Guidehouse®

outwit complexity™

# Securing the Future with Quantum-Safe Cryptography

## How financial institutions can proactively and comprehensively safeguard vital data and functions

As the widespread use of quantum computing edges closer, the financial services industry stands at a crossroads. This technological revolution, while promising groundbreaking advancements, also poses a formidable challenge to the foundations of modern cybersecurity. With their unprecedented processing power, quantum computers will inevitably render current cryptographic systems obsolete, potentially exposing a host of underestimated data security risks.

For financial services companies in particular, this transition represents a significant material risk. For these trusted custodians of vast amounts of personal data, protecting sensitive information is paramount. Therefore, the immediate need to begin a migration toward environments deemed “quantum-safe” should be a high priority for financial services companies.

Post-quantum cryptography isn’t just a technical capability upgrade, but a strategic imperative for the longevity and resilience of financial services firms in an evolving digital landscape. It represents the next identified frontier in data security, designed to withstand the cryptographic assaults powered by quantum computing.

This stark reality necessitates immediate action from financial services companies to safeguard their clients’ data and maintain their trust when “Q-Day” (the day quantum computers become powerful enough to break the encryption algorithms that currently secure our digital communications) arrives.

## Quantum computing and its implications

Quantum computing represents a paradigm shift in computational power and problem-solving capabilities. Unlike classical computers, which use bits to process information in binary form (0s OR 1s), quantum computers leverage the principles of quantum mechanics to process data in qubits (0s AND 1s). Qubits can exist simultaneously in multiple states (a phenomenon known as superposition) and can be entangled. This allows quantum computers to perform many calculations simultaneously, thereby solving complex problems exponentially faster than classical computers. Quantum computing will likely also be the “super-brain” powering the next generation of AI once both are at scale.

Some technologists and scientists currently estimate that quantum computers will break widely used encryption algorithms, including RSA (Rivest–Shamir–Adleman) and ECC (elliptic-curve cryptography), by the end of this decade. These are the foundational methods of encryption securing large amounts of digital communications and data today. IBM has reported that it is on track to deliver a fault-tolerant, error-corrected quantum computing system by 2029.[1] With that in mind, the urgency of transitioning to quantum-safe cryptography can't be overstated.

Quantum computing represents a paradigm shift in computational power and problem-solving capabilities.

## What is post-quantum cryptography?

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to be secure against the capabilities of quantum computers. These algorithms employ mathematical problems that are believed to resist quantum-driven attacks. Examples include lattice-based, hash-based, and code-based cryptography. Post-quantum cryptography aims to develop and implement encryption methods that will withstand the advanced processing power of quantum computers, ensuring the continued protection of even the most sensitive information considered quantum-safe.

Financial services companies of all sizes handle vast amounts of personal, financial, and health-related data, making them prime attack targets. By proactively adopting post-quantum cryptography safeguards, companies can protect their data assets, comply with emerging regulations, and maintain their reputation as trusted custodians of even the most sensitive client information.

