consult hyperion
consulting by fime

Quantum resilience in payments: a 2026 strategic imperative.

REPORT

Author:

Raphael GUILLEY

November 2025

consult hyperion

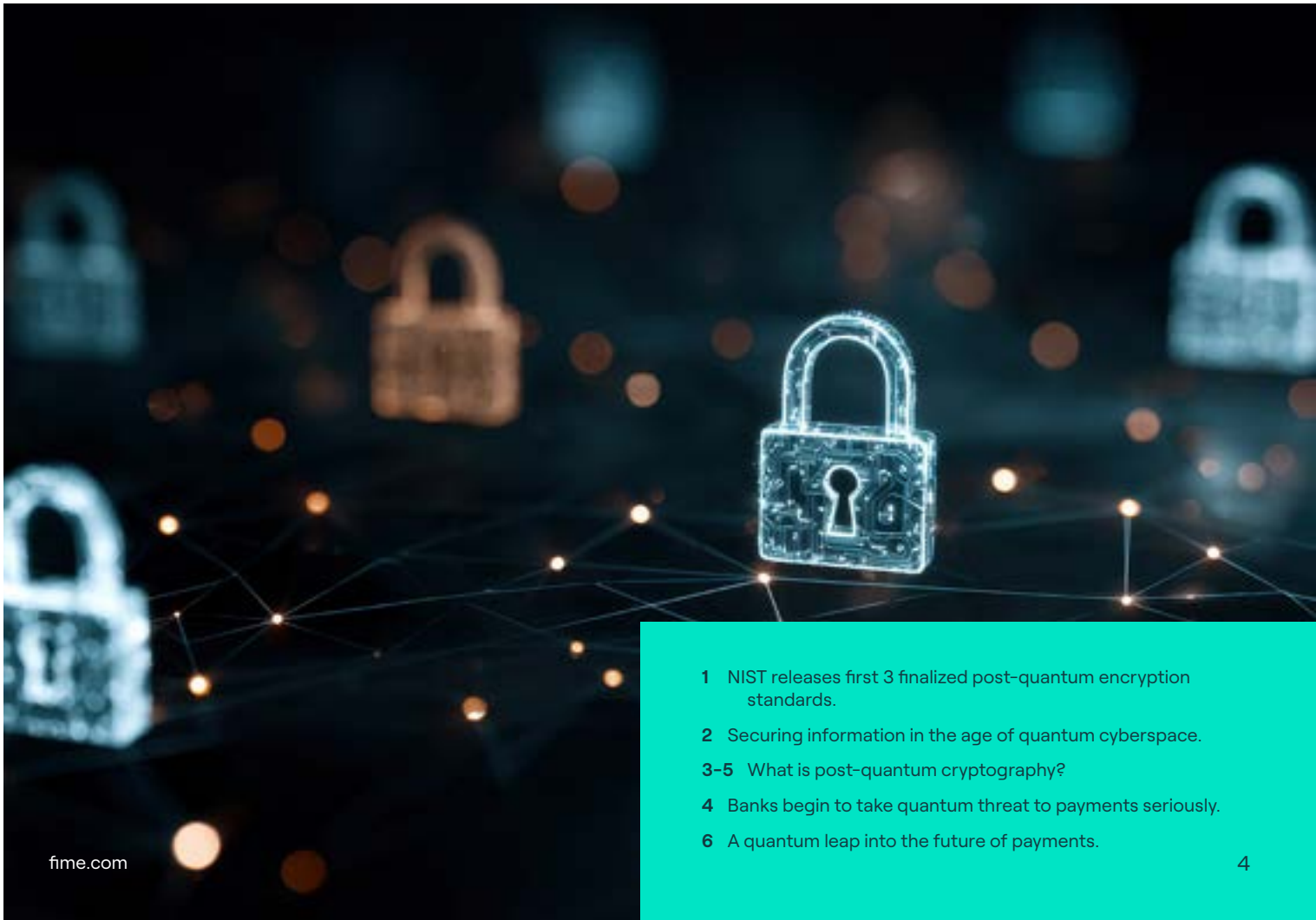
Table of contents

back to contents

1. Introduction.

In the wake of recent breakthroughs and warnings, the financial sector is waking up to a once-theoretical threat that is fast becoming tangible. The U.S. National Institute of Standards and Technology (NIST) has finalized new encryption standards built to withstand quantum attacks, urging organizations to **begin transitioning "as soon as possible"**[1]. At the same time, intelligence experts caution that hostile state actors and cybercriminals are **already harvesting encrypted financial data today** – storing it in hopes of decrypting it once quantum computers mature[2]. This convergence of technological progress and geopolitical risk has made **post-quantum cryptography (PQC)** a pressing issue for banks, payment schemes, and payment service providers (PSPs) worldwide.

