INTELIDATA CYBERSECURITY NEWSLETTER

The Quantum Threat is Closer Than You Think:

Why Organizations Must Begin Their Post-Quantum Cryptography (PQC) Journey Today

For years, organizations have relied on cryptographic algorithms such as RSA, ECC, Diffie-Hellman, and traditional PKI infrastructures to secure sensitive information, authenticate users, protect transactions, and maintain trust across digital ecosystems.

These cryptographic foundations currently protect:

- Online Banking & Financial Transactions
- Digital Certificates & PKI
- VPN Communications
- Cloud Applications
- Email Security
- Identity & Access Management Systems
- IoT Devices
- Manufacturing Systems
- Critical Infrastructure
- Healthcare and Government Records

However, the emergence of Quantum Computing is expected to fundamentally disrupt this security model.

While practical large-scale quantum computers may still be several years away, cybersecurity experts, governments, and standards bodies across the globe agree on one thing:

Organizations need to start preparing now.

Understanding the Quantum Risk

Today's encryption standards are designed to resist attacks from conventional computers.

Quantum computers, however, operate using quantum mechanics and have the potential to solve certain mathematical problems exponentially faster than classical computers.

This means that cryptographic algorithms widely used today—including RSA and ECC—could eventually become vulnerable to quantum attacks.

A successful quantum attack could potentially compromise:

- Confidential business information
- Customer and employee data
- Intellectual property
- Financial transactions
- Digital signatures
- Authentication systems
- Long-term archived information

The concern is particularly significant for organizations handling data that must remain confidential for 5, 10, or even 20 years.

The “Harvest Now, Decrypt Later” Threat

One of the most concerning emerging cyber threats is known as:

Harvest Now, Decrypt Later (HNDL)

Attackers may already be collecting encrypted information today and storing it for future decryption once quantum computing capabilities mature.

This means that even if your data is secure today, it may not remain secure tomorrow.

Industries particularly exposed include:

Financial Services

Customer data, transaction records, payment systems, and banking communications.

Healthcare

Medical records, patient information, clinical research, and healthcare systems.

Automotive & Manufacturing

Connected vehicle platforms, intellectual property, production systems, and supplier communications.

Government & Public Sector

Citizen records, national infrastructure, and classified communications.

Technology & SaaS

Cloud applications, source code repositories, customer platforms, and API ecosystems.

What is Post-Quantum Cryptography (PQC)?

Post-Quantum Cryptography refers to cryptographic algorithms specifically designed to resist attacks from both classical and quantum computers.

To address future risks, the cybersecurity industry is transitioning toward new cryptographic standards that can provide long-term protection against quantum-enabled attacks.

Global standards organizations, including NIST, have already initiated the standardization and selection of quantum-resistant cryptographic algorithms.

Organizations worldwide are now beginning to assess their readiness and develop migration strategies toward quantum-safe architectures.

Why Organizations Need a PQC Readiness Assessment

Many organizations are unaware of where cryptography is being used within their environment.

Encryption often exists across:

- Applications
- Databases
- APIs
- Network Infrastructure
- Cloud Services
- Security Products
- PKI Environments
- Third-Party Solutions

Without visibility into cryptographic dependencies, future migration efforts become complex, costly, and risky.

A structured readiness assessment helps organizations:

✓ Identify vulnerable cryptographic assets

✓ Understand quantum-related business risks

✓ Prioritize remediation activities

✓ Develop realistic migration timelines

✓ Improve compliance readiness

✓ Reduce future operational disruption

Intelidata's PQC Compliance & Readiness Assessment

Intelidata helps organizations evaluate their preparedness for the quantum era through a comprehensive advisory and assessment framework.

Our approach combines cybersecurity expertise, governance practices, cryptographic assessment methodologies, and business-focused risk management.

Our Assessment Methodology

Phase 1 – Discovery & Stakeholder Engagement

We begin by understanding the organization's environment, security architecture, business objectives, and compliance requirements.

Activities include:

- Stakeholder interviews
- Architecture discussions
- Scope identification
- Business impact understanding

Phase 2 – Cryptographic Discovery & Inventory

We identify cryptographic implementations across the organization.

This includes:

- Encryption algorithms
- Digital certificates
- PKI infrastructure

- SSL/TLS implementations
- Key management systems
- Secure communication protocols
- Authentication mechanisms

Deliverable: ### Cryptographic Asset Inventory

Phase 3 – PQC Readiness Assessment

Our experts evaluate the current cryptographic landscape and identify technologies that may be vulnerable to future quantum attacks.

Assessment areas include:

- RSA implementations
- ECC usage
- VPN technologies
- Certificate management
- Cloud security controls
- Third-party dependencies

Deliverable: ### PQC Readiness Assessment Report

Phase 4 – Gap Analysis & Quantum Risk Assessment

We perform a detailed evaluation of gaps and associated risks.

The assessment covers:

- Technical exposure
- Business impact
- Regulatory considerations
- Operational dependencies

Deliverables: ### Gap Analysis Report ### Quantum Risk Assessment

---

Phase 5 – Migration Strategy & Roadmap

Based on the assessment findings, Intelidata develops a practical and phased migration roadmap.

The roadmap includes:

- Priority systems
- Recommended migration sequence
- Resource planning
- Risk mitigation measures
- Governance recommendations

Deliverable: ### PQC Migration Roadmap

Key Deliverables

Upon completion of the engagement, organizations receive:

📌 Cryptographic Asset Inventory

📌 PQC Readiness Assessment Report

📌 Gap Analysis Report

📌 Quantum Risk Assessment

📌 Cryptographic Dependency Mapping

📌 Executive Summary Presentation

📌 PQC Migration Strategy & Roadmap

📌 Management Recommendations Report

What's Included

- Stakeholder workshops
- Cryptographic discovery exercises
- Architecture review
- Certificate and key management assessment
- Third-party dependency review
- Risk analysis
- Executive reporting
- Strategic migration planning

What's Excluded

The engagement is advisory and assessment-focused and does not include:

- PQC implementation activities
- Technology procurement
- Software development or code modifications
- Production environment changes
- Penetration testing
- Vulnerability assessments
- Certification or attestation services
- Managed security operations
- Ongoing monitoring services

Why Choose Intelidata?

Intelidata brings extensive experience in:

- Cybersecurity Consulting
- ISO 27001 & Compliance Programs
- Governance, Risk & Compliance (GRC)
- Security Architecture
- vCISO Services
- Cloud Security
- Security Assessments
- Managed Security Services

Our experts help organizations prepare not only for today's threats but also for the cybersecurity challenges of tomorrow.

The Time to Prepare is Now

Quantum computing may not replace traditional computing tomorrow—but organizations that delay planning risk facing significant technical, operational, and compliance challenges in the future.

The transition to quantum-safe cryptography will not happen overnight. It requires visibility, planning, governance, and a structured migration strategy.

Organizations that begin preparing today will be better positioned to protect sensitive information, maintain customer trust, and remain resilient in an evolving threat landscape.

🔐 Prepare Today. Secure Tomorrow. Become Quantum Ready with Intelidata.

📧 info@intelidata.co.in
🌐 www.intelidata.co.in