## The state of quantum computing today

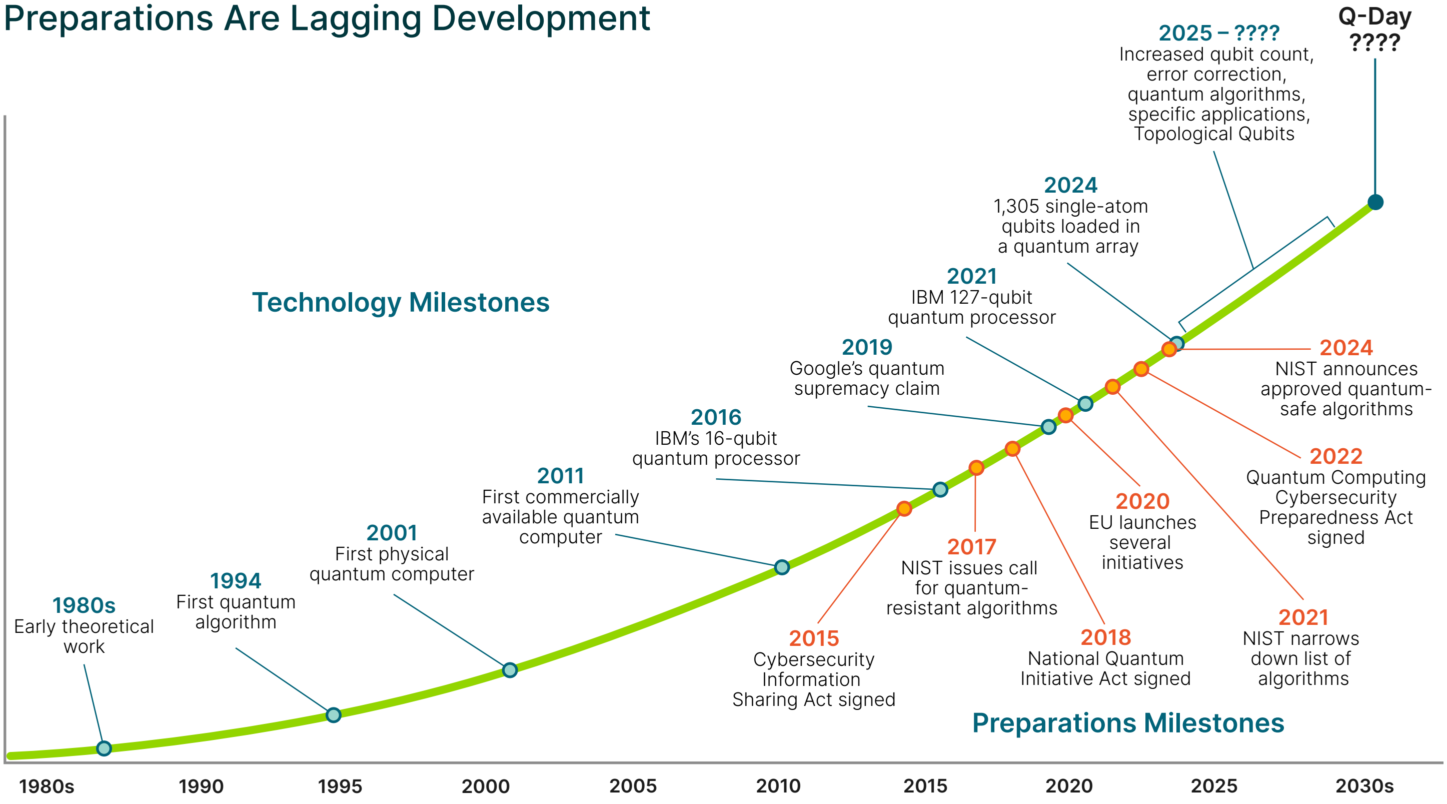
Today, quantum computing is in a stage of rapid development, with significant advancements made by leading technology companies and research institutions. Key players including IBM, Google, and Microsoft, along with startups such as Rigetti Computing and D-Wave Systems, have developed functioning quantum computers. While these quantum computers have demonstrated remarkable potential, their performance relative to traditional computers remains limited by several factors, including qubit coherence time, error rates, and scalability.

Current quantum systems are bulky and require extremely low operating temperatures, posing significant technical and environmental challenges. It may take several years to overcome these limitations and achieve large-scale, fault-tolerant quantum computing capable of breaking contemporary cryptographic algorithms. Or, given the material progress made in the last two years in qubit power, the threat to current encryption methods may be sooner than many organizations currently believe.

Recently, Microsoft unveiled its Majorana 1 quantum chip – a topological processor that leverages a novel state of matter to significantly improve qubit stability and scalability. Unlike traditional superconducting qubits that suffer from short coherence times and high error rates, Majorana 1's "topological" qubits are inherently more stable, with built-in error resistance at the hardware level. This breakthrough underscores the pressing need to advance post-quantum cryptography (PQC) frameworks, as more scalable quantum systems could compromise conventional encryption methods sooner than anticipated. For financial institutions, such developments intensify the urgency of quantum security preparations, with experts warning that the timeline for quantum threats is accelerating and organizations must begin implementing quantum-safe measures now.

