QUANTUM-RESISTANT ENCRYPTION: A QUANTITATIVE ANALYSIS OF ORGANIZATIONAL CYBERSECURITY PREPAREDNESS

by

OSCAR E. GONZALEZ

B.S., Florida Atlantic University, 2001

M.S., Nova Southeastern University, 2008

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

2026

Quantum-resistant encryption: A quantitative analysis of organizational cybersecurity preparedness

Oscar E. Gonzalez, *Middle Georgia State University, oscar.gonzalez@mga.edu*

Abstract

Quantum computing poses a significant and emerging threat to classical cryptographic systems that currently secure global digital infrastructure. As post-quantum cryptographic (PQC) standards continue to develop, organizations vary widely in their preparedness to transition to quantum-resistant encryption. This quantitative study examines the extent to which perceived vulnerability to quantum threats, awareness of post-quantum cryptography, and policy and governance support predict organizational readiness for PQC adoption. Using a descriptive-correlational research design, data will be collected through a structured survey administered to cybersecurity and information technology professionals across multiple industry sectors. Multiple regression, analysis of variance, and correlation analyses will be employed to identify predictive relationships and sector-based differences in readiness. The findings of this study are expected to provide empirical insights into organizational preparedness for quantum-related cybersecurity risks and to inform strategic planning, policy development, and future research efforts aimed at strengthening cybersecurity resilience in the quantum era.

Keywords: quantum-resistant encryption, post-quantum cryptography, organizational readiness, cybersecurity preparedness, quantum computing threats.

Introduction

As digital systems become increasingly interconnected, safeguarding sensitive information emerges as a top priority across all sectors. Modern cybersecurity frameworks heavily rely on established encryption techniques such as RSA, Diffie–Hellman, and elliptic curve cryptography (ECC) to secure communication, financial transactions, critical infrastructure, health data, and cloud services. However, the rise of quantum computing poses a significant threat to the long-term effectiveness of these cryptographic methods. Quantum computers use qubits, superposition, and entanglement to process data exponentially faster than classical computers (Li et al., 2023), enabling them to solve the mathematical challenges that underpin today's encryption schemes.

Quantum computing represents a significant shift in computational power, enabling machines to handle vast datasets using quantum bits (qubits) that can exist in multiple states simultaneously. Unlike classical computers, which operate on binary principles, quantum systems employ superposition and entanglement to tackle complex mathematical problems with remarkable speed (Li et al., 2023). While this technological advancement has the potential to revolutionize areas like medicine, artificial intelligence, and logistics, this innovation simultaneously presents a direct threat to the cryptographic systems that secure our communications and data infrastructures (Alagic et al., 2025).

Though quantum computing promises breakthroughs in fields such as drug discovery and optimization, this emerging technology also poses unprecedented challenges for digital security. Researchers show that quantum algorithms, notably Shor's algorithm, could theoretically compromise widely used public-key cryptosystems. Meanwhile, organizations such as the National Institute of Standards and Technology (NIST; Alagic et al., 2025) are working to standardize post-quantum cryptographic (PQC) algorithms to resist quantum attacks. Nonetheless, despite these technical strides, the readiness of organizations and alignment of policies vary significantly across sectors.

The shift to quantum-resistant encryption not only presents a technological hurdle but also a strategic one. Empirical data is crucial in understanding how organizations perceive quantum threats, their familiarity with PQC technologies, and their readiness to implement quantum-resistant solutions. This study aims to address this gap by assessing the factors influencing organizational preparedness and examining differences in readiness for PQC adoption across industries.

Quantum computing poses a quantifiable, time-sensitive threat to current cybersecurity systems. Classical cryptographic algorithms, now foundational to modern digital infrastructure, are increasingly vulnerable as quantum computational capabilities advance. Although post-quantum encryption standards are emerging, empirical evidence suggests that organizations vary significantly in: 1) Perceived vulnerability of their systems to quantum threats, 2) Awareness of post-quantum cryptographic solutions, 3) Policy and governance support within their institutions, and 4) Actual readiness to transition to quantum-resistant encryption.

These differences may be further influenced by industry sector, resulting in uneven preparedness across critical national and global infrastructure. The lack of quantitative data on these relationships limits the effectiveness of coordinated transition planning. Understanding the predictive factors of organizational readiness and the degree of variation across sectors is essential for developing strategic, evidence-based approaches to PQC adoption.