Post-Quantum Cryptography (PQC) refers to new cryptographic algorithms designed to resist attacks from quantum computers as well as classical ones. It is not "quantum encryption" in a sci-fi sense, but rather traditional mathematical encryption **using problems that even quantum computers should find should find intractable**[3]. The need for PQC arises because quantum machines operate on fundamentally different principles, harnessing quantum physics to perform certain calculations astronomically faster than normal computers. For example, a sufficiently powerful quantum computer could factor the large prime-based keys underpinning RSA and ECC encryption **in a matter of days or hours**, a task that would take a classical supercomputer **millions of years**[4]. This means that the public-key cryptography securing everything from **online banking to payment networks** could be broken essentially overnight once a "cryptographically relevant" quantum computer comes online[5]. It's a looming **"Day Zero" threat** often discussed in security circles – the moment current encryption fails. And as one industry expert put it, that day might **arrive much sooner than originally thoughts**[6].



2. Why 2025 is a turning point.

The year 2025 finds the financial industry at an inflection point. Quantum computing advances are no longer academic news; they are **boardroom agenda items**. A recent industry briefing noted that quantum risk has rapidly evolved from a theoretical footnote to an **"urgent readiness challenge"** climbing the list of concerns for executives, regulators, and technology strategists. Two years ago, many in payments scoffed at PQC as irrelevant; today, skepticism is giving way to strategic action. "Many questioned if it was even relevant to the payments sector," recalls Camilla Bullock, CEO of Emerging Payments Association Asia. "It's no longer a theoretical risk, **it's a readiness challenge**"

Several developments in 2025 underscore why acting in 2026 is imperative. NIST's first PQC standards – including algorithms like CRYSTALS-Kyber for encryption and Dilithium for digital signatures – were published in final form, with NIST explicitly **encouraging system administrators to integrate them immediately.** These standards are the fruit of an eight-year global effort and mark the beginning of a new crypto era. At the geopolitical level, the **G7 Cyber Expert Group** of central bankers and finance ministries issued a report in late 2024 flagging quantum computing as both a potential boon and a grave risk to the financial system. The group **urged all jurisdictions to start planning for quantum threats**, to collaborate across public and private sectors, and to **raise awareness of the need for quantum-resistant technologies.** Notably, financial regulators have begun quietly querying banks on their quantum preparedness – a clear signal that guidelines or mandates could soon follow.

Perhaps most alarmingly, national security agencies warn that **adversaries are actively preparing**. Nefarious actors – from hostile nation-states to organized crime – are believed to be **intercepting and stockpiling encrypted data right now**, anticipating a future when quantum decryption will unlock today's secrets. This tactic, often termed **"harvest now, decrypt later,"** means that data breaches occurring now can lie dormant, only to erupt once quantum codebreaking becomes feasible. For the payments world, where data like transaction records, customer account details, and cryptographic keys underpin trust, this is a ticking time bomb. Any organization that delays upgrading its cryptography might discover in a decade that an adversary has a trove of its historical data ready to decrypt. **The window for proactive defense is narrowing.**

In short, 2025 is a watershed moment. **The tools to fight back (PQC standards)** are emerging and t**he threat timeline** – once estimated decades away – is continually being revised to sooner dates. This puts banks, payment schemes, and PSPs in a strategic race against time: act now to ensure resilience, or risk that within the next few years the foundations of digital security are yanked out from under the financial system.

3. Payment systems at risk: threats on the horizon.

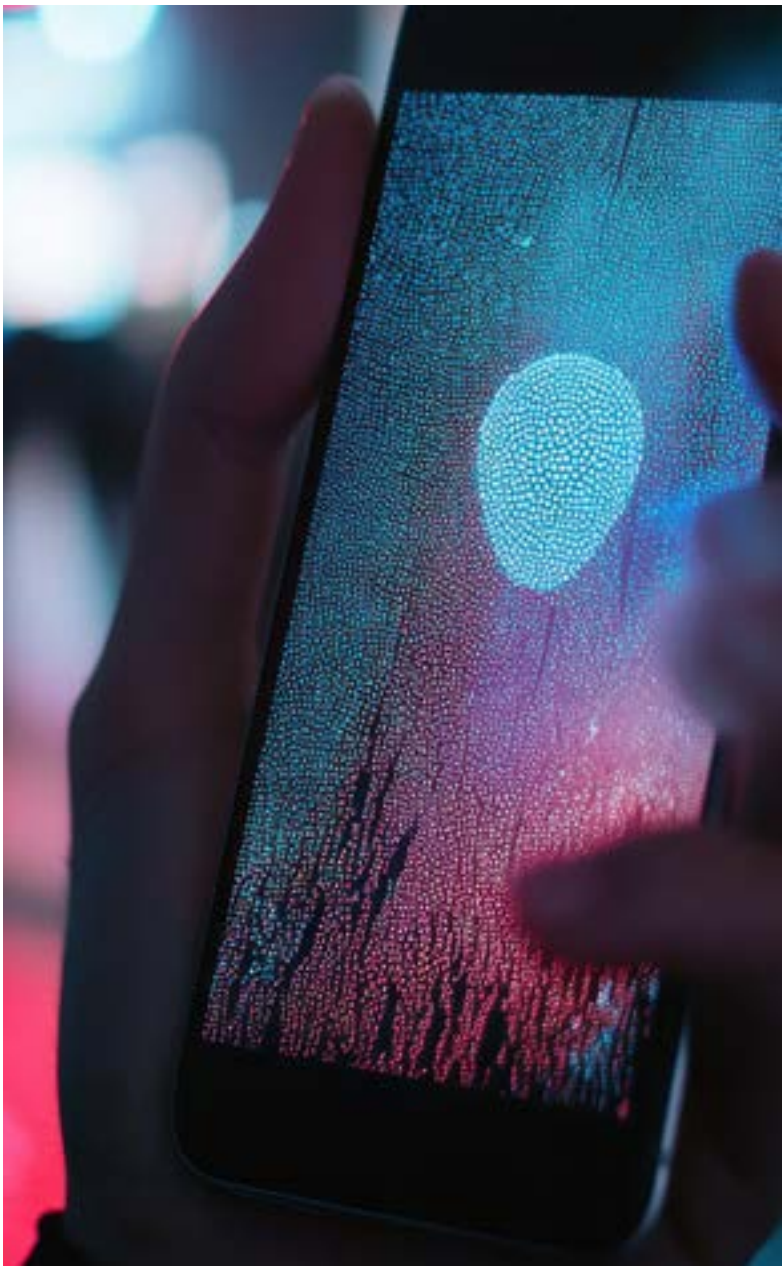
Why are payment systems particularly at risk from quantum attacks? The payments ecosystem relies deeply on cryptography – it is the invisible shield guarding every transaction, message, and digital signature. As quantum computing advances, **three key risk areas** stand out for banks and payment providers.

