DODGING QUANTUM CURVEBALLS: A PLAYBOOK FOR CRYPTO AGILITY IN CRITICAL INFRASTRUCTURE

by

CHELSEA LYNN ATKINS

B.S., Middle Georgia State University, 2020

M.S., Middle Georgia State University, 2021

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2025

Dodging quantum curveballs: a playbook for crypto agility in critical infrastructure

Chelsea L. Atkins, *Middle Georgia State University,* chelsea.atkins@mga.edu

Abstract

The rise of quantum computing presents a significant threat to traditional encryption, making proactive post-quantum cryptography adoption necessary. This study examines the barriers and facilitators of PQC readiness in critical infrastructure sectors. Through qualitative analysis, this research proposes a 7-phased post-quantum cryptography adoption framework to guide organizations in mitigating risk and ensuring a smooth transition.

Keywords: quantum computing, post-quantum cryptography, crypto agility, critical infrastructure

Introduction

As quantum technology continues to advance, it is crucial for organizations, particularly those in critical infrastructure sectors, to prepare for its disruptive potential. The ability of quantum computers to quickly solve mathematical problems poses a serious threat to traditional public key cryptographic methods such as RSA and ECC, which are highly vulnerable to attacks using quantum algorithms, such as Shor's Algorithm (Cheng et al., 2024). Critical infrastructure sectors, such as energy, finance, transportation, and public safety and defense, are especially vulnerable because they rely on secure communications and data protection to maintain the safety, stability, and economic well-being of society. The consequences of failing to prepare for quantum threats are immense, potentially leading to widespread data breaches, sabotage of operational systems, and risk to national security (Oliva del Moral et al., 2024).

While skeptics may argue that the timeline for quantum computing's practical use is uncertain, the potential impacts are too significant to delay preparation. The concept of "Harvest Now, Decrypt Later" further proves the urgency, as threat actors can steal and store sensitive data now with the intention of decrypting it once quantum computers become available (Ott et al., 2022). Post-quantum cryptography (PQC) is emerging as a necessary replacement for vulnerable cryptographic systems that currently support authentication, secure communications, and data protection for millions of organizations globally (Ott et al., 2022). The National Institute of Standards and Technology (NIST) led efforts to address this transition by releasing PQC standards in August 2024, including ML-KEM, SLH-DSA, and ML-DSA, which provide quantum-resistant cryptographic solutions (NIST, 2024). These suggested algorithms are designed to withstand early quantum attacks; however, many organizations, particularly those with limited resources like community banks or small service providers, will struggle with implementing these new standards into their systems securely.

Given the heightened risk that quantum computing poses to critical infrastructure, these sectors make an ideal focus for studying quantum readiness. However, while quantum experts and government agencies stress the importance of PQC adoption, there is a lack of actionable steps towards PQC implementation. This study explores how critical infrastructure sectors perceive quantum threats, assess their preparedness, and identify key barriers that prevent early adoption. By examining readiness gaps and organizational challenges, this research will contribute to a conceptual framework that helps organizations navigate the complexities of adopting quantum-resistant practices. Since the stakes are high, from potential large-scale service disruptions to national security threats, guidelines and insights gained from studying critical infrastructure can serve as a model for other organizations, including smaller businesses and those in less critical sectors.

Despite NIST's efforts to develop and publish PQC standards, there is limited understanding of how industries are preparing for their adoption. While larger organizations may have the resources to prepare, smaller organizations may face significant, cost-extensive challenges. This research aims to explore the perceptions and challenges that influence quantum readiness.

This research seeks to answer the following questions:

> **RQ1**: How do organizations in critical infrastructure sectors perceive and approach quantum readiness in the context of emerging quantum computing threats, and what factors influence their preparedness to adopt NIST's post-quantum cryptographic standards, particularly in terms of crypto agility?
>
> **RQ2**: What challenges and barriers prevent critical infrastructure sectors from transitioning to post-quantum cryptography, and how do these organizations assess or anticipate navigating these challenges over time?
>
> **RQ3**: What strategies, best practices, and resources could help critical infrastructure organizations enhance their quantum readiness and crypto agility, and how do these strategies evolve as organizations gain awareness and encounter industry-wise shifts?
>
> **RQ4**: How do decision-makers in critical infrastructure sectors conceptualize and prioritize risks associated with quantum computing, and what external factors (e.g. regulations, collaborations, funding) could drive or accelerate their transition to quantum-resistant practices?

This study seeks to study the perceptions of cybersecurity experts, cryptographers, and other technology stakeholders as they begin to discuss and plan a transition to these quantum-resistant algorithms within their organizations. By analyzing these perceptions, this research seeks to develop a practical framework that promotes crypto agility, counters decision-making barriers, and lays the groundwork for effective PQC adoption.

Review of Literature

Quantum Computing Threats

Threats to Public Key Encryption

In 1994, Peter Shor developed an algorithm that a quantum computer could use to factor a large number into prime numbers quickly. This later became known as Shor's Algorithm (Cheng et al., 2024). In traditional methods of asymmetric cryptography, security is dependent on mathematical complexities. Thanks to Shor's Algorithm, quantum computers can use a public key to deduce the private key in a condensed amount of time, ultimately rendering methods of asymmetric key encryption useless (Vaishnavi & Pillai, 2021). NIST's new standards, ML-KEM, SLH-DSA, and ML-DSA are considered resistant to the capabilities of early quantum computers, which will initially lack the qubit capacity to tackle highly complex mathematical problems. However, as more advanced quantum computers are developed with higher qubit capacity, these algorithms, along with those with long bit key lengths like RSA-2048, can become vulnerable to quantum attacks. A 2023 Global Risk Institute report presented a survey of 37 quantum experts. The survey indicated that a quantum computer capable of breaking RSA-2048 in a 24-

hour timeframe was likely to occur within 15-20 years (Mosca & Piani, 2023). This survey emphasizes the need for quantum readiness and crypto agility as stronger encryption standards are introduced.

