Real-world lessons *for* PQC migration

Ryan Hurst

Digital security and cryptography expert
CEO at Peculiar Ventures, Advisor SpruceID
Former Google and Microsoft

We secure video game DRM better than bank keys

The video game industry rotates keys better than banks or agencies.

THE PROBLEM: Poor key management risks mission failure.

THE SOLUTION: Start with visibility.

Sound familiar?

What PQC migration is not

~~New algorithms alone~~

~~A one-time project~~

~~More scanners~~

~~Compliance checkbox~~

These are tactics. Not the foundation.

The data shift

PAPER MODEL

1995-2020

Manual audits > Slow, incomplete

Zero visibility post-audit

DIGITAL MODEL

How it's changing

SIEM/EDR/CMDB > Real-time insights

Continuous visibility enables action

Not just data collection.

A new model for crypto governance.

What PQC migration is

"Real-time discovery of crypto assets proven with existing data evaluated against PQC readiness maintained through automation."

Discovery **Data-driven** **Readiness** **Automated**

Failure pattern VS success pattern

UK PIV (2010s)

Manual updates → Delays

Heartbleed (2014)

$500M+ → Unmapped keys

NSA PQC Plan (2020s)

Manual risk → Slow adoption

Pattern: Manual methods fail at scale.

Result: 7 out of 10 PQC efforts stall.

Google (2010s)

Automated certs → Billions managed

Microsoft (2020s)

Dynamic keys → Zero Trust

NSA Timeline (2025)

Automation drives PQC

Pattern: Automated lifecycle, mapped dependencies, continuous governance

Success rate: ~3 out of 10.

The security catastrophe

HEARTBLEED 2014

$500M+ lost

PQC RISK: Quantum could break RSA/ECC

MULTI-AGENCY: Unmapped dependencies amplify damage

RECOVERY: Billions in mitigation

This was operational failure, not theory.

Why this matters for MITRE

You don’t manage “PQC” in abstract.

You manage *mission crypto:*

Defense systems
Agency APIs
OT networks
Cloud platforms

→ **Federal relies on you**

→ **Operations depend on you**

Digitizing crypto transforms mission assurance.

What “Discovery” means for MITRE

When discovery is data-driven, these questions matter:

WHO MAPS THE DATA?	WHO UPDATES THE MAPS?	WHO ACTS ON THE DATA?
Teams or vendors?	When systems change?	CIO or CISO?

These are governance questions for mission readiness.

What “Automated” means for MITRE

Manual: one-time fixes, high risk. Automated: continuous protection

BUDGET NEED

Initial cost: $X
Annual automation: 10-15% of $X

CRYPTO RISK

Quantum: 5-10 year horizon
Plan: Ongoing agility

Automation isn’t optional—it’s survival.

Before you commit to any approach

Understanding PQC is tells you what to ask:

BECAUSE IT'S DISCOVERY-DRIVEN

Who maps and updates data?

BECAUSE IT'S AUTOMATED

Can you fund 20+ years of automation?
What's your PQC migration plan?

BECAUSE IT'S MISSION-CRITICAL

Who's your anchor tenant? How do you mitigate mission risk?

If you can't answer, you're not ready.

Success looks like this

You know you're ready when

- ✔ Anchor tenants drive demand
- ✔ 10-15% annual automation budget
- ✔ PQC migration plan in place
- ✔ Dependency maps updated
- ✔ Mission risks assessed

3 out of 10 succeed. 7 fail without this.

What PQC migration is

- ✔ PQC migration is real-time discovery proven with data evaluated for readiness maintained through automation.
- ✔ *Not* just new algorithms.
- ✔ A new *model* for mission crypto.
- ✔ Tech is easy. Governance is hard.