How to Prioritize Systems and Applications for PQC Migration in a Harvest-Now, Decrypt-Later World

1. The Urgency of the Harvest-Now, Decrypt-Later Threat

When people think of quantum computing and cryptography, the typical mental image is a futuristic computer instantly cracking RSA or ECC keys. While that image is accurate, it belies the real danger that is much more subtile, and is already here. Attackers don't need a fully capable quantum computer today to put your organization at risk. They only need the foresight to record (targeted) encrypted traffic and archives now, with the expectation that in 5, 10, or 15 years, they will be able to return and decrypt it.

This practice, known as Harvest-Now, Decrypt-Later (HNDL), fundamentally changes how we must think about security.

Consider industries where data has long-term sensitivity:
- **Healthcare:** Patient records, genomic research, or medical device telemetry that must remain private for a lifetime.
- **Finance:** Transaction records, payment card data, and trading algorithms that reveal systemic risks if exposed years later.
- **Government and defense:** Diplomatic cables, intelligence communications, or classified projects that remain sensitive for the next 50, 70 or 100 years, or even indefinitely.
- **Intellectual property:** Pharmaceutical designs, aerospace blueprints, or source code that represent competitive advantage for decades.

For these domains, even if quantum computers capable of breaking current encryption won't be practical for 10–15 years, adversaries who collect data now will eventually succeed in decrypting it. That makes the threat current, not hypothetical.

2. Assessing Data Sensitivity and Longevity

The first step in any PQC (Post-Quantum Cryptography) migration program is to recognize that not all data requires the same level of protection. A chat message between two employees about lunch plans has little long-term value, while a proprietary algorithm could be catastrophic if decrypted in 15 years.

To prioritize, two questions must be asked about every system or application:

1. How sensitive is the data?
- Does it contain regulated information (e.g., HIPAA, GDPR, PCI DSS)?
- Would its exposure create reputational damage, financial loss, or pose a national-security risk?
- Does it include cryptographic keys or credentials that, if compromised, could unlock other data?

2. How long must the data remain secure?
- Does the protection window extend months, years, or decades?
- Would the value of the data decay quickly (e.g., one-time authentication tokens) or persist indefinitely (e.g., medical history, IP filings)?

The combination of sensitivity and longevity creates a risk profile. Data that is both highly sensitive and long-lived demands immediate PQC consideration. Short-lived, low-value data may fall to the bottom of the priority list.

3. Mapping Cryptographic Dependencies Across Systems

Knowing what needs protection is one thing. Knowing where cryptography is embedded in your environment is another. Most organizations underestimate how pervasive cryptographic functions are. It's not just TLS certificates and VPN tunnels:

- **Infrastructure**: Certificate authorities, PKI hierarchies, authentication servers, secure email gateways.
- **Applications**: Databases, web apps, mobile apps, SaaS integrations.
- **APIs and microservices**: Service-to-service communication often depends on cryptographic handshakes.
- **IoT and edge devices**: Embedded firmware may use RSA/ECC in ways that are extremely difficult to replace post-deployment.
- **Cloud services**: Key management, data encryption, and customer-facing APIs rely on classical algorithms.

Conducting a crypto inventory is a critical early activity. The goal is to identify:
- Where public-key cryptography (RSA, ECC, DH, ECDH) is used.
- Which libraries, standards, and protocols are in play (e.g., OpenSSL, TLS 1.2, S/MIME).
- The dependencies between systems, because sometimes upgrading one system (e.g., the certificate authority) is a prerequisite for others.

The output is a map of cryptographic dependencies. This doesn't just show what needs PQC migration; it reveals linchpin systems where failure to migrate leaves everything else vulnerable.

4. Prioritizing Migration by Risk and Feasibility

Once sensitivity, longevity, and dependencies are clear, organizations can build a rational prioritization plan. This is where business risk and technical feasibility meet.

