pwc

Post-quantum security in Malaysia

What Q-Day means for business

July 2026

Table of contents

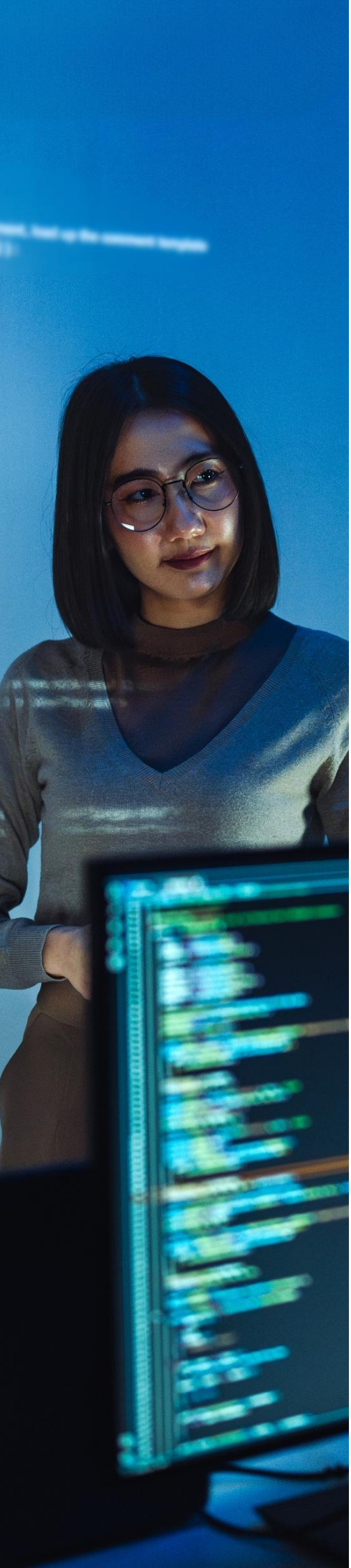
Introduction **03**

Why now: Digital trust and ecosystem stability are at stake **04**

Where risk lies: Quantum risk is not evenly distributed across industries **07**

What to do: A practical roadmap for PQC migration **11**

The path forward for business leaders **12**



The countdown to Q-Day has begun—the moment quantum computers will render today's encryption standards obsolete

The conversation is rapidly moving away from whether quantum computing will become powerful enough to break today's public-key encryption methods, because it will. This specific point in time—known as Q-Day—looms upon the horizon. More importantly, it gives rise to a more practical question: who will be ready when it does?

For Malaysian organisations, the challenge lies in preparing for this eventuality; deliberately and on their own terms. Digital infrastructure is increasingly embedded in the nation's economy, from cloud ecosystems to the rise of digital banking, and the nationwide rollout of 5G infrastructure. Our reliance on digital systems means we cannot afford inaction in protecting this critical infrastructure.

Preparedness won't just be about securing data. Organisations taking action today will have a clearer understanding of their technological dependencies, stronger governance over their assets and a more resilient digital foundation. At stake is the trust and stability of the digital ecosystem that will define Malaysia's future prosperity.

So, where should Malaysian business leaders focus first? In our view, the answer lies in the following three realities that will define the transition to a post-quantum world.

Why now

Digital trust and ecosystem stability are at stake

Where risk lies

Quantum risk is not evenly distributed across industries

What to do

A practical roadmap for PQC migration

Why now

Digital trust and ecosystem stability are at stake

While it is tempting to view post-quantum cryptography (PQC) as a distant compliance obligation, the consensus is clear across nations and major vendors—the timeline to Q-Day is drawing closer. This new reality is driving a wave of definitive action.

In the United States, the White House solidified this urgency by issuing a National Security Memorandum in June 2026 that set a firm migration timeline for government agencies and critical infrastructure. Crucially, the private sector is not waiting for mandates to act. Tech giants like Google, Cloudflare, and Amazon Web Services are already deploying PQC across their global networks, from browsers to cloud services. This reflects a broader global consensus, as other nations like France are also phasing out certifications for non-PQC products.