Harvest Now, Decrypt Later

The phrase "Harvest Now, Decrypt Later" describes the storage of stolen data by a threat actor until a time when a quantum computer becomes accessible. This concept operates under the assumption that the stolen data contains information that remains constant or retains its value over a long period, such as social security numbers, trade secrets, or biometric data (Ott et al., 2022). By transitioning to quantum-resistant encryption earlier rather than later, organizations can ensure that even if their sensitive data is stolen, it remains secure in the long term.

NIST's Post-Quantum Standards

PQC standards include code-based, hash-based, lattice-based, and isogeny-based systems that have demonstrated resistance to known types of quantum attacks. While these methods are compatible with current cryptographic methods, they may face vulnerability in the future as new quantum computers are developed and PQC algorithms become too advanced for classical methods (Baseri et al., 2024). NIST's publication of ML-KEM, SLH-DSA, and ML-DSA algorithms in August of 2024 encourages organizations to begin transitioning to these new standards as soon as possible. The standards provided include the encryption algorithms' computer code, instructions for implementation, and their intended applications (NIST, 2024).

Quantum Readiness in Infrastructure

Despite the answer sheet being provided, many organizations may not appreciate the risks that quantum computers represent or still have a lot of work to do to prepare for them. Mosca and Mulholland (2017) suggest that organizations can calculate quantum risk by adding the lifetime of their assets ("x") to the time it would take for migration ("y"). The sum is then compared to the estimated time it would take threat actors to gain access to quantum technology ("z") to create the formula "x + y >\< z". If "z" is greater than the sum, then the organization can conclude they are at a lower risk of a quantum attack occurring before assets can be protected. If "z" is less than the sum, then the organization may be at a much higher risk of a quantum attack occurring before assets can be protected. Although Mosca and Mulholland's risk assessment provides a great foundation for organizations to consider, critical infrastructure sectors encounter even greater risks that must be taken into account.

Industrial control systems (ICS) are systems that are used to monitor, control, and automate industrial processes in critical infrastructure sectors like energy, transportation, and water treatment. ICS have an extended use lifetime, are difficult to update with different encryption algorithms, and usually require a complete replacement when issues arise (Vermeer et al., 2023). A significant case study of this kind of attack was the Stuxnet worm in 2010, which was designed to target the ICS working on the Iranian uranium enrichment program. Reports suggested that there was a 23% decline in centrifuges in the Natanz facility after the attack, delaying the production of Iran's nuclear energy (Farwell & Rohozinski, 2011). ICS systems are integral to many critical infrastructure sectors. If they are not properly prepared with post-quantum cryptographic solutions, they present a significant risk to societal functioning and public safety, such as widespread economic losses, compromised public health, and even loss of life.

Another significant concern in critical infrastructure is the impact that quantum computing will have on the payment industry. Automated Teller Machines (ATMs), Europay, Mastercard, and Visa (EMV) chip cards, contactless payments, and point-of-sale (POS) machines are just a few of the many components within the financial sector that rely on public key encryption algorithms for secure transactions. FS-ISAC reports that over 20 billion devices in the financial industry will need to be migrated to PQC (FS-ISAC, Inc., 2025). The Automated Clearing House (ACH) is cited by Nacha (2024a), the organization responsible for managing it, to have processed 33.6 billion payments totaling $86.2 trillion in 2024, making ACH one of the largest payment systems in the United States. ACH is most well known for the direct deposit of payroll, social security benefits, and tax refunds (Board of Governors of the Federal Reserve System, n.d.). The ACH network symbolizes a critical component of the U.S. financial industry, showcasing the potential for widespread disruption due to a cryptographically relevant quantum computer's ability to compromise its encryption methods (Asenjo et al., 2022; Nacha, 2024b).

Cryptographic Agility

Cryptographic agility refers to the ability to rotate different cryptographic algorithms. As new algorithms are introduced, crypto agility allows organizations to adapt to the changes without causing significant changes to the overall technology infrastructure (Alnahawi et al., 2023). Crypto agility is imperative to the implementation of post-quantum encryption algorithms because it allows organizations to switch between algorithms as new, stronger ones are developed over time as the threat landscape changes. The concept of crypto agility allows for the use of hybrid schemes, where both classical methods of encryption and PQC methods can be used in conjunction. Hybrid systems allow organizations to safely address the risk of quantum computing, even the threat of "Harvest Now, Decrypt Later," while still relying on trusted methods of classical encryption (Ott & Peikert, 2019).

Existing Frameworks for Migration

There is limited research on migration to PQC within the critical infrastructure sectors, given the recent NIST PQC publication; however, existing research agrees on the importance of considering migration. Organizations that have sensitive data that have a shelf-life longer than five years should begin implementation immediately (Joseph et al., 2022). All reviewed frameworks identified the necessity for comprehensive risk assessments, which may help to inventory an organization's current cryptographic systems (Hassan et al., 2024; Aydeger et al., 2024; Joseph et al., 2022; Baseri et al., 2024).