High Priority (Migrate First):
- **Public Key Infrastructure (PKI):** Certificate authorities, OCSP responders, signing services.
- **TLS endpoints:** External-facing web services, VPN gateways, and APIs handling customer traffic.
- **Key management systems (KMS):** Any system storing or distributing encryption keys.
- **Data archives:** Encrypted backups or records that must remain confidential for decades.
- **Defense and critical infrastructure systems:** Where compromise could have national-security or life-safety implications.

Medium Priority:
- **Internal APIs and business apps:** Important, but may be insulated by network segmentation or limited retention periods.
- **Cloud workloads with short-lived data:** Where quantum risk is lower due to data volatility.
- **Enterprise SaaS platforms:** Vendor roadmaps may dictate timing; medium priority until PQC support

matures.

Low Priority (Defer or Replace):
- **Legacy systems near end-of-life:** In some cases, it may be cheaper and safer to retire than to retrofit.
- **Ephemeral communications:** Systems where data expires in hours or days, reducing HNDL impact.
- **Transitory systems**: Proof-of-concept or non-critical workloads.

Importantly, feasibility must temper risk. Migrating cryptography on IoT devices deployed in the field, for example, may be technically prohibitive. In such cases, organizations must weigh the cost of migration against compensating controls (e.g., upgrading gateways, limiting exposure, or accelerating device replacement cycles).

5. Building a Continuous PQC Migration Roadmap

Post-quantum migration is not a "big bang." It is a multi-year transformation program requiring sustained governance. A continuous roadmap ensures progress while reducing disruption.

Key recommendations include:
- Adopt hybrid approaches: NIST has selected CRYSTALS-Kyber (for key exchange) and Dilithium (for signatures), but operational maturity takes time. Many vendors now offer hybrid modes that combine classical algorithms with PQC. These provide insurance against both near-term and long-term threats.
- Test in controlled environments: Begin pilots in lab settings before rolling out to production. Measure performance, compatibility, and failure modes.
- Build crypto agility: Don't treat PQC migration as a one-off replacement. Design systems so algorithms can be swapped with minimal disruption. Future cryptographic advances (including new PQC standards or vulnerabilities) will demand agility.
- Integrate with enterprise risk management: Align PQC migration with data-protection policies, compliance frameworks, and business continuity planning.
- Educate stakeholders: Boards, executives, and end users must understand that this is not speculative. The HNDL threat means that inaction today creates real exposure tomorrow.

The roadmap should be structured in phases:
1. Discovery & Inventory: Complete the cryptographic map.
2. Risk Assessment: Rank systems based on sensitivity × longevity × feasibility.
3. Pilot & Hybrid Deployment: Begin with high-priority systems in test and staging.
4. Enterprise Rollout: Expand PQC to production systems, adjusting based on lessons learned.
5. Ongoing Governance: Monitor NIST and vendor updates, refresh standards, and continue crypto-agility practices.

Conclusion

Harvest-Now, Decrypt-Later reframes the quantum threat as immediate rather than distant. The attackers of the future may already have your encrypted data today. That makes PQC migration not simply a matter of innovation but of survival.

By systematically evaluating data sensitivity, longevity, and cryptographic dependencies, and by applying risk-driven prioritization, organizations can protect the systems that matter most while building the agility to adapt as standards evolve.

The time to start is not when a quantum computer reaches maturity. The time to start is now.

Sensitivity × Longevity Prioritization Matrix

Sensitivity	Short Longevity (days–months)	Medium Longevity (1–5 years)	Long Longevity (5–20+ years)
Low	Low Priority: Ephemeral logs, temp caches, internal test systems.	Medium Priority: Operational metrics, basic analytics, transient cloud workloads.	Medium Priority: Low-value archives and non-critical historical data.
Medium	Medium Priority: Internal APIs, SaaS integrations, low-risk employee data.	Medium Priority: Routine business apps, short-lived customer records, common transactions.	High Priority: Databases with regulated records (e.g., GDPR, HIPAA), time-sensitive IP.
High	Medium Priority: Encrypted communications with short shelf life (e.g., chat, tickets).	High Priority: Authentication/identity, payment systems, legal contracts, finance records.	Critical Priority: PKI/CA, identity providers, long-term archives (defense, healthcare/genomics), core IP, KMS.