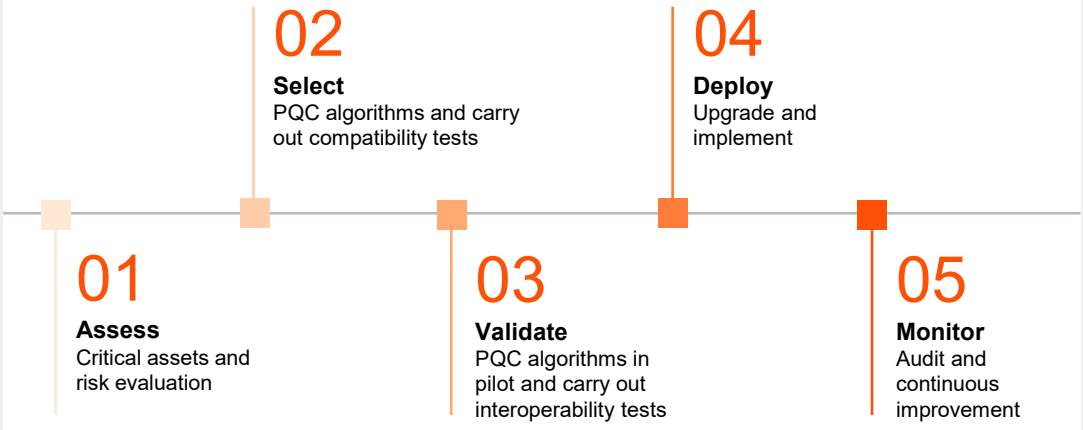
With the window for preparation narrowing, acting now is a business imperative. In our view, three factors underpin the case for action.

1

The national direction is already set for businesses

While the regulatory environment is still being shaped, the government's signal is clear. The development of a national PQC Migration Framework offers organisations a pathway to quantum-safe encryption. This was reinforced in November 2025 with the launch of the National PQC Migration Plan 2025–2030 and a PQC Sandbox Programme, positioning Malaysia as the first Southeast Asian nation to publish a structured national framework for the transition.

The five phases of the National PQC Migration Plan 2025–2030



While Malaysia is leading the way regionally, we are far from alone on the global stage. Leading economies, including Canada and the European Union, have already set firm national milestones, with discovery to be completed by 2028 and full migration by 2035. The message to the market is clear: quantum-safe encryption is fast becoming the expected global standard, and organisations should read the direction of travel rather than wait to be compelled by it.

2

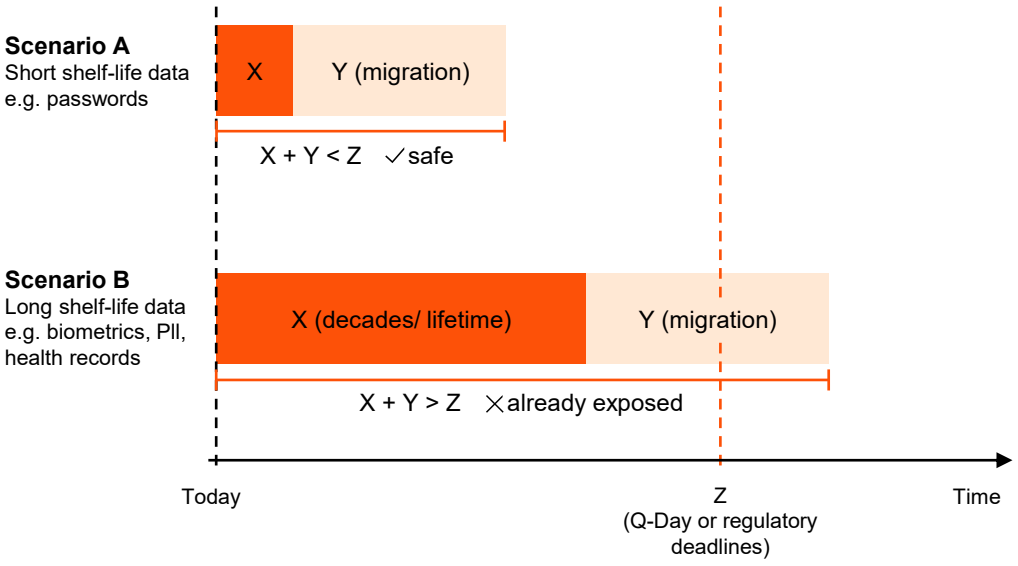
The migration takes years—the 'harvest now, decrypt later' clock has started

This may be the single most under-appreciated fact. The journey from a standardised algorithm to full integration across an enterprise typically takes 10 to 20 years, reflecting the complexity of building new cryptography into products, procuring them, and integrating them across infrastructures.

Even if Q-Day is a decade away, the work must begin today, notwithstanding regulatory deadlines. Mosca's Theorem captures the challenge: if your data must stay secure longer than it will take to complete your migration, you're already behind the curve.

