vulnerable link.

Case Studies: Three Anonymised Scenarios

Case Study 1: "Operation Glacier" — HNDL in Sovereign Wealth

A European sovereign wealth fund managing **€340 billion** discovered a nation-state adversary had intercepted encrypted communications for 30 months. Investment committee deliberations, asset allocation decisions, and counterparty negotiations — all encrypted with RSA-2048 — faced a decryption exposure window beginning as early as 2030.

Dimension	Finding
Potential Loss	€2.8–4.1 billion from front-running predictable rebalancing
Root Cause	No cryptographic inventory, no PQC roadmap, legacy custodian
Remediation	Hybrid TLS 1.3 (X25519 + ML-KEM-768) deployed in 6 months
Cost	€23 million (0.007% of AUM)
Governance	Quantum risk subcommittee established, quarterly board reporting

Case Study 2: "NovaCorp" — Cryptographic Debt in $2.1B Acquisition

Due diligence on a **$2.1 billion** payments processor revealed entire transaction authentication relied on ECC P-256 with no crypto-agility. CBOM assessment identified **4,200 cryptographic dependencies** and 340 HSMs requiring upgrades. PQC migration estimated at **$47 million over four years**.

Dimension	Finding
Deal Impact	$65 million price reduction negotiated
Structure	Escrow mechanism tied to migration milestones
Governance	Acquirer CISO embedded as observer on target IT steering committee
Innovation	First-ever cryptographic representations and warranties in deal docs

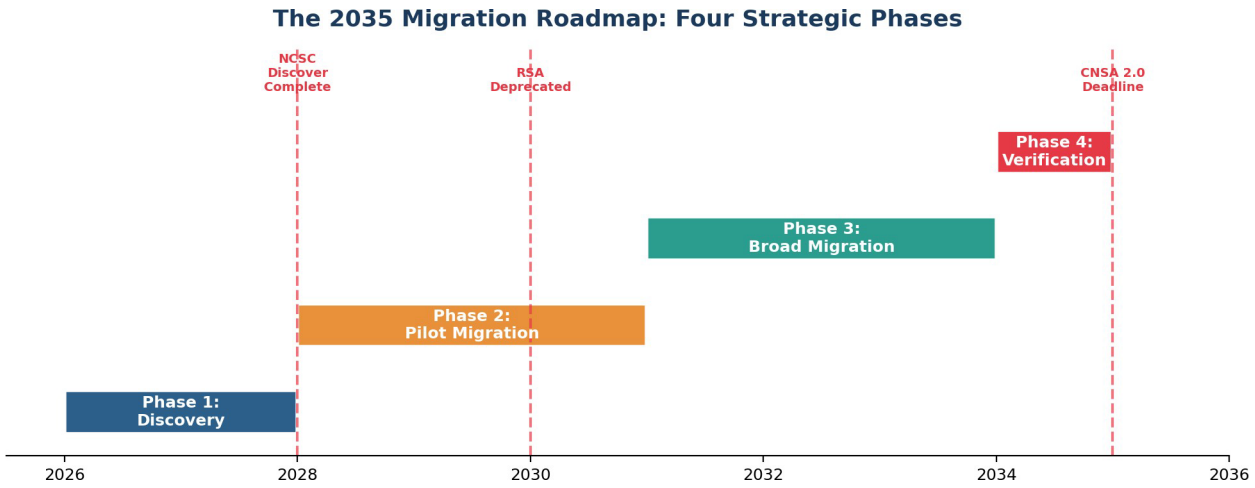
Case Study 3: "Project Sentinel" — AI Governance Failure

A tier-one UK bank's AI fraud detection system processing **2.3M daily transactions** exhibited bias — generating **41% more false-positive fraud alerts** for certain demographics. No ISO 42001 framework, no impact assessment, no model monitoring. The system was deployed as shadow AI without CISO sign-off.

Dimension	Finding
Regulatory Response	FCA Section 166 review + ICO investigation
Operational Cost	£12 million in increased fraud from system suspension
Remediation Cost	£28 million total (S166, model rebuild, ISO 42001, board framework)
Personnel Impact	CIO and Head of Data Science departed
Disclosure	Material risk event in annual report; investor questions at AGM