Recent studies on quantum resource estimation demonstrate that large-scale quantum algorithms could efficiently break these encryption schemes, potentially compromising the confidentiality and integrity of digital communications (Gheorghiu & Mosca, 2025; Li et al., 2023). The problem lies not only in the vulnerability of these cryptographic systems but also in the lack of a cohesive global strategy for transitioning to quantum-resistant algorithms. While organizations such as the National Institute of Standards and Technology (NIST; Alagic et al., 2025) are standardizing post-quantum cryptography, broader implementation across industries remains fragmented and slow. Moreover, the anticipated availability of quantum computers within the next decade makes this transition time-sensitive, as delays could expose critical infrastructure to large-scale security breaches.

This gap underscores the urgent need to examine both the technical and organizational dimensions of adopting quantum-resistant encryption solutions to secure future digital infrastructure.

The purpose of this quantitative study is to determine the extent to which perceived vulnerability to quantum threats, awareness of post-quantum cryptography, and governance support predict organizational readiness for PQC adoption. Additionally, the study aims to assess whether significant differences in readiness exist across major industry sectors, such as finance, healthcare, education, government, and technology. By providing empirically grounded insights, this research will help policymakers, cybersecurity leaders, and organizational decision-makers develop strategies for accelerating quantum-resistant security transitions.

The significance of this research lies in the study's ability to provide an empirical assessment of organizational preparedness for quantum-based cybersecurity threats by offering measurable data that clarifies actual readiness levels. This research also identifies key predictive factors, such as vulnerability perceptions, awareness, and policy support, that most strongly influence the adoption of post-quantum cryptography (PQC). Additionally, the study provides sector-level insights to guide tailored transition strategies in high-risk industries, including healthcare, finance, and government, where cryptographic breaches could have severe consequences. The findings further support the development of national and international policy frameworks by revealing governance strengths and gaps related to PQC. Ultimately, this research contributes to global efforts to accelerate quantum-safe migration and protect digital infrastructure as practical quantum computing systems emerge.

Consistent with the purpose of this study, the following research questions guide the investigation:

RQ1: To what extent do perceived vulnerability of traditional encryption, awareness of post-quantum cryptography, and policy/governance support predict organizational readiness to adopt quantum-resistant encryption?

RQ2: Do organizational readiness levels for post-quantum cryptography adoption vary across industry sectors, including their relationship to organizational policy and governance support?

Review of literature

Quantum Computing Threats to Classical Encryption

The advancement of quantum computing represents a fundamental challenge to classical cryptographic systems that secure modern digital infrastructure. Public-key encryption algorithms such as RSA and elliptic curve cryptography (ECC) rely on mathematical problems—integer factorization and discrete logarithms—that are computationally infeasible for classical computers but tractable for sufficiently powerful quantum machines. Research by Gidney and Ekerå (2021) demonstrated that a large-scale quantum computer could factor a 2048-bit RSA key within hours, providing empirical evidence that classical encryption schemes face realistic future compromise. Similarly, Dam et al. (2023) and Liu and Moody (2024) emphasized that quantum-enabled attacks are no longer theoretical concerns but measurable risks with projected timelines. These findings provide a foundation for assessing perceived vulnerability, as organizations must increasingly recognize that the encryption mechanisms currently in use may become obsolete as quantum capabilities mature.

Development of Post-Quantum Cryptography

In response to the vulnerabilities posed by quantum computing, post-quantum cryptography (PQC) has emerged as a critical research area focused on developing encryption algorithms that are resistant to both classical and quantum attacks. Lattice-based cryptographic schemes, including Kyber and Dilithium, have gained prominence due to their computational efficiency and strong security assumptions. Nguyen et al. (2025) provided a comprehensive survey demonstrating that lattice-based algorithms are currently the most viable candidates for widespread adoption. Prior research, such as Aikata et al. (2022), further validated this position by presenting KaLi, a hybrid lattice-based framework optimized for performance and post-quantum security. These studies collectively support the growing consensus that PQC technologies are technically mature enough for implementation, making organizational awareness a critical factor influencing adoption readiness.

Implementation and Migration Challenges

Despite the technical maturity of PQC algorithms, transitioning from classical cryptographic systems to quantum-resistant solutions presents significant operational challenges. Dobias et al. (2025) identified performance overhead, hardware compatibility, and system integration as major barriers to implementation. Baseri et al. (2024) further noted that legacy network infrastructures are often ill-equipped to support the computational demands of quantum-safe protocols. Governance and interoperability challenges also hinder adoption, as highlighted by Liu and Moody (2024), who emphasized the absence of standardized migration pathways across industries. These findings underscore that organizational readiness is not solely dependent on algorithm availability but also on institutional planning, technical expertise, and resource allocation.