Mosca's Theorem illustrates why preparation must start now

X = data shelf life Y = migration time Z = arrival of cryptographically relevant quantum computer



Adversaries can intercept and store encrypted data today, intending to decrypt it once quantum computers mature. Because sensitive data often retains its value for many years, this data is effectively already compromised—the breach simply has not been realised yet. The exposure is most acute for National Critical Information Infrastructure (NCII) entities such as those in the healthcare, financial services and telecommunications sectors.

This threat, however, is not confined to critical infrastructure. Every organisation possessing long-lived, sensitive data—from intellectual property to customer records—faces a similar countdown. The focus thus shifts from the possibility of a breach to the inevitability of decryption. For any leader, the ultimate question becomes: when this data is exposed, will inaction be a defensible position?

3

The awareness gap is itself a business risk

Perhaps the most pressing concern is mindset. Many organisations, especially those outside direct regulatory mandates, treat the threat as remote and conclude there is nothing to do today.

Organisations that delay will, in time, find themselves running large legacy estates of quantum-vulnerable systems, carrying risk that becomes progressively more challenging and costlier to unwind. Because migration takes years and harvesting is already underway, doing nothing can reduce the options available for a measured, controlled transition.

Which path will you choose for your PQC migration journey?

Path A:

Act now—orderly and planned

The outcome:

Your organisation is quantum ready with much lower and predictable cyber costs

Path B:

Wait and see—disruptive scramble

The outcome:

Your organisation will be in constant crisis response with cyber costs increasing exponentially

Malaysian businesses are gaining ground in the PQC migration

Malaysian businesses are not far behind in the shift to PQC. While 42% of Malaysian C-suite executives say that their organisations have yet to implement or plan quantum-resistant security measures, there is notable progress among industry leaders. In fact, around 47% of Malaysian C-suite executives report that they have already begun piloting and testing quantum-resistant security solutions—well ahead of the global average of 29%.

Where risk lies

Quantum risk is not evenly distributed across industries

Now that we've established when to act, let's examine where quantum risk is concentrated. The threat is not evenly distributed: it is most significant where long-lived confidential data intersects with cryptography that could be intercepted or forged in the future.

The practical implication is a clear order of priority: organisations should prioritise looking into systems that process their most sensitive or long-lived data, and those that manage critical communications.

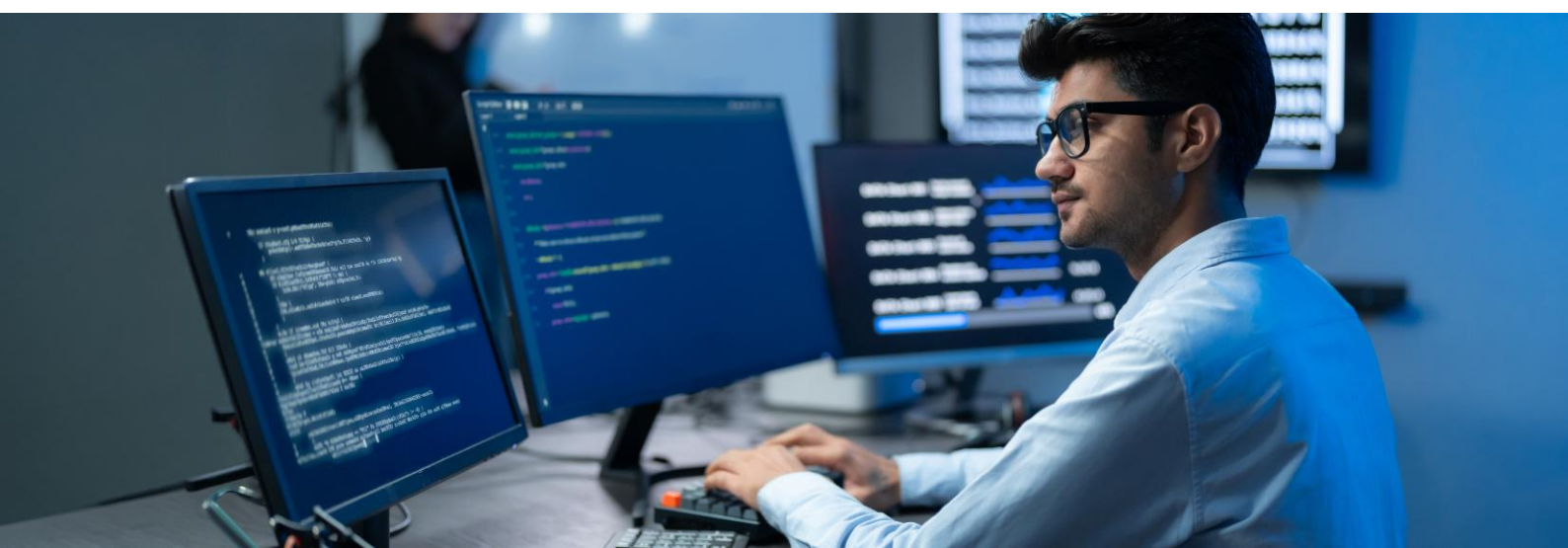
The global picture puts the scale of the challenge into perspective