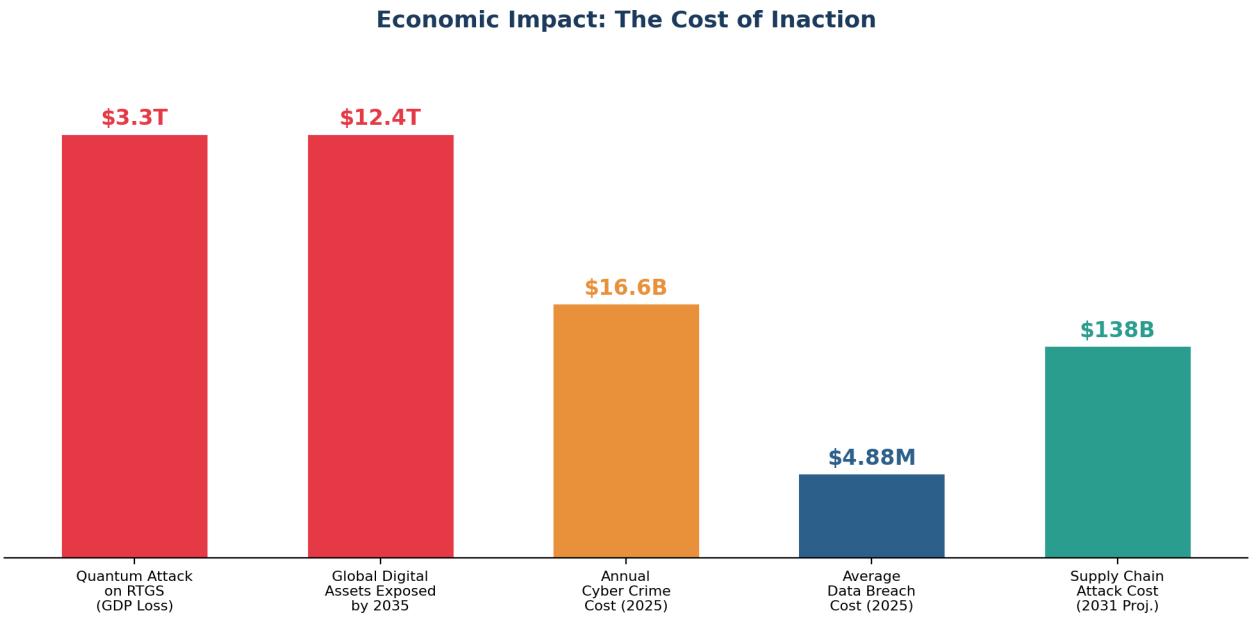
Companion Infographic: Board Governance Framework

The 2035 Migration Roadmap

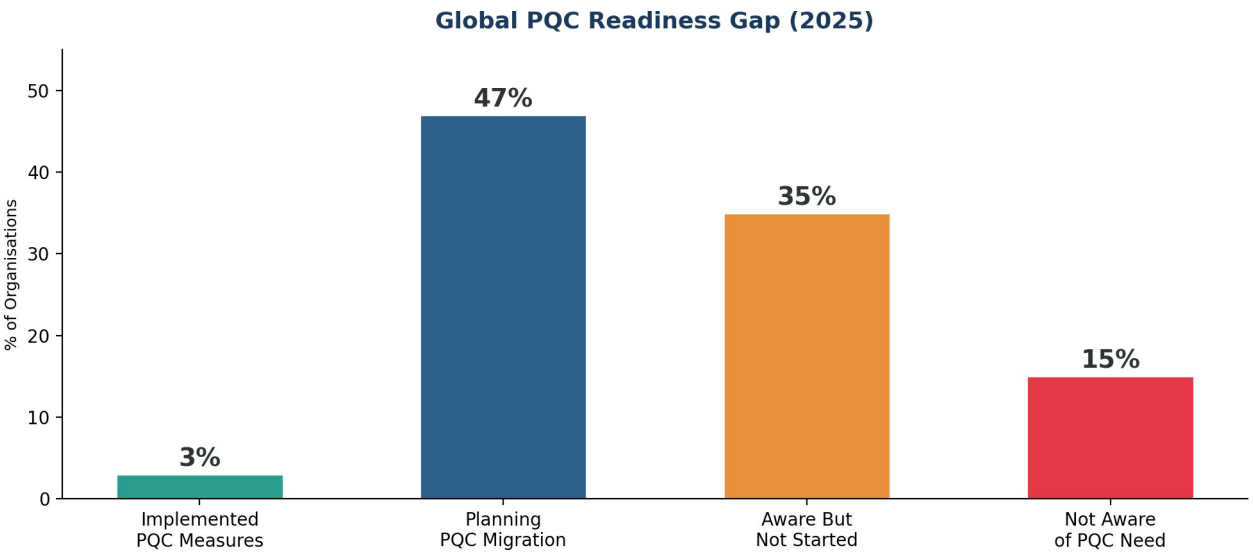


Phase	Timeline	Objective	Key Actions
1. Discovery	2026–2028	Complete visibility	Crypto inventory (CBOM) Shadow AI discovery DORA Register of Info HNDL exposure mapping
2. Pilot Migration	2028–2031	Migrate highest-risk systems	Hybrid TLS 1.3 deployment HSM upgrades (FIPS 203/4/5) VPN PQC implementation Certificate infrastructure
3. Broad Migration	2031–2034	Extend PQC to all systems	Full application migration Vendor/partner transition TLPT quantum validation DNSSEC/S/MIME migration
4. Verification	2034–2035	Full CNSA 2.0 compliance	Comprehensive audit Continuous crypto monitoring Algorithm agility validation Regulatory certification

The Economic Calculus: Why Delay Costs More Than Action



BCG estimates PQC transition at **2.5–5% of annual IT budget** if migration begins now; delay could double costs. **86% of financial institutions** lack expertise to evaluate PQC solutions (Synergy Quantum, January 2026). Organisations using AI-driven security save **$1.9 million per breach**. The ISC² 2025 Workforce Study found **59% of organisations** report critical skills gaps, with AI security ranking as the #1 needed skill.