Sector-Based Differences in PQC Adoption

Research indicates that readiness for PQC adoption varies significantly across industry sectors due to differing regulatory requirements, operational constraints, and risk exposure. In healthcare, Tiwo et al. (2025) demonstrated the necessity of quantum-resistant encryption to protect sensitive patient data in cloud-based systems. In contrast, Xiong et al. (2025) examined smart grid and Internet of Things (IoT) environments, where computational constraints require hybrid encryption approaches. Jiang and Wang (2024) highlighted similar challenges in cloud infrastructure, emphasizing the need for scalable, quantum-resistant authentication mechanisms. These sector-specific studies justify the examination of industry-based differences in readiness and support the use of analysis of variance (ANOVA) to identify statistically significant variations across organizational contexts.

Policy and Governance Considerations for PQC Adoption

Beyond technical and organizational factors, effective adoption of quantum-resistant encryption depends on policy and governance alignment at institutional, national, and international levels. Liu and Moody (2024) argued that inconsistent regulatory frameworks and policy inertia significantly delay PQC implementation. Lin and Lin (2025) further demonstrated that organizations with strong governance structures and leadership support are better positioned to integrate quantum-safe cryptographic systems. Prior research highlights the importance of cross-sector collaboration among governments, industry, and academia to promote standardization and interoperability (Nguyen et al., 2025). Collectively, these studies highlight policy and governance support as a measurable determinant of organizational readiness, reinforcing the inclusion of policy and governance support as a key construct in quantitative assessments of PQC adoption.

Research Gap

The literature clearly demonstrates that quantum computing poses an imminent threat to classical encryption and that technically viable post-quantum solutions are available. However, gaps remain in understanding how organizations perceive these threats, how aware companies are of PQC technologies, and how governance structures influence readiness for adoption. While prior studies have focused on algorithm development and sector-specific applications, limited empirical research has quantitatively examined the organizational factors that predict readiness across industries. This study addresses this gap by systematically analyzing perceived vulnerability, awareness, and policy/governance support as predictors of organizational readiness for quantum-resistant encryption.

Methodology

Research Design

This study employed a quantitative, descriptive-correlational research design to examine organizational readiness for adopting quantum-resistant encryption technologies. The design was selected to identify predictive relationships among perceived vulnerability to quantum threats, awareness of post-quantum cryptography (PQC), policy and governance support, and organizational readiness for PQC adoption. Additionally, the design supported comparison of readiness levels across industry sectors. This approach was appropriate for addressing the study's research questions through statistical analysis of survey data collected from cybersecurity and information technology professionals.

A descriptive-correlational design was well-suited to this study, as the design measured relationships among naturally occurring variables without manipulation. The research excluded experimental intervention or treatment, focused instead on associations among perceptions, awareness levels, governance support, and

readiness within organizational contexts. This design facilitated statistical analysis of predictive relationships through multiple regression and group comparisons via analysis of variance (ANOVA). Collecting quantifiable survey data from cybersecurity professionals enabled objective measurement of constructs and supported evidence-based conclusions regarding organizational preparedness for quantum-resistant encryption.

Participants and Sample Population

The target population consisted of cybersecurity professionals, information technology managers, and information systems administrators working in organizations that rely on cryptographic technologies to protect digital systems and data. Participants were drawn from multiple industry sectors, including finance, healthcare, education, government, and technology.

Data was collected using SurveyMonkey™, and a total of 43 participants completed the survey. The instrument consisted of 22 questions measured on a 7-point Likert scale, including demographic items.

This study employed a non-probability convenience sampling method, a commonly used approach for accessing specialized or readily available participant populations in applied research (Stratton, 2021). Participants were recruited through professional cybersecurity associations, online research panels, and LinkedIn professional groups. Convenience sampling was appropriate for this study because the method allowed access to a specialized professional population with relevant experience in cybersecurity and information technology. Given the exploratory nature of the research and the focused target population, this sampling approach provided practical access to qualified participants while enabling examination of relationships among key variables related to organizational readiness for post-quantum cryptography adoption. Eligibility criteria required participants to be 18 years of age or older and currently employed in a role related to cybersecurity or information technology.