A single-day quantum attack on one major US bank's payment access has been modelled at **US$2.0–US$3.3 trillion in indirect losses** (10%–17% of GDP) and a 6-month recession

Quantum-safe signatures are roughly **38× larger** than today's equivalents (2,420 vs 64 bytes), straining legacy payment-message formats

>90% of internet traffic relies on encryption protocols built on today's public-key cryptography, making the transition to PQC one of the largest technology transformations of the next decade

Source: Hudson Institute, NIST FIPS 204, Canadian Centre for Cyber Security, European Commission, CISCO, Microsoft



It’s not one threat, but two

Most people focus on confidentiality: the 'harvest now, decrypt later' attack where adversaries steal encrypted data today to break it open tomorrow.

But there is a second, equally dangerous threat: the forging of long-lived digital signatures. This would allow an attacker to impersonate your software updates, your executives, or your critical systems. For banks, government, and critical infrastructure, both threats are very real.

1 The ‘stolen data’ threat (Harvest now, decrypt later)

Adversaries steal your encrypted data today, planning to unlock it with future quantum computers

The impact: Past and present confidential data becomes vulnerable

2 The ‘forged trust’ threat (Forge later)

Adversaries forge the digital signatures that verify your software, executives, and systems.

The impact: Trust in your future compromised

What this means for industries

For Malaysian leaders, the global picture translates into tangible, sector-specific risks and challenges—and concrete actions that can begin today. In our experience, banking, telecommunications and healthcare warrant the earliest attention, given their reliance on long-lived data and globally-interconnected infrastructure.

Industry	Key risks	Key challenges	What leaders can do now
Financial services	Future decryption of harvested financial data and forgery of digital signatures on transactions enable systemic fraud and erode trust in payments and contracts	• Inflexible and costly legacy core systems • Dependency on centrally-paced ecosystem upgrades • Upgrade timelines dictated by vendor roadmaps • Complex third-party and cross-border dependencies • Maintaining high-availability uptime	• Prioritise a crypto-inventory to identify high-risk data and systems • Pilot hybrid PQC on high-value, long-confidentiality systems • Build crypto-agile architecture to enable a phased, dual-rail migration. • Embed PQC-ready clauses into all new vendor and bank contracts
Telecommuni-cations	Future decryption of harvested network traffic and forgery of signed software updates or commands, threaten control over critical national infrastructure	• Long network-equipment lifecycles result in slow upgrades • Must retrofit 5G without disrupting nationwide service • Multi-vendor reliance requires roadmap alignment • Awaits maturing of global protocol standards which should roughly happen between 2027 to 2028	• Mandate PQC-readiness and crypto-agility in all new network procurement • Prioritise migrating internal systems and operator-controlled network layers first • Coordinate with vendors and standards bodies to align PQC protocol rollouts
Healthcare	Future decryption of harvested patient data and forgery of medical records or device data create severe risks to patient safety and undermine clinical trust	• Public-private fragmentation and differing data rules—the gap the new national digital-health rollout aims to close • Legacy systems and constrained public budgets lacking crypto-agility • Zero-disruption-to-care limits rapid change and testing	• Prioritise an inventory of systems and devices to identify high-risk assets and vendor dependencies • Mandate crypto-agility in all new procurements to stop accumulating technological debt • Classify patient data by confidentiality lifetime to focus scarce resources on the most critical information

Source: BNM discussion paper on AI in the Malaysian Financial Sector, BNM Risk Management in Technology policy document, The Banker, Malaysia's Ministry of Communications, The Edge, The evolution of healthcare digitalization policies in Malaysia: A four-decade narrative review (1985-2025), PwC analysis

The solution exists. The challenge is implementing it

The technology for PQC migration already exists today, removing uncertainty around technical feasibility. This shifts the challenge firmly to implementation. While hurdles such as ecosystem interoperability, vendor dependency, and the need for crypto-agility remain, they are now issues of coordination and execution rather than innovation. In Malaysia, rapid digitalisation may amplify these complexities, but it also creates a timely opportunity for organisations to modernise architectures, strengthen partner alignment, and embed more agile, future-ready cryptographic foundations.