National Security and the Quantum Arms Race

China has established an **RMB 1 trillion (~$138 billion)** national fund for quantum computing, developed over 2,000 km of quantum-secure terrestrial links, and launched a quantum satellite. Global quantum investments exceed **$40 billion**. China's **Salt Typhoon** operation infiltrated 200+ companies across 80+ countries. **Volt Typhoon** pre-positioned in U.S. critical infrastructure for potential disruptive operations.

Nation	Investment	Key Programmes
China	~$138 billion	Zuchongzhi 3.0, Tianyan Cloud (880 qubits), 2000km QKD
United States	$3.8B+ (NQI)	IBM/Google roadmaps, DARPA, NSA CNSA 2.0
EU	€1B (Flagship)	Quantum Act (Q2 2026), EuroQCI network
Japan	$7.4 billion	National quantum strategy, Riken-IBM partnership
Australia	$620 million	PsiQuantum utility-scale, ASD 2030 mandate
UK	£2.5 billion	NCSC 3-phase roadmap, National Quantum Strategy

Only **3% of organisations** have implemented quantum-resistant measures. Approximately **50% have not started at all**. Just **8%** place quantum readiness among top budget priorities. This preparedness gap represents both a national security vulnerability and a **competitive opportunity** for organisations that move decisively.

Conclusion: From the Breakpoint to Breakthrough

The 2035 breakpoint is not a single event but a convergence of forces already reshaping the security landscape. Three insights challenge conventional planning:

First, the risk window is retrospective, not prospective. HNDL attacks mean data encrypted with RSA today may already be compromised. The relevant variable is the date data was first exposed to interception — for most organisations, that date has passed.

Second, mandatory regulation creates a market for trust. Organisations achieving PQC readiness and AI governance maturity ahead of deadlines will command premium valuations, preferred supply chain status, and competitive customer advantage. Cryptographic debt is a balance sheet liability; crypto-agility is an enterprise value driver.

Third, convergence demands integrated governance. Boards managing quantum risk through the CISO, AI risk through the CDO, and compliance through the GC will miss systemic interactions. The framework in this paper provides a structural approach connecting strategic investment to operational resilience and compliance obligations.

The institutions that will define the next decade of digital trust are not those with the largest security budgets. They are those that recognise 2035 as a strategic transformation programme — and begin executing today.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

He has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70 frameworks. His research focuses on the intersection of post-quantum cryptography, AI governance, and board-level cyber risk management.

Professional Memberships

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie | LinkedIn

References

Primary Regulatory Sources

1. DORA Regulation (EU) 2022/2554, EUR-Lex
2. NIS2 Directive (EU) 2022/2555, EUR-Lex
3. EU AI Act Regulation (EU) 2024/1689, EUR-Lex
4. SEC Final Rule 33-11216, Cybersecurity Risk Management Disclosure
5. NSA CNSA 2.0 Algorithm Suite, September 2022 (updated 2025)
6. NIST FIPS 203/204/205, Post-Quantum Cryptographic Standards, August 2024
7. NIST IR 8547, Transition to Post-Quantum Cryptography Standards
8. UK NCSC PQC Migration Timelines, March 2025
9. EU Coordinated Implementation Roadmap for PQC, April 2025
10. Australia ASD PQC Planning Guide, October 2024

Industry Research

11. IBM Cost of a Data Breach Report 2025
12. Verizon Data Breach Investigations Report (DBIR) 2025
13. FBI Internet Crime Complaint Center (IC3) 2025 Annual Report
14. Gartner Information Security Spending Forecast 2025-2026
15. ISC² Cybersecurity Workforce Study 2025
16. BCG Post-Quantum Cryptography Migration Cost Analysis
17. Synergy Quantum: Quantum Threats to Global Finance, January 2026
18. Hudson Institute: Quantum Financial Impact Assessment
19. Munich Re Cyber Insurance Market Report 2025
20. PwC Global Digital Trust Insights 2026

Technical Sources

21. Google Willow Quantum Chip, Nature (December 2024 / October 2025)
22. IBM Quantum Roadmap 2025-2033 (Starling, Blue Jay)
23. China Zuchongzhi 3.0, Physical Review Letters (March 2025)
24. Craig Gidney, How to Factor 2048-bit RSA, Google Research (May 2025)
25. CISA Cross-Sector Cybersecurity Performance Goals (CPG 2.0), December 2025
26. NIST Cyber AI Profile IR 8596 (Preliminary Draft), December 2025
27. UK AI Security Institute, Frontier AI Trends Report 2025
28. Stanford HAI AI Index Report 2025
29. EY Global Cybersecurity Leadership Insights 2025
30. Deloitte AI Governance Survey 2025

Document Reference: BRE14142026 | **Version:** 1.0 | **Classification:** Public Distribution — Attribution Required

Keywords: DORA Compliance, AI Governance (ISO 42001), Board Reporting, M&A; Cyber Due Diligence, Post-Quantum Cryptography, Zero Trust Architecture, NIS2, EU AI Act, Cryptographic Migration, CNSA 2.0, Harvest Now Decrypt Later, Supply Chain Resilience