"Harvest now, decrypt later" attacks.

Payment data often retains value for years – think of interbank SWIFT messages, transaction logs, or customer PII linked to payments. Attackers know this, and some are **capturing encrypted traffic now** precisely because those ciphertexts may be readily decrypted in the future[7]. This threat is not hypothetical; it is **already occurring** according to intelligence reports. For example, a criminal group might harvest encrypted credit card authorization logs or VPN traffic from a bank today, store it, and then decrypt large volumes of sensitive information in five or ten years when a capable quantum computer is available. The consequences could range from massive privacy breaches to replaying transactions or impersonating secure communications retroactively. The existence of this "time capsule" attack vector is a prime reason experts say **systems need to start using quantum-resistant encryption as soon as possible** – waiting until quantum machines are here will **already be too late** for data we're transmitting in 2025.

Cross-Border Infrastructure Vulnerabilities.

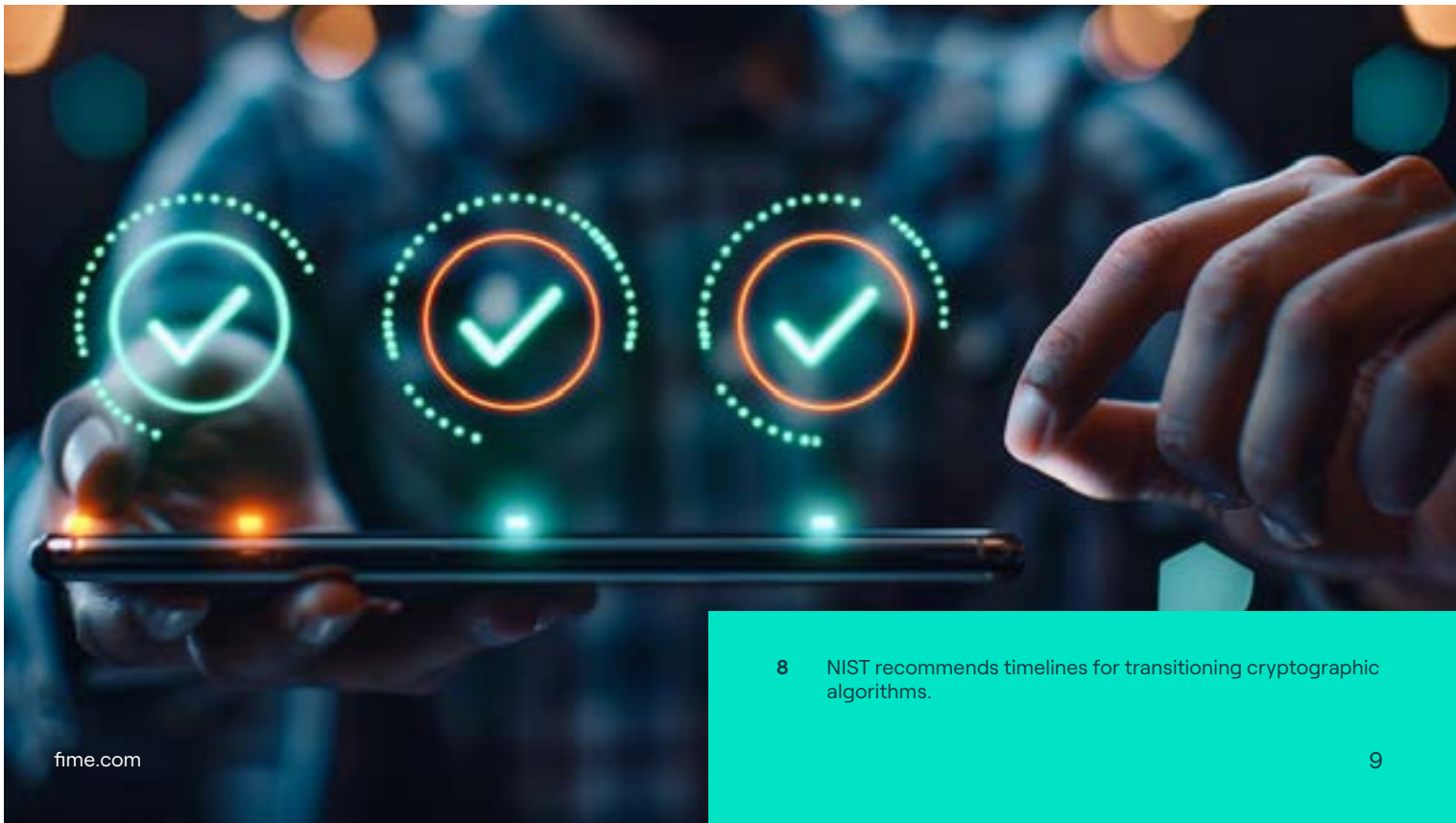
Payments are the **plumbing of global finance**, often spanning multiple countries and networks. This means vulnerabilities are shared – a weakness in one link can jeopardize the whole chain. For instance, a cross-border payment might travel through a domestic bank, a regional switching network, and the SWIFT global network. If any one of these has not upgraded its cryptography in time, a quantum-enabled adversary could target that weakest link to compromise the transaction. **Legacy encryption in one jurisdiction becomes everyone's problem.** The Bank for International Settlements (BIS) has highlighted quantum computing as one of the most important cyber threats to the financial system, warning it could **"expose all financial transactions and much of our stored financial data to attack"** if we don't act in advance. It's easy to imagine, for example, a scenario where encrypted payment orders between two countries are siphoned and decrypted by a third country's intelligence service, undermining not only security but also geopolitical trust. This is why **global coordination is critical**. International bodies like the **EU Agency for Cybersecurity and the G7** have called for joint efforts to avoid **regulatory gaps and asymmetries across countries** in PQC adoption. Payment systems are only as strong as their weakest participant; ensuring quantum resilience demands industry-wide and cross-border alignment.