Given the expectation for PQC standards to change over time, research also expresses the need for crypto agility to be applied within the framework of PQC migration to limit disruption across the infrastructure and allow for smooth migration (Joseph et al., 2022). Hybrid strategies are suggested to combine classical and PQC for backward compatibility and allow for crypto agility without the need to replace entire systems (Baseri et al., 2024). Hybrid systems can be implemented as modifications to existing protocols such as TLS (Hassan et al., 2024).

Methodology

This research utilized semi-structured interviews as the primary methodology, which is ideal for more complex social and behavioral questions. Grounded Theory (GT) is an approach to theory development that is widely used within semi-structured qualitative studies. GT can be used to create mid-range theories of processes through systematic coding and analysis of data, which is especially useful for emerging areas of crypto agility and quantum readiness (Blandford, 2013). GT is well-suited for this unstructured area of study because it allows the collected data to shape the theory naturally instead of selecting a theory before conducting research. Multi-Grounded Theory (MGT) expands on GT concepts by allowing theories and ideas to develop more naturally while limiting the shortcomings of GT *(*Goldkuhl & Cronholm, 2010).

Participants

Participants were selected based on roles that provide direct insight into organizational decision-making related to quantum readiness, such as experts in cybersecurity, cryptography, quantum computing, or critical infrastructure management. This study focuses on individuals who are responsible for cybersecurity strategy, encryption policies, or technology adoption, as they influence how an organization discusses, plans, and ultimately implements PQC.

Using a theoretical sampling approach allowed the researcher to enlist the help of the participants to inform the theory, which helped refine the theory by focusing on participants who could provide the most relevant data for the analysis as the theory changed. This iterative sampling ensured that emerging themes were explored in depth (Blandford, 2013). This study focused on four participants from various organizations.

Interviews

Interview participants were found using a variety of methods, including LinkedIn, industry associations and professional groups such as (ISC)², NIST working groups, other academic and research institutions, government agencies and policymakers, and referrals. Networking with experts provided additional connections to experts in the field of quantum-resistant cryptography and critical infrastructure. Interviewing such seasoned professionals proved to be an advantage to developing open-ended, semi-structured interviews that facilitated insights that allowed for the development of the multi-grounded theory. Such expertise contributed to uncovering patterns and relationships that led to a well-founded theoretical framework on quantum readiness.

Interview Protocol

Interviews were conducted using a semi-structured approach, providing flexibility to explore the insight and experiences of subject matter experts while still allowing for comparisons across the different interviews. This protocol consisted of a series of broad, open-ended questions designed to elicit deep conversations regarding the participant's experiences, decision-making processes, and perspectives of quantum readiness in their industry and organizations.

Data Analysis

Data analysis followed Multi-Grounded Theory (MGT), which combines empirical, theoretical, and internal validation to refine emerging concepts (Goldkuhl & Cronholm, 2010). In the Theory Generation phase, initial codes were developed without preconceived ideas. The codes and patterns developed over time to create the theory. The Explicit Grounding phase then compared these codes against established cybersecurity and quantum readiness frameworks to ensure alignment with existing knowledge. The final phase, Research Interest Reflection and Revision, refined the theoretical framework to ensure it had relevance and applicability to critical infrastructure environments.

To ensure consistency, MAXQDA, a qualitative data analysis tool, was used to categorize emerging patterns from coding into themes and to provide visualization of theoretical insights to support the practicality of the research. To minimize researcher bias, the findings were compared to existing research to prevent triangulation on a single perspective. Patterns among participants who were from different organizations and industries emerged and research was not based on isolated responses. Theory

Condensation (Goldkuhl & Cronholm, 2010) occurred when all interviews were completed, and the analyzed data did not introduce any more concepts to influence the theory any further.

Results

The analysis of interviews across four separate critical infrastructure industries identified both barriers and facilitators of PQC readiness. The following findings are structured to answer each research question.

Regarding research question one, while participants acknowledged the risks posed by quantum computing, most expressed a perceived lack of urgency within their sectors or organizations to proactively prepare. Many attributed this to the current state of quantum development, noting that without a quantum computer powerful enough to break modern encryption standards, the need to act remains a future problem rather than an immediate priority. The prevailing sentiment was that, since most experts still predict viable quantum threats are still at least a decade away, organizations feel they have plenty of time to address the issue at a later time.

Despite the common theme, one participant stood out as an exception. Unlike the others, this organization had already begun taking active steps towards quantum readiness. While it was acknowledged that full PQC adoption is not yet feasible, they are proactively researching crypto agility strategies and working to integrate PQC into their security roadmap. This finding demonstrates that some sectors within critical infrastructure recognize the urgency and are acting ahead of regulatory mandates, though they do remain the minority.

The lack of urgency among most of the participants was further fueled by education and awareness gaps. Although participants were familiar with quantum computing as a concept, most admitted to having little to no knowledge of post-quantum-resistant algorithms. Despite the publication of NIST's post-quantum cryptographic standards in 2024, many were either unaware of their release or uncertain about how to integrate them into their existing security frameworks. Several participants also noted a lack of visibility in their cryptographic infrastructure, recognizing the need to inventory encryption systems before any meaningful steps toward quantum resilience could be taken.

Additionally, crypto agility practices were not actively considered in any of the organizations that were interviewed, with one key exception. The same outlier participant who had already begun quantum readiness planning noted they had evaluated crypto agility strategies but had not fully implemented them due to various constraints in this area.