1 **Ecosystem interoperability**

Your security is only as strong as your partners'. A quantum-safe upgrade may not be effective if your vendors, suppliers, and service providers haven't made the transition. This makes PQC migration as much a coordination challenge as a technical one.

2 **Vendor dependency**

Most companies inherit their cryptograph through the products they buy. This means your migration timeline is heavily dependent on the product roadmaps of your vendors. In practice, you can only move as fast as your slowest critical supplier in the ecosystem.

3 **Building crypto-agility**

The goal isn’t just to replace today’s algorithms. It's to re-architect systems so cryptography is flexible and adapts with routine technology updates, instead of triggering a decades-long transformation programme.

What to do

A practical roadmap for PQC migration

Knowing the urgency and risk areas leads us to the final question: what is the required response? The most dangerous mistake that business can make is treating PQC migration as a swap of one algorithm for another—it is not.

PQC migration is a global-scale change to IT and operational technology that will likely span multiple leadership cycles in most large organisations. The new algorithms are not drop-in replacements: differences in key size, signature size, and performance ripple through protocols, libraries, hardware, and public key infrastructure (PKI), requiring careful planning and testing across the estate.

This is an ecosystem-wide activity, and where managed service providers deliver most of an organisation's IT, leaders must ensure those providers are migrating too. It's a whole-enterprise effort.

At a high level, the PQC journey comprises four stages. Detailed guidance from national frameworks and global standards bodies can help organisations put them into practice.

Stage	What it means	Why it matters
1 **Commit and identify**	Secure executive sponsorship and funding; run a discovery exercise to find out where cryptography is used across the organisation.	You cannot migrate what you cannot see. Discovery is rightly treated as the first milestone of any credible plan.
2 **Prioritise**	Focus first on systems with the most valuable or long-lived data, and on long-lived hardware.	Not all exposure is equal; sequencing by data confidentiality lifetime concentrates effort where it counts.
3 **Migrate**	Execute a phased transition, typically running classical and post-quantum cryptography side-by-side during a transition period.	Hybrid approaches preserve interoperability while the broader ecosystem catches up.
4 **Sustain**	Build crypto-agility: the capability to replace algorithms without interrupting a running system.	This is the durable end-state: every future cryptographic transition becomes a configuration change, not a crisis.

A successful migration is underpinned by good asset management, clear visibility into systems, and actively managed supply chains, all of which are matters of enterprise governance, not an isolated IT task.

A compliance cost can turn into a strategic investment

A crypto-inventory delivers immediate risk reduction by uncovering existing vulnerabilities like weak algorithms, mismanaged certificates, and shadow IT. This allows you to strengthen defences against current threats as you plan towards addressing PQC risks.

The path forward for business leaders

The main takeaway for business leaders in Malaysia is the need to begin preparing now. The national plan provides the roadmap, the risk of data harvesting creates the urgency, and the multi-year migration process defines the timeline, leaving little room for delay.

PQC is more than a security challenge. Organisations that start today and approach this as a strategic initiative will be better positioned to adapt to evolving risks and build long-term resilience for the decades ahead.

Awareness is the first step, but action is what matters

Here are five questions every Malaysian business leader should be asking now to test if their organisation is truly prepared for a post-quantum future.

01

Do we know where our cryptography lives?

Have we run a discovery exercise across IT, OT, cloud and third parties? You cannot migrate what you have not identified.

02

Who owns this—and is it funded as a multi-year programme, not an IT project?

Migration spans multiple leadership cycles and significant budget, so it needs sustained sponsorship beyond project-level funding.

03

What is our longest-lived sensitive data, and is it already being harvested?

Have we identified data that must stay confidential past 2035?

04

Have we written quantum-readiness into procurement and vendor contracts?

PQC migration is ecosystem-wide; signalling demand to suppliers now shapes the products that reach the market.

05

Are we aligned to the National PQC Migration Plan 2025–2030? Is this on the board's agenda?

Quantum risk should be incorporated into the enterprise risk register and tracked against the national timeline, supported by defined quarterly KPIs.

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than **364,000 people** in **136 countries** and **137 territories**. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

Contact us

Clarence Chan
Digital Trust and
Cybersecurity Leader,
PwC Malaysia
clarence.ck.chan@pwc.com

Tian Yi Woon
Cyber Threat Operation,
Senior Manager
PwC Malaysia
tian.yi.woon@pwc.com

Author

Alex Cheng
Director,
Cyber Threat Operations,
PwC Malaysia
alex.ct.cheng@pwc.com