Long-Term digital signature exposure.

The financial industry depends heavily on digital signatures for authentication and integrity – from signing payment instructions and legal contracts to code signing for banking software and devices. **Digital signatures, like those based on RSA or ECC, will be as vulnerable as encryption to quantum attacks.** The twist with signatures is that many signed artifacts need to remain trustworthy for years or decades. Consider a software update for a payment terminal or ATM: it might be signed today and installed across devices that won't all be replaced for 10+ years. If an attacker in 2030[8] can forge that signature (because the algorithm was broken), they could push malicious software into critical infrastructure. Similarly, many banking documents, customer agreements, or even blockchain transactions rely on digital signatures whose validity must persist. Industry experts have pointed out the need to **migrate code signing and authentication to quantum-resistant algorithms well before quantum day zero**, especially for devices and applications that will be in use in the 2030s. Another angle is certificate authorities and the TLS/SSL certificates securing online banking – these too have multi-year lifespans and must be made quantum-safe to prevent future impersonation of banking websites or payment gateways. The bottom line is that **long-lived trust** is at risk. Every digital certificate or signed record that isn't quantum-safe is a potential future forgery. Banks and payment schemes will need to re-issue and re-establish these trust anchors using PQC long before quantum computers arrive, a massive coordination effort in its own right.

In sum, the **threat landscape for payments** in the quantum era spans both the immediate tactical level (e.g. encrypted traffic being captured today) and strategic, long-term issues (e.g. the integrity of financial records and systems in a decade's time). It touches not only security and IT teams, but also enterprise risk, legal/compliance (consider the legal validity of signatures), and ultimately the **continuity of business operations**. David Piesse, an insurance technology expert, put it starkly: if we allow encryption to be broken by quantum computing, and fail to respond in time, **"we're all digitally naked"**. In other words, the protective layer enabling electronic finance would be stripped away, exposing everyone. No bank or PSP can afford to let that happen.



8 NIST recommends timelines for transitioning cryptographic algorithms.

4. The business case for quantum readiness: resilience, trust, and compliance.

For C-level executives and boards, quantum security is not just a technical issue – it is a **strategic business imperative.** Financial institutions that prepare early will safeguard not only their data, but their reputation and market position. Those that lag risk severe consequences. Here's why investing in PQC readiness makes compelling business sense.

Resilience and continuity of operations.

Banks and payment schemes form part of national critical infrastructure. A quantum-induced cryptographic collapse could lead to systemic outages – imagine if keys used in interbank payment clearing or ATM networks were suddenly compromised, transactions could halt. Preparing now by upgrading algorithms and building crypto-agility directly contributes to operational resilience. **Ensuring transaction systems continue to function securely in the face of new threats** protects revenue streams and prevents disruption to the economy. In contrast, an institution caught unprepared might face lengthy downtime, massive incident response costs, and even insolvency risk if trust in its systems evaporates. From a business continuity and disaster recovery standpoint, quantum risk mitigation is emerging as a **top priority for the next decade**.

Preserving customer trust and brand reputation.