As it relates to research question two, a lack of awareness, training, and strategic planning emerged as the most significant barrier to quantum readiness, accounting for 23.64% of all coded segments as shown in Table 1. While participants recognized quantum computing as a disruptive technology, most lacked foundational knowledge about post-quantum cryptographic standards, implementation strategies, or the urgency of migration. Several participants stated they had little to no formal training on PQC, nor had anyone in their organizations, leaving their security teams unprepared to assess quantum risks or strategize for mitigation. Three of the four participants stated they do not maintain an internal inventory of their cryptographic assets, leaving them unaware of which systems and how many systems will require PQC migration. Without this foundational awareness, strategic planning efforts are either delayed or wholly nonexistent, reinforcing the passive stance that has been observed in many organizations. This knowledge gap contributes to a cycle of inaction, where organizations understand there is an incoming risk but lack the guidance needed to take the first steps toward PQC implementation.

Table 1: Barriers to PQC Adoption Frequency Chart

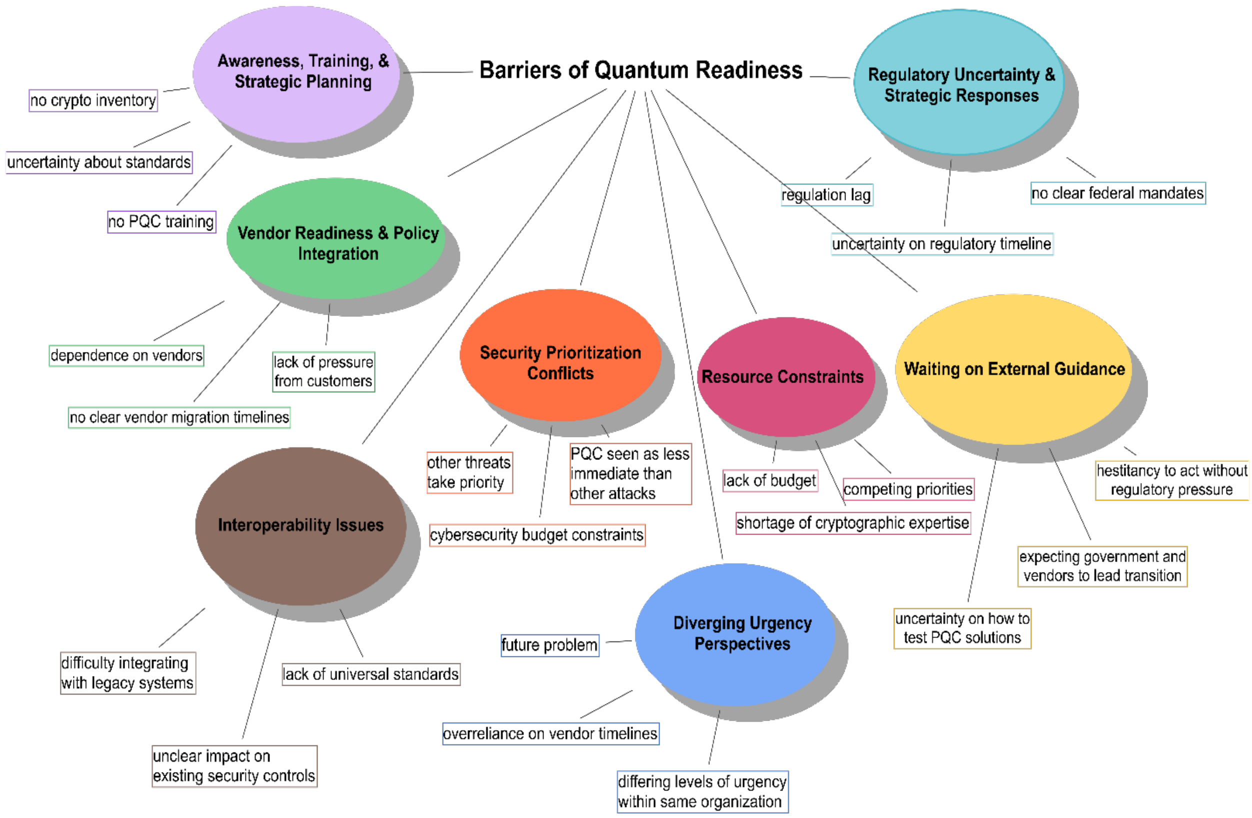
	Segments	Percentage
Awareness, Training, & Strategic Planning	52	23.64
Diverging Urgency Perspectives	32	14.55
Regulatory Uncertainty & Strategic Responses	31	14.09
Vendor Readiness & Policy Integration	29	13.18
Interoperability Issues	26	11.82
Waiting on External Guidance	22	10.00
Resource Constraints	16	7.27
Security Prioritization Conflicts	12	5.45
TOTAL	220	100.00

Regulatory lag was a widespread frustration, especially for those in critical infrastructure sectors that depend on compliance-driven cybersecurity policies. Participants felt that by the time regulatory guidance reaches them, it is often outdated or requires further revisions. Many saw early action as a waste of their time because they believed that any premature effort would result in wasted resources if new regulations forced a change in their work. Even with NIST's post-quantum cryptographic standards already published, participants expressed uncertainty about whether their specific regulatory agencies would issue formal guidance on quantum security risks, or if that guidance would reach them in time to prepare for the threat. Participants noted that the lack of visibility in the regulatory body's decision-making reinforced the reluctance to take initiative.