Instrumentation

Data were collected using a structured online survey adapted from previously validated instruments used in cybersecurity readiness and technology adoption research, including instruments developed by Liu and Moody (2024) and Dam et al. (2023). The survey consisted of five constructs: 1) Demographics - 4 items, questions 1 through 4. 2) Perceived Vulnerability of Classical Encryption - 4 items, questions 5 through 8. 3) Awareness of Post-Quantum Cryptography - 5 items, questions 9 through 13. 4) Organizational Readiness for PQC Adoption - 5 items, questions 14 through 18. 5) Policy and Governance Support for Quantum Security - 4 items, questions 19 through 22.

The Demographics construct collected non-identifying background information, including industry sector, professional role, and years of experience.

All non-demographic items were measured using a 7-point Likert scale, ranging from 1 (Strongly disagree) to 7 (Strongly agree). Higher scores indicated stronger agreement with each construct.

Content validity was established through expert review by three researchers with expertise in cybersecurity and cryptography. Internal consistency reliability for the non-demographic constructs was assessed using Cronbach's alpha, with a coefficient of 0.70 or higher considered acceptable.

Data Collection Procedure

Prior to data collection, approval was obtained from the Institutional Review Board (IRB) of Middle Georgia State University. Data were collected using an anonymous online survey administered through

SurveyMonkey™. Eligible participants received an invitation via email, which included a brief description of the study, eligibility criteria, an estimated completion time, and a link to the informed consent form.

Participation was voluntary, and respondents could withdraw from the study at any time without penalty. The survey required approximately 10–15 minutes to complete.

To increase response rates, a structured follow-up protocol was implemented. A reminder email was sent seven days after the initial invitation. A final reminder was distributed four days after the first reminder, after which data collection was closed. No additional follow-up contact was made beyond the two reminder emails. Completed responses were screened for missing data and inconsistent response patterns. Surveys with substantial incomplete data were excluded from analysis.

Data Management and Confidentiality

No personally identifiable information was collected. All survey responses were anonymous and stored on a password-protected computer accessible only to the researcher. Data was reported only in aggregate form to prevent identification of individual participants or organizations. Research data will be retained securely for three years following completion of the study and then permanently destroyed.

Data Analysis

Quantitative data was analyzed using IBM SPSS Statistics. Descriptive statistics, including means, standard deviations, and frequencies, were calculated to summarize participant demographics and overall response patterns.

To address Research Question 1, multiple regression analysis was conducted to determine the extent to which perceived vulnerability, awareness of PQC, and policy/governance support predicted organizational readiness for PQC adoption.

To address Research Question 2, a one-way analysis of variance (ANOVA) was performed to examine differences in readiness levels across industry sectors. When significant differences were identified, post hoc analyses were conducted to determine the source of variation. Additionally, Pearson correlation analysis was used to examine the relationship between organizational readiness and policy/governance support.

Prior to interpretation, diagnostic tests for normality, multicollinearity, and model fit were conducted to ensure statistical validity. Statistical significance was evaluated at the $p < .05$ level, and effect sizes were reported to support interpretation of findings.

Results

Data from 43 participants were analyzed using IBM SPSS-equivalent statistical procedures. All Likert-scale responses were coded from 1 (Strongly disagree) to 7 (Strongly agree). Composite scale scores were computed by averaging item responses for each construct.

Descriptive Statistics

Descriptive statistics indicated that participants reported relatively high perceived vulnerability to quantum computing threats ($M = 5.73$, $SD = 0.87$), moderate awareness of post-quantum cryptography ($M = 4.75$, $SD = 1.18$), and moderate perceptions of policy and governance support ($M = 4.76$, $SD = 0.91$).

In contrast, organizational readiness for adopting quantum-resistant encryption was comparatively low (M = 2.56, SD = 1.28).

Participants generally reported high perceived vulnerability to quantum threats and moderate awareness and governance support. However, organizational readiness was notably low. The key findings, including mean scores and standard deviations for each construct, are presented in Table 1.

Table 1

Descriptive Statistics for Study Variables

Variable	N	M	SD
Perceived Vulnerability	43	5.73	0.87
Awareness of PQC	43	4.75	1.18
Governance Support	43	4.76	0.91
Organizational Readiness	43	2.56	1.28

Note. Scores based on a 7-point Likert scale (1 = Strongly disagree, 7 = Strongly agree).

Reliability Analysis

Internal consistency reliability was assessed using Cronbach's alpha. Perceived Vulnerability ($\alpha = .71$), Awareness ($\alpha = .79$) and Organizational Readiness ($\alpha = .93$) demonstrated acceptable to excellent reliability. Policy and Governance Support yielded lower reliability ($\alpha = .49$).