Trust is the currency of banking. Customers, whether retail or corporate, entrust their money and sensitive information to financial institutions with the expectation of safety. A quantum-enabled breach – say, a scenario where a bank's historical transactions are decrypted and leaked, or fraudulent transactions spike because security was weak – would be a **nightmare for customer confidence**. The mere perception that a bank is not keeping up with security advances can become a competitive disadvantage. Conversely, proactively reinforcing systems with quantum-safe measures can be a **brand differentiator**. It sends a message to clients and partners that the institution is forward-thinking and vigilant about emerging risks. Just as banks that led on cybersecurity or fraud prevention earned market trust, so too will **quantum-resilient banks** be seen as safer havens. Early movers can even help educate the market, framing their quantum readiness as part of their value proposition of uncompromised security. In a digital economy, **losing trust is an existential threat** – maintaining that trust through the quantum transition is non-negotiable.

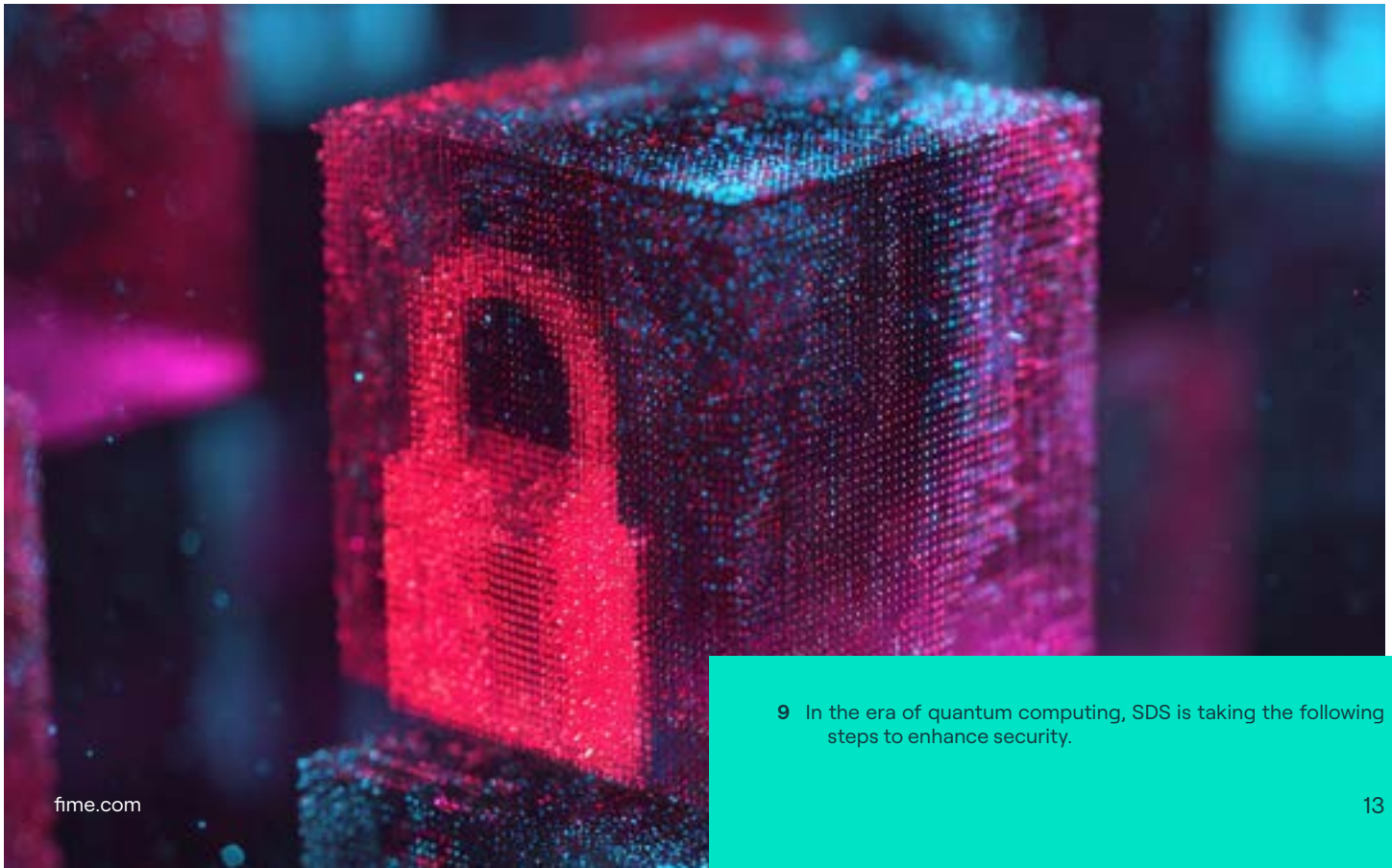
Regulatory and compliance drivers.

Financial regulators globally are increasingly aware of the quantum threat. As noted, the G7 cybersecurity experts have explicitly encouraged regulators to push for planning and awareness on PQC. In the United States, a National Security Memorandum (NSM-10) in 2022 set 2035 as the target for federal systems to migrate to quantum-safe cryptography and standards bodies like NIST have outlined a phased timeline calling for most legacy encryption to be deprecated by 2030 and replaced by 2035. It's reasonable to expect that banking regulators will follow suit with guidelines or requirements for financial institutions. Indeed, some bank examiners have already begun **asking institutions about their quantum preparedness** in supervisory meetings. We can anticipate regulations that might require quantum risk assessments, crypto-agility measures, or board-level reporting on transition plans. **Aligning with these emerging expectations early not only avoids non-compliance risk and penalties, but positions the bank as a leader and influencer** in any industry standards that develop. It's much better to help shape the rules through proactive engagement than to play catch-up under regulatory pressure.