Vendor dependency and vendor relationships were another major concern for all interviewed organizations. Organizations rely heavily on third-party vendors for software, security tools, and encryption mechanisms, with very little developed in-house. As a result, their quantum security strategy is entirely dependent on their vendors' willingness to act. Participants noted that vendors show no urgency in transitioning to quantum-resistant encryption, reinforcing the passive stance that many other organizations have taken. Without industry-wide vendor adoptions, most participants felt there was little they could do to accelerate the transition on their own.

To better understand how these barriers interconnect, a thematic analysis was conducted. Figure 1 presents a thematic visualization illustrating the relationships between key obstacles to post-quantum cryptography adoption and the subthemes that make up each barrier. These themes highlight that the delay in quantum readiness stems from a combination of skepticism and reliance on external factors.

Figure 1: Thematic Visualization


Barriers of Quantum Readiness
Awareness, Training, & Strategic Planning
no crypto inventory
uncertainty about standards
no PQC training
Regulatory Uncertainty & Strategic Responses
regulation lag
no clear federal mandates
uncertainty on regulatory timeline
Vendor Readiness & Policy Integration
dependence on vendors
lack of pressure from customers
no clear vendor migration timelines
Security Prioritization Conflicts
other threats take priority
PQC seen as less immediate than other attacks
cybersecurity budget constraints
Resource Constraints
lack of budget
competing priorities
shortage of cryptographic expertise
Waiting on External Guidance
hestitancy to act without regulatory pressure
expecting government and vendors to lead transition
uncertainty on how to test PQC solutions
Interoperability Issues
difficulty integrating with legacy systems
lack of universal standards
unclear impact on existing security controls
Diverging Urgency Perspectives
future problem
overreliance on vendor timelines
differing levels of urgency within same organization

Regarding research question 3, while there are many barriers that may hinder organizations from adopting PQC, some factors facilitate and accelerate the transition to quantum-resistant security practices. The research identified six facilitators to quantum readiness as seen in Table 2. These factors are elements that enable and encourage organizations to prioritize PQC adoption.

Table 2: Facilitators of PQC Adoption Frequency Chart

	Segments	Percentage
Monitoring Quantum Advancements	36	22.09
Security Leadership & Decision-Making Influence	34	20.86
Organizational Constraints vs. Strategic Adaptation	30	18.40
Regulatory Influence	28	17.18
Quantum Readiness Frameworks & Strategic Planning	18	11.04
Risk-Based Implementation	17	10.43
TOTAL	163	100.00

While all participants acknowledged monitoring quantum advancements in the news, few participants engaged in proactive research or strategic planning to prepare for PQC. Participants were generally aware of key threats such as “harvest now, decrypt later” and the NIST PQC standards, but admitted they were waiting on external forces, such as vendors to integrate PQC solutions or regulatory bodies to mandate adoption, before taking any significant action.

One participant stated that while quantum computing was listed in their organization’s risk register, it was deprioritized until Chinese scientists claimed to break RSA encryption with a 50-bit integer, which reignited internal discussions among leadership.

Organizations that were more advanced in their PQC preparation had already begun to establish structured roadmaps for migration, citing key steps such as identifying cryptographic dependencies, exploring hybrid encryption models, and engaging with security leadership early to ensure that quantum readiness is recognized as a strategic priority. Leadership involvement was identified as a key differentiator between organizations that were proactively preparing and those that were delaying action. Participants noted that when leadership actively prioritized PQC, the organization was more likely to push to develop concrete strategies. Organizations, where leadership was perceived to be uninformed of quantum risks, lacked any sort of structured plans.

Every participant identified regulatory mandates as the most significant driver for PQC adoption. Organizations in highly regulated industries (e.g. finance, healthcare, government) were more likely to take early steps toward quantum readiness due to anticipated requirements. Some participants referenced government initiatives such as OMB Memo 23-02, which require federal agencies to inventory cryptographic assets and prepare mitigation plans.

As to research question four, most participants in this study did not see quantum computing as an immediate concern despite acknowledging the long-term risks it will pose to their environments in the future. Many believed that a cryptographically relevant quantum computer was still far enough in the future to allow ample time for migration planning; however, participants were unsure of the necessary steps for transition or how long implementation would take.

Most participants were firm about waiting for external guidance when assessing quantum risk. Some participants expect regulatory bodies to mandate the PQC transition well before quantum threats become an urgent issue and stated that they would not act until such mandates were given. Other participants expressed hesitancy to take early action, even though they were worried about the risk, due to concerns that regulations could shift, forcing them to redo work and waste resources. Vendor dependency was also a key factor in delaying proactive readiness efforts. One participant emphasized that their organization relies entirely on third-party vendors for encryption solutions, leaving them unable to update their systems independently. This approach dictates that some quantum adoption is reliant on vendor timelines rather than an organization’s internal security posture.

Participants also cited competing security priorities as a reason for their inaction. Ransomware and AI-driven cyber threats were seen as more immediate and pressing concerns, leading organizations to allocate resources toward defending against active threats rather than planning for quantum risks. As a result, participants felt that PQC readiness was often deprioritized in favor of addressing cybersecurity risks that already impact their environments.

Discussion

This research studied how organizations in critical infrastructure perceive and prepare for post-quantum cryptography (PQC) to develop a practical framework that promotes crypto agility, counters decision-making barriers, and lays the groundwork for effective PQC adoption. This discussion will explore the implications of these findings and propose a framework that organizations can use to build crypto agility and prepare for PQC migration.