[1] The Wall Street Journal, "'Q Day' Is Coming. It's Time to Worry about Quantum Security."

## Preparations Are Lagging Development



## Is Y2Q the next Y2K?

Some IT organizations believe quantum-safe cryptography's data security vulnerability is similar to the Y2K risk profile, which prompted companies to scramble in the last few years of the prior century to solve a problem that may or may not have existed. These professionals believe a risk from quantum computing may be on the horizon, but they still have time.

Others more familiar with the details of quantum-safe cryptography are closely following National Institute of Standards and Technology (NIST) guidance, which is driving the regulations and requirements that many of the largest firms will likely have to operationalize in the next 24 months. At present, there is no precise date as to when a quantum computer, sufficiently scaled and in the hands of a bad actor, will start cracking the current encryption algorithms. However, organizations should nonetheless consider several crucial points:

**Vulnerability is a problem *now*.** Deploying our current public key cryptography infrastructure took almost two decades. Depending on the changes needed, implementing the next one could also take many years. Without a definite date when this threat will be realized, IT organizations should be preparing now. The importance of this preparation can't be stressed enough. Some data has a long shelf life and may already be compromised. The practice of "harvest now, decrypt later"—whereby cyber criminals or rogue nation-states hack and gather massive amounts of encrypted data and store it, waiting patiently until quantum computers are available for decryption—is likely already a factor. Much critical enterprise data, including schematics, formulae, algorithms, and trade secrets, has a long shelf life. In addition, the base PII (personally identifiable information) included in client/customer data, such as Social Security numbers and health information, should be protected for that client's lifetime at minimum.

**Federal agencies are now actively getting ready.** In December 2022, President Joe Biden signed into law the Quantum Computing Cybersecurity Preparedness Act, which forces all federal agencies to develop plans to transition their systems to post-quantum encryption standards capable of surviving the arrival of Q-Day.

**It's not just about security.** As awareness of Q-Day trickles down to the public at large, touting post-quantum cryptography standards could become a differentiator in the marketplace.

## Specific vulnerabilities for banks and insurance companies

The potential threat of a quantum computer attack on a financial services company cannot be overemphasized. The consequences of the resulting loss of customer data would be catastrophic. Customer trust, the cornerstone of any financial institution, would also be severely compromised or shattered. The reputational damage would be immense, leading to the loss of business, legal repercussions, and a significant decline in market value. In an industry where reputation is everything, the fallout from a quantum computer attack could be irreparable. Here are some specific areas that need urgent attention:

**Client data security.** Financial services companies store vast amounts of personal data, including Social Security numbers, addresses, and financial information. If adversaries intercept and store this data today, massive privacy breaches will ensue once quantum computers gain decryption capacities.

**End Point Devices (IoT).** Many IoT devices currently use potentially vulnerable encryption keys to secure data transmissions. Without appropriate quantum safe security measures in place, payment terminals, ATMs, and other IoT devices used to transact huge volumes of business every second could be at risk for material data breaches, or worse.

**Claims processing and policy management.** Claims-processing systems and policy management platforms depend on secure encryption to maintain data integrity and confidentiality. Quantum computers could easily penetrate system encryption and allow unauthorized access to claims-processing systems, resulting in fraudulent processing, payment redirection, or worse.

**Third-party vendor security.** Financial services companies often work with third-party vendors for various services, including data storage, analytics, and IT support. If these vendors don't adopt quantum-safe encryption, the supply chain becomes vulnerable to quantum computer-driven attacks. A breach at a third-party vendor could expose sensitive data, even if the primary company's systems are secure.