Competitive and strategic advantage.

Beyond avoiding downsides, there is a forward-looking competitive angle. The advent of quantum-safe technology will spur new products and innovations – for example, quantum-safe digital identity verification, VPNs, or blockchain systems. Financial institutions that build expertise now can leverage that knowledge to develop new services or to partner with fintechs in the quantum security space. Think of quantum resilience as part of being a **"trusted innovator."** In payments, where new entrants and tech firms constantly challenge incumbents, being ahead on security can be a selling point. For instance, consider a payment gateway marketing itself as "quantum-secure end-to-end" – that could attract security-conscious clients in sectors like healthcare or defense. Also, institutions that delay may find themselves scrambling and spending more later, perhaps in a panicked transition when a breakthrough occurs. Early preparation is often more cost-effective and allows for deliberate, phased upgrades rather than hasty rip-and-replace. As Gartner has noted, **crypto-agility and PQC migration should already be among the top strategic tech trends in 2025**[9]. Those who treat it as a strategic opportunity can **outpace competitors** who see it as just another IT chore.

In summary, preparing for post-quantum cryptography is akin to buying insurance against an inevitable storm – but it's also more than that. It's an investment in the **future-readiness** of the organization. Much like banks that invested early in digital transformation were better positioned when online and mobile banking took off, banks that invest in quantum-safe security will be better positioned for the cryptographic upheaval ahead. Given the stakes – the integrity of every transaction and the confidentiality of every piece of customer data – **quantum resilience must be viewed at the highest strategic level.**



9 In the era of quantum computing, SDS is taking the following steps to enhance security.

5. Preparing today: concrete steps for quantum resilience.

Faced with this looming challenge, what should CxOs – from Preparing Today CIOs and CISOs to CEOs and board risk committees – actually do in 2026 to prepare? Transforming an established bank or payment scheme's cryptography is a complex endeavor that will span years. However, there are **practical steps that leaders can initiate right now** to set the foundation. The roadmap starts with assessment and strategy, moves through engagement and planning, and never loses sight of the evolving technology landscape.

Inventory cryptographic assets and data.

It is impossible to protect what you don't know you have. Thus, a comprehensive **cryptographic inventory** is essential. This means cataloging all the places where cryptography is used across the organization's applications, networks, and devices. **Identify every algorithm, key length, certificate, and cryptographic library in play** – from the TLS on your customer-facing websites to the VPN tunnels between data centers, from the algorithms in your HSMs (Hardware Security Modules) to the signing keys used for code and documents. The ABA Cybersecurity paper emphasizes building a clear inventory of assets and crypto use cases as the first step to identify risks and achieve crypto-agility. Pay special attention to two things: (a) **critical systems and high-availability** services, which likely have the most consequences and may need priority in upgrades; and (b) data with a long shelf life, which might still need protection 5, 10, or 20 years from now. For each system or dataset, ask: How long does this need to remain secure? If the answer extends into the 2030s, mark it as a candidate for early PQC migration. Also, engage your enterprise architecture and application owners to list out **external dependencies and vendor products** that perform encryption or authentication. Many risks will hide in third-party components – an off-the-shelf core banking system or a cloud service may use vulnerable crypto under the hood. Knowing these now allows you to put pressure on vendors (next step). Finally, don't ignore the **"shadow" cryptography** – outdated protocols or forgotten systems still enabled in your environment (for instance, an old TLS 1.0 endpoint or an SFTP server using RSA keys). Each identified item in this inventory should be assessed for quantum vulnerability. A useful exercise is to classify them: which rely on RSA/ECC or other quantum-vulnerable algorithms vs. which use symmetric crypto (which is more quantum-resistant but may need larger keys). This inventory and classification effort will directly inform your transition game plan, acting as the backbone of your **structured risk analysis** for quantum threats.

Perform a crypto-agility and risk assessment.

Begin with a frank evaluation of your organization's cryptographic readiness. **Crypto-agility** is the capacity to swap out cryptographic algorithms with minimal disruption, and it's quickly becoming a critical KPI for security architecture. Gartner defines crypto-agility as "the ability to enable rapid adaptations of new cryptographic primitives and algorithms without making disruptive changes to a system's infrastructure". CxOs should ask: How hard would it be for us to replace RSA with Dilithium, or ECC with a lattice-based scheme, in our core systems? If the answer is "very hard," then legacy systems or hard-coded algorithms are a liability. A crypto-agility assessment will identify where **rigid cryptography implementations** exist – for example, older payment switches, card authorization systems, or proprietary protocols that only support specific algorithms. This assessment should be tied into overall risk management: understand which systems and data would cause the biggest impact if current encryption failed. As Matt O'Keefe, cyber leader at KPMG, notes, the quantum threat spans business, technical, governance, and regulatory domains. Therefore, form a cross-functional task force (IT, security, risk, compliance, enterprise architecture) to collectively assess where you stand and what the priorities are. The output of this phase should be a high-level quantum risk register and a roadmap to enhance crypto-agility – essentially, a plan to **make your cryptographic systems nimble and prepared for change.**

Engage vendors and industry partners.