Interpretation of Findings

The research found that while organizations recognize the risks posed by quantum computing, many hesitate to act due to regulatory uncertainty, reliance on vendors, and competing security policies. Quantum readiness is often deprioritized in favor of more immediate security threats. This lack of urgency is largely driven by a lack of awareness and education – many organizations do not fully grasp the risk a cryptographically relevant quantum computer poses because they do not know which of their systems rely on vulnerable encryption. They lack this knowledge because they have not conducted a cryptographic inventory, and they avoid conducting an inventory because it is not yet required by regulation in all critical infrastructure industries. This creates a cycle of inaction that is bound to keep repeating until a change occurs.

If organizations followed quantum experts and emerging research in the field, they might better understand the urgency of the threat. Many fail to realize that the shelf life of their data determines when they need to act (Mosca & Mulholland, 2017)– sensitive information that must remain secure for years or decades is already at risk due to "harvest now, decrypt later". The reality is that much like zero-day vulnerabilities, the arrival of quantum computing will be sudden, leaving little time to prepare.

Although organizations are responsible for their security frameworks, many rely heavily on regulatory mandates to drive change. Some industries remain uncertain whether their regulatory bodies will become primary targets due to widespread weaknesses. Organizations also place too much trust in their vendors, assuming they will handle PQC migration appropriately; however, most participants admitted that they have not discussed PQC with their vendors nor do they require vendors to demonstrate a migration plan through contract terms or procurement policies.

Despite these many challenges, the research also identified several facilitators that organizations can leverage to improve their quantum readiness. Accessing credible sources, such as monitoring the news, following NIST guidelines, and reviewing recent research, can provide organizations with a clearer understanding of the evolving threat landscape. Strong leadership is also essential because organizations where executives actively engage with quantum security risk discussions are more likely to be prepared to face the coming threat.

Proposed PQC Adoption Framework: A Structured Approach to Crypto Agility

Based on the findings from this study and a review of relevant literature, a PQC adoption framework has been developed to guide organizations in preparing for the transition to post-quantum cryptography. This framework addresses the key barriers that were identified in the research, including regulatory uncertainty, vendor dependence, and the lack of strategic prioritization. By incorporating established best practices and industry recommendations, the framework provides a 7-phase approach to enhancing cryptographic agility, security-critical assets, and ensuring long-term resilience against quantum threats. It is important to note that many of these suggested phases can be done in conjunction with other phases and are not sequential phases.

Leadership Engagement & Strategic Planning

Leadership buy-in is essential for securing resources, setting priorities, and driving PQC adoption. Research shows that successful risk management depends on security experts establishing trust with their senior leadership and gaining management support for cybersecurity investments (Michalec, Milyaeva, & Rashid, 2022); however, most study participants indicated that their executives do not perceive quantum computing as an imminent threat, leading to limited engagement with PQC planning. Organizations that actively involve leadership in PQC discussions were found to be further along in their migration efforts.

Organizations should establish a PQC transition task force to oversee mitigation strategy. Research indicates that many organizations will need to update applications and systems to safeguard assets against cryptographically relevant quantum computers (Giron, 2023). Interview findings supported this, with participants noting that cross-departmental collaboration is necessary to ensure that cryptographic transitions do not disrupt business operations.

PQC adoption should be aligned with broader strategic initiatives, such as cloud migration, digital transformation, and trust-building measures (FS-ISAC, Inc., 2023). Organizations that integrate PQC migration into existing IT efforts can streamline adoption and reduce operational issues. Several of the study participants echoed this sentiment, emphasizing that PQC planning should be part of a holistic approach to enterprise security and infrastructure resilience.

This phase should be broken down into two distinct steps. The first step focuses on leadership buy-in and the first round of strategic planning that assesses a timeline to conduct the cryptographic inventory and quantum risk assessments. The second step must be returned to after the cryptographic inventory and quantum risk assessments have been completed so that organizations can begin planning for a phased migration strategy.

Cryptographic Inventory & Asset Classification

Organizations often hesitate to act because they lack visibility into which of their systems rely on vulnerable cryptography. Automated cryptographic discovery and inventory (ACDI) tools can help organizations map cryptographic dependencies by automating data collection on encryption usage in certain environments; however, ACDI tools may not be fully capable of performing all cryptographic inventorying tasks, requiring manual work for certain cryptographic assets, such as software with embedded encryption or proprietary vendor solutions. Organizations should request that their vendors provide detailed cryptographic documentation, including algorithms and key lengths, to support manual inventorying efforts (Cybersecurity and Infrastructure Security Agency, 2024).

A well-structured cryptographic inventory should include details on cryptographic algorithms, configuration, and the data they protect. This inventory must be regularly updated and queryable to ensure accessibility. Dependencies and migration obstacles should be identified in advance to facilitate seamless transition planning. Inventories should also specify whether hybrid cryptographic methods are in use, which could affect migration strategies. To conduct a comprehensive cryptographic inventory, organizations should consider multiple tooling categories such as installed software, connected hardware, communication, stored data, and source code scanning (Schmitt et al., 2024).

Once an inventory is created, organizations should classify assets based on data sensitivity and encryption lifespan. High-risk systems should be prioritized for PQC migration, ensuring encryption transitions align with risk assessment results. Prioritization should factor in migration costs, external dependencies, and regulatory compliance to reduce disruptions (Näther et al., 2024). Assets should be categorized according to their criticality and expected security risk exposure, ensuring a structured approach to PQC migration (FS-ISAC, Inc., 2023).

Awareness & Risk Assessment

Organizations should integrate quantum risk assessments (QRA) into their existing cybersecurity risk management processes to evaluate data vulnerability and assess their preparation for post-quantum cryptography (Mosca & Mulholland, 2017). This framework considers and builds upon Mosca's approach to QRAs by incorporating insights from this research, addressing barriers to adoption, and outlining practical steps for implementation.