**Long-term data confidentiality.** Financial services companies must protect data that will remain valuable for decades, such as loan application data, long-term policyholder records, and claims histories. Quantum computer-driven decryptions threaten the confidentiality of this historical data, potentially exposing it to future decryption attacks. If stolen and eventually decrypted, any of this data could lead to significant privacy violations and legal repercussions.

## Vital next steps

To ensure data security and maintain industry leadership, companies must take decisive action today to address the looming threat of misapplied quantum computing power against current cryptographic systems. Transitioning to quantum-safe cryptography requires a comprehensive, phased approach that addresses immediate vulnerabilities while laying the groundwork for long-term security and resilience. Companies can proactively protect their data and ensure continued compliance and trust in an increasingly uncertain technological landscape by implementing a strategic plan addressing short-term awareness and assessment, medium-term transition and implementation, and long-term resilience and readiness.

## Short-term actions: Laying the foundation

In the short term, financial services companies must focus on raising awareness, conducting risk assessments, and beginning their journey on the Quantum Readiness Roadmap (QRR).

- Start by educating key employees at all levels throughout the organization about the risks posed by quantum computing and the importance of quantum-safe measures.
- Conduct a comprehensive risk assessment to identify the most valuable data to safeguard under the organization's cryptographic strategy.

- Begin an inventory of all encrypted assets and assess encryption requirements against the organization’s risk landscape. This includes everything from data at rest in databases to data in transit across communication channels.
- Establish a cross-functional team involving leadership, IT, cybersecurity, compliance, and legal departments to develop a strategic plan for transitioning to quantum-safe cryptography.

Companies should embed quantum-safe practices into their core operations and continuously monitor the evolving quantum landscape.

## Medium-term goals: Transition and implementation

In the medium term, the focus should shift toward integrating quantum-safe cryptographic algorithms into existing systems.

- Begin by prioritizing the most critical systems and data that need protection, then implement post-quantum cryptographic solutions such as lattice-based, hash-based, and code-based algorithms. NIST recently selected three algorithms based on these methods, and Federal Information Processing Standards (FIPS) for these algorithms were published in August 2024. Pilot these solutions in non-critical environments to ensure they function correctly and efficiently.
- Collaborate with vendors and third-party service providers to ensure that they adopt quantum-safe practices, securing the entire supply chain.
- Update policies, procedures, and documentation to reflect the new cryptographic standards and ensure compliance with emerging regulatory requirements.

During this phase, investing in ongoing training for IT and cybersecurity staff is crucial to effectively handling the new cryptographic technologies. This will ensure that the organization remains nimble and can quickly adapt to future quantum computing developments.

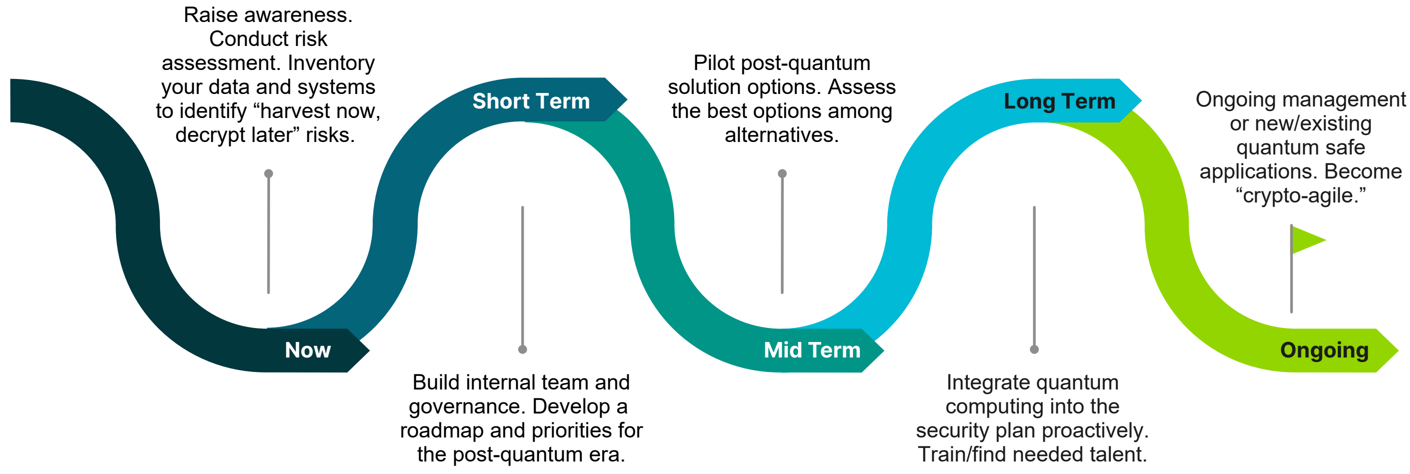
## Long-term strategy: Become crypto-agile