No bank or PSP is an island. Quantum-proofing the entire payment ecosystem requires coordination, and much of your technology stack is likely vendor-supplied. It is critical in 2026 to **start the conversation with all key vendors, partners, and service providers** about their PQC roadmap. Make quantum resilience a standing item in vendor due diligence and tech strategy discussions. For example, ask your core banking software provider or card processing switch vendor: Do you have a timeline to support NIST's post-quantum algorithms? Inquire with cloud providers and fintech partners how they plan to implement quantum-safe encryption for the services you use. The goal is twofold: **ensure your vendors are not the weak link**, and signal to the market that customers demand quantum-ready solutions. Some encouraging signs are already visible – a SWIFT executive recently revealed that SWIFT (the network underpinning global bank payments) has begun implementing a quantum-resistant encryption layer to protect its central messaging authentication, using third-party PQC algorithms. This shows that major financial infrastructure players are starting to move, but they need their member banks to come along. Industry collaboration groups can help: for instance, participate in the FS-ISAC's Post-Quantum Cryptography working group, which is sharing threat intelligence and best practices for the financial sector. By engaging in these forums, banks can pool knowledge on vendor solutions and even **influence standardization efforts**. Regulators too encourage this outreach – the G7 guidance explicitly calls for public-private collaboration in tackling quantum risks. In practice, engaging vendors in 2026 might also mean launching joint pilots or proofs-of-concept. If you rely on a payment gateway, you might partner with them to test a quantum-safe API in parallel to the current one. If you're a card issuer working with a network like Visa/Mastercard, coordinate on trials for quantum-safe keys in card personalization. Every conversation and joint effort now builds muscle memory for the bigger transitions ahead.

Monitor standards and plan controlled pilots.

The quantum security landscape is dynamic – new algorithms, implementation techniques, and standards will continue to emerge over the next few years. CxOs must ensure their organizations **stay in the loop** on these developments. Dedicate resources (or external consultants) to **track standardization updates** from NIST, ISO, the IETF, and local cyber agencies. For example, NIST will be releasing additional standards (like for alternative algorithms and hash-based signatures) through 2024-2025; staying aware of these helps you anticipate what to adopt. Likewise, guidance from bodies like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) or the European ENISA can provide actionable recommendations – make monitoring these a part of your security governance (the ABA recommends keeping an eye on NIST and CISA efforts as a basic action. While monitoring, organizations should also **experiment and pilot** with PQC in low-risk environments **sooner rather than later**. There is no substitute for hands-on experience to

discover integration challenges and performance impacts. For instance, consider setting up a test system that uses a PQC TLS library (several open-source implementations exist) between a front-end and back-end application, to observe any latency or compatibility issues. Some central banks have already done something similar: **Project Leap**, led by the BIS Innovation Hub with European central banks, tested quantum-resistant communication between the Bank of France and Deutsche Bundesbank, using a hybrid classical-and-post-quantum encryption approach. The project demonstrated that it's feasible to apply new quantum-safe schemes to real financial messages without breaking everything, but also highlighted that **operational unknowns remain** – such as impacts on real-time processing and system complexity. Banks and PSPs should take a page from this and run their own **PQC pilots in 2026**: for example, a payments switch could simulate clearing a batch of transactions signed with a Dilithium-based digital signature and measure verification times; a mobile banking app team could prototype a quantum-safe key exchange for its API calls. These trials will help identify issues early (maybe certain algorithms produce very large keys that strain legacy protocols, or require more CPU, etc.), allowing time to adapt. They also serve as excellent training for in-house talent. By 2026's end, your institution should aim to have a **PQC migration playbook** in draft form – outlining how you would transition each major system when the time comes, what the dependencies are, and who is responsible. That playbook will evolve, but starting it now forces the organization to grapple with practicalities rather than abstractions.

Adopt a structured risk management approach.

Lastly, as these steps are undertaken, it's vital to treat the quantum transition as a managed program with appropriate oversight. This is where proven methodologies like Consult Hyperion's **Structured Risk Analysis** (SRA) can be invaluable. SRA is a methodical approach to making security decisions driven by rational analysis rather than fear or guesswork. Often, investments in security fail to happen because the risk seems intangible – or the opposite, money is thrown at a problem due to panic. A structured approach cuts through these extremes. According to Consult Hyperion's whitepaper, SRA helps organizations "take rational steps to improve their information security" by balancing threat likelihoods, impacts, and costs[10]. In the context of PQC, an SRA framework would evaluate which assets are most at risk, which mitigations give the best risk reduction for the effort, and how to prioritize actions in alignment with business objectives. For example, SRA might reveal that a payment scheme's biggest exposure is in its interbank settlement messages – so resources should focus there first, perhaps by implementing a hybrid encryption solution as an interim step. Meanwhile, it might de-prioritize another area where data is ephemeral and low-sensitivity. This ensures **rational allocation of budget and time**, avoiding both complacency ("it will never happen to us") and blind panic spending. Executive leadership should demand such structured analysis as part of any major security transformation, and quantum resilience is no exception. Embedding the quantum roadmap into the enterprise risk management process will also elevate visibility – e.g., quarterly updates to the board on quantum risk status – which helps sustain momentum over what will be a multi-year journey.