A major challenge identified in this study is the lack of urgency surrounding quantum threats, largely driven by low awareness and limited understanding of the risks involved. As a result, education must be the next logical step in PQC adoption. Scholarly research in PQC is becoming increasingly relevant as the development of cryptographically relevant quantum computer processes. Leading organizations, such as NIST (National Institute of Standards and Technology, 2024) and Cybersecurity and Infrastructure Security Agency (CISA), regularly publish guidance on emerging quantum threats and migration strategies, yet many organizations fail to take advantage of these resources. Staying informed on PQC developments is a continual process that requires engagement with industry reports, regulatory updates, and evolving best practices.

Once organizations have developed a foundational understanding of quantum computing risks, they can begin taking proactive steps to develop a strategic migration plan for PQC and return to the next step of the strategic planning phase.

Vendor Management & Supply Chain Coordination

Many organizations rely heavily on third-party vendors for cryptographic solutions but do not require PQC readiness as a contractual requirement. Though it is too early in the quantum timeline to require vendors to be fully PQC compatible, organizations can inquire about cryptographic practices and PQC roadmaps as part of procurement, prepare to require PQC readiness clauses in vendor contracts, and establish industry partnerships to push for vendor transparency and accountability.

Phased PQC Migration Strategy

A gradual transition is necessary to maintain operational stability and avoid security gaps during PQC implementation. Giron et al. (2024) recommend that organizations begin their transition with hybrid cryptography, which integrates classical encryption algorithms with PQC algorithms. The hybrid approach allows for a smoother transition while post-quantum standards continue to be refined (Bishwas & Sen, 2023). Participants in the study revealed that organizations are hesitant to fully replace their cryptographic systems due to lingering doubts about the current post-quantum standards' long-term security, further emphasizing the need for a hybrid approach.

To address uncertainties surrounding PQC security, organizations should prioritize high-risk and long-lived data for early migration (Hale, Bindel, & Van Bossuyt, 2023). A risk-based approach ensures that sensitive data remains secure throughout the transition, reducing the likelihood of future vulnerabilities. This further aligns with Mosca & Mulholland's (2017) quantum risk assessment framework for determining the urgency of cryptographic transition based on data lifespan and system dependencies.

Policy & Regulatory Engagement

The study made it clear that many organizations hesitate to act without clear regulatory mandates for PQC adoption. Existing research suggests that organizations should actively engage with regulatory agencies to anticipate compliance requirements and avoid last-minute adoption challenges (Bishwas & Sen, 2023). Several interview participants indicated that uncertainty about federal timelines contributed to their inaction, reinforcing the need for proactive regulatory engagement.

Participants in this study expressed frustration over the lack of direct communication between regulators and industry leaders, making it difficult for organizations to plan long-term security strategies. Some organizations reported that their leadership preferred to wait for formal mandates, which could ultimately leave them vulnerable. Organizations that continue to use a passive approach to PQC may be at a disadvantage once regulatory agencies publish new mandates that require rushed implementation of security measures without the time for adequate preparation.

Continuous Monitoring and Future-Proofing

Quantum computing threats continue to evolve, making adaptive security strategies crucial. Bishwas & Sen (2023) highlight the importance of regularly updating cryptographic policies to respond to emerging vulnerabilities, while Hasan et al. (2024) agree, stating these policies should include strategies for dealing with possible compromises of PQC systems and switching to newer, more resistant algorithms as they are readily developed. Ongoing assessment of PQC systems ensures that cryptographic infrastructures remain up to date as security standards evolve. Some organizations in this study reported that they struggle to dedicate resources to long-term PQC monitoring as more immediate cybersecurity threats like ransomware and AI-driven attacks take precedence. Failing to maintain continuous awareness of quantum advancements leaves organizations unprepared for future security changes. Monitoring breakthroughs in quantum computing is critical to ensuring that security strategies remain adaptable. Without sustained investment in PQC research and innovation, organizations may be forced into reactive security measures once cryptographically relevant quantum computers emerge, increasing operational risks and potential compliance challenges (Rodriquez, 2025).

Recommendations for Future Research & Policy

Future studies should explore industry-specific PQC migration challenges, especially in high-risk sectors. Government agencies and other regulatory bodies should establish clearer PQC transition mandates to reduce hesitation to act.

Conclusion

While the timeline of a cryptographically relevant quantum computer is heavily argued by experts and skeptics alike, quantum threats are imminent, and organizations that delay PQC migration risk significant security vulnerabilities. “Harvest Now, Decrypt Later” is a substantial threat to all organizations that handle long-lived sensitive data, including Social Security numbers, classified military intelligence, and medical records. These types of data will be prime targets for these types of attacks, furthering the argument that the risk of quantum is not a distant concern but an immediate security challenge.

Organizations must shift from passive observation to active participation in PQC preparedness to ensure smooth transitions to post-quantum cryptography. The 7-phased approach suggested in this paper ensures a structured and proactive mitigation strategy, addressing awareness, cryptographic inventorying, leadership engagement, vendor coordination, phased implementation, regulatory alignment, and continuous monitoring, enabling organizations to mitigate risk and adapt to evolving quantum threats effectively.

References

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. Journal of the American College of Clinical Pharmacy, 4(10), 1358-1367.