In the long term, companies should embed quantum-safe practices into their core operations and continuously monitor the evolving quantum landscape.

- Establish a long-term strategic roadmap that includes regular reviews and updates to cryptographic protocols as new quantum-safe algorithms and standards emerge.
- Invest in research and development to stay ahead of technological advancements.
- Consider partnerships with academic institutions and industry consortia focused on quantum computing and cryptography.
- Foster a culture of innovation and data security within the organization, encouraging continuous improvement and adaptation to new threats and opportunities.
- Develop a robust incident response plan tailored to potential quantum-driven breaches, ensuring that the organization can respond swiftly and effectively if needed. Regularly test and update this plan to maintain preparedness.

By taking these proactive steps, companies can reinforce data security, strengthen customer trust, and position themselves as leaders in the secure digital landscape of the future.

## PQC — A Path Forward



Now

Raise awareness. Conduct risk assessment. Inventory your data and systems to identify “harvest now, decrypt later” risks.

Short Term

Build internal team and governance. Develop a roadmap and priorities for the post-quantum era.

Mid Term

Pilot post-quantum solution options. Assess the best options among alternatives.

Long Term

Integrate quantum computing into the security plan proactively. Train/find needed talent.

Ongoing

Ongoing management or new/existing quantum safe applications. Become “crypto-agile.”

The advent of quantum computing heralds unprecedented opportunities and significant challenges, particularly for financial services companies. By understanding the immediate and future threats posed by quantum computers to current encryption methods, companies can take proactive measures to transition to quantum-safe cryptography. The importance of preparing for a post-quantum world extends beyond theoretical risks. The timeline for quantum supremacy is uncertain, but the potential for overnight vulnerability means that companies must act now.

Procrastination in adopting quantum-safe measures could lead to unprecedented breaches, regulatory penalties, and a loss of customer confidence that could take years to rebuild. By proactively recognizing and embracing quantum-safe cryptography, financial services companies can protect their data assets, comply with emerging regulations, and position themselves as leaders in technological innovation and security.

## Guidehouse can help

Guidehouse Consulting is uniquely positioned to guide your organization toward becoming quantum-safe across all technology systems. Our comprehensive approach includes inventorying your cryptographic assets, conducting full-scale risk assessments, and prioritizing and managing remediation efforts. We meticulously assess your critical systems end-to-end and establish a robust roadmap that instills confidence for your leadership, staff, and clients.

### Contacts

Jeff Zych, Partner
jzych@guidehouse.com

Nicole Turner, Partner
nturner@guidehouse.com

Dr. Murthy Rallapali, Consultant
mrallapali@guidehouse.com

### About Guidehouse

Guidehouse is a global consultancy providing advisory, digital, and managed services to the commercial and public sectors. Purpose-built to serve the national security, financial services, healthcare, energy, and infrastructure industries, the firm collaborates with leaders to outwit complexity and achieve transformational changes that meaningfully shape the future.

guidehouse.com/industries/financial services   linkedin.com/showcase/guidehouse-financial-services   @GHTechSolutions