10 Structured Risk Analysis (SRA) whitepaper.

By following these steps – inventory, assess, engage, monitor, pilot, and plan with rigor – financial institutions can move from vague awareness to concrete preparation. It's worth emphasizing that **very few banks have begun their transitions in earnest**; those reading this in 2025 have the opportunity to be frontrunners. The task may seem daunting (hundreds of applications and cryptosystems to eventually update), but it is achievable through phased, well-governed effort. As one payment CEO quipped, the challenge is like having to **"find and replace each instance of encryption"** across your operations – a painstaking process, yes, but one that can be systematically tackled. And with the right partners and frameworks, the journey can even become a source of innovation and strength.

6. Conclusion: from imperative to opportunity.

The coming quantum revolution has been described as a threat and a menace to today's cryptography – all true. But with foresight and leadership, it can also be the catalyst for building **next-generation security and trust** in the financial system. The strategic imperative for banks, payment schemes, and PSPs is clear: **start now, or risk being too late**. As we've seen, the timeline to quantum supremacy is uncertain, but the prudent assume a worst-case sooner scenario, especially given experts warn a quantum codebreaker could appear within a decade. Waiting until a cryptanalytic breakthrough is in hand of adversaries is not an option; by then, everything encrypted in prior years would be vulnerable. Inaction or delay is essentially **gambling with the institution's future**.

On the brighter side, those who act decisively will not only avert disaster, but stand to differentiate themselves. In an industry built on trust, **quantum resilience may become a competitive benchmark** – much like banks are rated on their cyber defenses today. The transition to PQC, though challenging, is also an opportunity to modernize infrastructure, improve agility, and perhaps even gain efficiencies (the new algorithms, for instance, have different performance profiles that could be leveraged in creative ways). It's a chance to re-architect security with a 20-year horizon in mind, which ultimately strengthens the digital ecosystem for all.

Financial institutions don't have to navigate this path alone. The complexity of cryptography migration and the evolving standards landscape make expert guidance invaluable. This is where firms like **Consult Hyperion** position themselves as trusted guides. Consult Hyperion's pedigree in securing **mass-market transaction systems – from national ID cards to global payment networks** – provides deep experience in marrying long-term security planning with practical implementation. As a consultancy at the forefront of payments and digital identity, we understand the interplay of technology, business, and compliance demands. Whether it's conducting cryptographic audits, devising enterprise-wide crypto-agility blueprints, or running pilot implementations in a Hyperlab environment, our approach is to ensure clients are not just protected but poised to thrive in the quantum age. We've helped design and stress-test the security for contactless payments and smart ticketing in major cities; now, we're helping clients map out their **quantum readiness frameworks** – so that the systems rolling out today will remain secure tomorrow.

The call to action for CxOs is unequivocal: make quantum resilience a pillar of your strategic agenda. Allocate the budget, empower your teams, and press your partners into action. Foster a culture that views security innovation (like PQC) as an enabler of business integrity and growth. Challenge your organization with provocative scenarios – What if an adversary could decrypt our last 10 years of transactions? – and let the answers drive urgency. As you do so, remember that preparing for the quantum future is not just defensive; it's about preserving the hard-won trust of your customers and the stability of the financial system itself. In the words of a payments veteran reflecting on industry evolution: "The technology now exists to do better, so we need to do better". Quantum computing may rewrite the rules of cryptography, but with preparation, i**t does not have to undermine the foundations of digital finance**. By acting now, banks and payment providers can ensure that when the quantum clock strikes, they are **ready – fortified, agile, and confident** – having turned a daunting challenge into yet another chapter of successful innovation in the payments industry.

Author:

Raphael GUILLEY
SVP Consulting
Consult Hyperion, Consulting by Fime

Raphaël has over 20 years of experience in the consulting industry, with extensive involvement in managing large-scale international projects across payments, smart mobility and digital identity. His areas of expertise include product management, agile development and product launches.

At Fime, Raphaël leads the global Consulting team under the Consult Hyperion brand, following Fime's acquisition of the company. He supports a wide range of stakeholders, including payment networks, financial institutions and transport operators, to solve complex challenges, explore new opportunities and expand into new markets.

Prior to joining Fime, Raphaël was VP of Risk & Compliance Solutions at IPC Systems Inc. He also worked in similar roles for Etrali Trading Solutions and Orange Business Services.

consult hyperion

consulting by fime

About Consult Hyperion

Consult Hyperion is an independent strategic and technical consultancy, specializing in the design and implementation secure electronic transactions. We help financial services and government organizations around the world exploit new technologies to secure electronic payments, digital ticketing and digital identity services. We offer advisory services, technical consultancy and testing and development services using a practical approach and expert knowledge of relevant technologies.

Consult Hyperion is part of the Fime group.

www.chyp.com