Alnahawi, N., Schmitt, N., Wiesmaier, A., Heinemann, A., & Grasmeyer, T. (2023). On the state of crypto-agility. Cryptology ePrint Archive.

Asenjo, J., Bassous, G., Knitter, S., & Pandy, S. (2022). Understanding the Value of Encryption in the ACH Network. Nacha.

Aydeger, A., Zeydan, E., Awaneesh, K. Y., Hemachandra, K. T., Mishra, S. K., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In 15th International Conference on Network of the Future (NoF). IEEE.

Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure. arXiv preprint arXiv:2404.10659.

Baseri, Y., Chouhan, V., Ghorbani, A., & Chow, A. (2024). Evaluation Framework for Quantum Security Risk Assessment: A Comprehensive Study for Quantum-Safe Migration. arXiv preprint arXiv:2404.08231.

Bishwas, A. K., & Sen, M. (2023). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. PricewaterhouseCoopers.

Blandford, A. E. (2013). Semi-structured qualitative studies. Interaction Design Foundation.

Board of Governors of the Federal Reserve System. (n.d.). *Automated clearinghouse services*. Federal Reserve. Retrieved March 14, 2025, from https://www.federalreserve.gov/paymentsystems/fedach_about.htm

Cheng, J. K., Lim, E. M., Krikorian, Y. Y., Sklar, D. J., & Kong, V. J. (2021, March). A survey of encryption standard and potential impact due to quantum computing. In 2021 IEEE Aerospace Conference (50100) (pp. 1-10). IEEE.

Cybersecurity and Infrastructure Security Agency. (2024, August 15). *Strategy for migrating to automated post-quantum cryptography discovery and inventory tools*.

Giron, A. A., do Nascimento, J. P. A., Custódio, R., Perin, L. P., & Mateu, V. (2023, September). Post-quantum hybrid KEMTLS performance in simulated and real network environments. In *International Conference on Cryptology and Information Security in Latin America* (pp. 293-312). Cham: Springer Nature Switzerland.

Goldkuhl, G., & Cronholm, S. (2010). Adding theoretical grounding to grounded theory: Toward multi-grounded theory. *International journal of qualitative methods*, *9*(2), 187-205.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

FS-ISAC, Inc. (2023). Post-Quantum Cryptography (PQC) Working Group Risk Model Technical Paper. FS-ISAC, Inc.

FS-ISAC, Inc. (2025). The Impact of Quantum Computing on the Payment Card Industry. FS-ISAC.

Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., ... & McKague, M. (2024). A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. IEEE Access.

Hale, B., Bindel, N., & Van Bossuyt, D. L. (2023). Quantum Computers: The Need for a New Cryptographic Strategy. In K. P. Balomenos et al. (Eds.), *Handbook for Management of Threats*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-39542-0_7

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237-243.

Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? *Big Data & Society*, January–June, 1–13. https://doi.org/10.1177/20539517221108369

Mosca, M. & Mulholland, J. (2017). A methodology for quantum risk assessment. Global Risk Institute. https://cdn.prod.website-files.com/63ef0996726f31b9968ba679/648c8e28cfee25748915738f_a-methodology-for-quantum-risk-assessment-pdf.pdf

Mosca, M., & Piani, M. (2024). *Quantum Threat Timeline Report 2024 Executive Summary*. Global Risk Institute in Financial Services. Retrieved from http://www.globalriskinstitute.org

Mosca, M. & Piani, M. (2023). Quantum threat timeline report 2023. Global Risk Institute. https://www.globalriskinstitute.org/publications/quantum-threat-timeline-report-2023

Nacha. (2024a). *ACH Network volume and value statistics*. Nacha. https://www.nacha.org/content/ach-network-volume-and-value-statistics

Nacha. (2024b). Protecting payments in the quantum era: What you need to know. Payments Innovation Alliance.

National Institute of Standards and Technology. (2024, August). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. U.S. Department of Commerce. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Näther, C., Herzinger, D., Gazdag, S.-L., Steghöfer, J.-P., Daum, S., & Loebenberger, D. (2024). Migrating software systems toward post-quantum cryptography–A systematic literature review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3450306

Oliva del Moral, J., deMarti iOlius, A., Vidal, G., Crespo, P.M., & Etxezarreta Martinez, J. (2024). Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. IEEE Internet of Things Journal, 11, 30217-30244.

Ott, D., Moreau, D., & Gaur, M. (2022). Planning for Cryptographic Readiness in an Era of Quantum Computing Advancement. In ICISSP (pp. 491-498).

Ott, D., & Peikert, C. (2019). Identifying research challenges in post-quantum cryptography migration and cryptographic agility. arXiv preprint arXiv:1909.07353.

Rodríguez, A. G. (2025, January 17). *A quantum cybersecurity agenda for Europe II: Enabling policy and investment options for the quantum transition*. Centre for European Policy Studies.

Schmitt, N., Henrich, J., Heinz, D., Alnahawi, N., & Wiesmaier, A. (2024). On Criteria and Tooling for Cryptographic Inventories. In S. Wendzel et al. (Eds.), **1** (pp. 49-72). Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/sicherheit2024_003

Scott, M. (2023). On TLS for the Internet of Things, in a Post Quantum world. *Cryptology ePrint Archive*.

Vaishnavi, A., & Pillai, S. (2021). Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. Journal of Physics: Conference Series, 1964(4), p.42002. IOP Publishing.

Vermeer, M. J., Heitzenrater, C., Parker, E., Moon, A., Lumpkin, D., & Awan, J. (2023). Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems. Journal of Critical Infrastructure Policy.