Quantum Technologies:

The Privacy & Security Threat – And the Path to Quantum Readiness

Brian T. Lenahan

Chair, Quantum Strategy Institute

Introduction & The Urgency in 2026

- Welcome/Background: From banking exec to quantum strategist via the Quantum Strategy Institute—helping organizations roadmap quantum/AI adoption since 2019.
- 2026 context: Hybrid quantum-classical workflows emerging; CRQC (cryptographically relevant quantum computers) estimates 2028–2035 (optimistic views 2028–2030); NIST PQC standards rolling out; "harvest now, decrypt later" (HNDL) attacks accelerating.
- Live poll: "**Has your organization conducted a crypto inventory for quantum vulnerability?**"
- Session goals: Understand threats, timelines, defenses (PQC + quantum enhancements), and build a prioritized action plan.
- Agenda preview and ground rules for interaction.

Quantum Technologies : Poll

What percentage of companies globally are currently preparing for quantum threats?

- 1%
- 10%
- 20%
- 50%

The Quantum Threat Landscape: Risks to Privacy, Compliance, and Trust

- Core risks: Shor's breaks RSA/ECC → TLS, VPNs, digital signatures, secure email, blockchain, certificates at risk. Grover halves AES-256 effective strength (still usable with upgrades).
- HNDL reality: Nation-states stockpiling encrypted data now—long-lived assets (health records, financial archives, IP, government secrets) most vulnerable.
- 2026 timeline realism:
  - CRQC likely 2030–2035; some forecasts earlier (2028–2030).
  - NIST/CISA/NCSC/EU roadmaps: Deprecate vulnerable algos ~2030; disallow by 2035; start migration now (EU urges end-2026 for critical systems).
- Business/privacy impacts: Massive breaches, GDPR/CCPA/HIPAA long-term violations, loss of customer trust, supply-chain cascades, regulatory fines.
- Real-world signals: **Government mandates**, enterprise audits starting, but 91% lack formal PQC roadmaps (per recent surveys).

Post-Quantum Cryptography: The Core Defense Strategy

- **NIST** 2024 standards recap + 2026 updates: ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+); hybrid crypto as bridge.
- Migration challenges & realities in 2026:
  - Crypto inventory/discovery (tools/libraries).
  - Integration complexity, skills gaps, costs.
  - Hybrid approaches dominant (classical + PQC); pure PQC rare yet.
  - Crypto-agility architectures for future-proofing.
- Step-by-step roadmap:
  - Assess crypto footprint (where/what algos).
  - Prioritize (public-facing TLS, long-term storage, high-sensitivity data).
  - Pilot PQC (OpenQuantumSafe, Bouncy Castle, vendor solutions).
  - Test interoperability/performance.
  - Roll out phased (critical systems by 2030).
- Beyond crypto: Quantum-safe protocols, preparing for QKD in high-security links (e.g., finance/government).

Interactive Deep Dive: Sector-Specific Scenarios & Group Discussion

- Break into small groups for 10 min:
  - Scenario 1: Financial institution with legacy systems + long-term customer data.
  - Scenario 2: Healthcare provider (HIPAA + patient records).
  - Scenario 3: Government/critical infrastructure (national security data).
- Groups discuss: High-risk assets, migration blockers, first 3 actions.
- 10 min debrief: Share insights (common themes—e.g., inventory gaps, budget concerns, regulatory drivers).

Beyond PQC: Emerging Quantum-Enhanced Security Tools & Future-Proofing

- QKD deployments 2026: **Real-world examples** (China's city-scale networks, EuroQCI, India 500+ km, enterprise pilots). Pros (information-theoretic security) vs. cons (distance limits, cost, integration).
- QRNG integration for better randomness in keys/certificates.
- Quantum sensing for physical-layer security.
- Synergies: Quantum + AI for threat detection; preparing for bi-directional quantum-AI impacts.
- Organizational readiness: Build quantum literacy, update risk registers, engage vendors, monitor standards (NIST ongoing rounds).

Extended Q&A and Personalized Action Planning

- Open Q&A (common: "Cost estimates?", "What if quantum arrives early?", "Vendor recommendations?").
- What Will You Take Away?:
  - Immediate steps: Crypto audit + PQC pilot.
  - Timeline alignment: Critical migration by 2030 (45 months away)
  - Resources: NIST roadmap, CISA guidance, Quantum Strategy Institute, **UBC contacts**.
- Personal action prompt: "What is one step your organization can take in the next 90 days?"

Closing & Key Takeaways

- Recap: Quantum is a **threat multiplier** but also an opportunity—proactive PQC migration + quantum enhancements build resilience.
- Final message: "Treat this like Y2K on steroids: The organizations acting in 2026–2028 will lead in trust, compliance, and advantage."
- Thank you + networking: **Connect via LinkedIn, Substack (*Quantum's Business*), or Quantum Strategy Institute** for roadmapping support.

Quantum Technologies:

The Privacy & Security Threat – And the Path to Quantum Readiness

THANK YOU