All constructs demonstrated acceptable reliability ($\alpha \geq .70$) except Governance, which showed lower internal consistency.

Regarding research question one, a multiple regression analysis was conducted to examine whether perceived vulnerability, awareness, and governance support significantly predicted organizational readiness. The overall regression model was statistically significant, $F(3, 39) = 8.07$, $p < .001$, accounting for 38.3% of the variance in readiness (R2 = .383). The key findings regarding the prediction of organizational readiness to adopt quantum-resistant encryption are presented in Table 2.

Table 2

Model Summary for Multiple Regression Predicting Organizational Readiness

Model	R	R^2	Adjusted R^2	F	Std. Error	df	p
Regression	.619	.383	.336	8.07	1.03	(3,39)	<.001

Note. Dependent variable: Organizational Readiness

Awareness of post-quantum cryptography was a significant positive predictor of readiness ($\beta = 0.72$, $p = .001$), indicating that higher levels of awareness were associated with greater organizational readiness. Policy and governance support was also a significant positive predictor ($\beta = 0.41$, $p = .043$).

Perceived vulnerability was a significant negative predictor of readiness (β = -0.75, p = .007). The key findings related to the prediction of organizational readiness by each construct, vulnerability, awareness, and governance support, are presented in Table 3.

Table 3

Regression Coefficients Predicting Organizational Readiness

Predictor	B	SE	β	t	p
Constant	2.11	0.89		2.37	.023
Vulnerability	-0.75	0.26	-0.41	-2.89	.007
Awareness	.072	0.20	0.49	3.54	.011
Governance Support	0.41	0.19	0.28	2.10	.043

Note. Dependent variable: Organizational Readiness.

These findings indicate that awareness and governance support are statistically significant contributors to organizational readiness, while perceived vulnerability is associated with lower reported readiness.

Regarding research question 2, a one-way analysis of variance (ANOVA) was conducted to determine whether organizational readiness differed across industry sectors. The results were not statistically significant, F(4, 38) = 2.29, p = .077.

Although differences approached statistical significance, readiness levels did not significantly vary across sectors. The key findings related to statistically significant differences in organizational readiness across industry sectors are presented in Table 4.

Table 4

One-Way ANOVA for Organizational Readiness by Industry Sector

Source	SS	df	MS	F	p
Between Groups	13.45	4	3.35	2.29	.077
Within Groups	55.79	38	1.06		
Total	69.25	42			

Note. Dependent variable: Organizational Readiness. Differences were not statistically significant at α = .05.

A Pearson correlation analysis was conducted to examine the relationship between governance support and readiness. Results indicated a statistically significant moderate positive correlation, r = .42, p = .005. This finding suggests that higher perceptions of governance support are associated with greater organizational readiness. The key findings related to the relationship between governance support and readiness are presented in Table 5.

Table 5

Pearson Correlation Between Governance Support and Organizational Readiness

Variable	1	2
1. Governance Support	—	
2. Organizational Readiness	.42**	—

Note. N = 43. **p < .01.

The results demonstrated that awareness of post-quantum cryptography and of governance support are significant predictors of organizational readiness to adopt quantum-resistant encryption. While perceived vulnerability was statistically significant, the relationship between perceived vulnerability and readiness was negative. No statistically significant sector-based differences in readiness were observed. Governance support showed a moderate positive association with readiness.

Discussion

The findings of this study provide insight into the factors influencing organizational readiness to adopt quantum-resistant encryption. Awareness of post-quantum cryptography (PQC) emerges as the strongest positive predictor of readiness, indicating that organizations with greater knowledge of PQC technologies are better prepared to transition. This aligns with prior research emphasizing the importance of awareness and knowledge dissemination in facilitating cybersecurity innovation (Dam et al., 2023; Liu & Moody, 2024). Policy and governance support also demonstrate a significant positive relationship with readiness, reinforcing the role of leadership, regulatory alignment, and strategic planning in enabling technological adoption (Lin & Lin, 2025; Nguyen et al., 2025).

In contrast, perceived vulnerability to quantum threats is a significant negative predictor of readiness, suggesting a gap between recognizing risk and taking action. While existing literature highlights quantum threats as a catalyst for cybersecurity advancement (Li et al., 2023; Gheorghiu & Mosca, 2025), these findings indicate that awareness of risk alone may not translate into preparedness due to resource or capability constraints (Baseri et al., 2024; Dobias et al., 2025). Additionally, no statistically significant differences in readiness are observed across industry sectors, suggesting that low preparedness is a widespread issue rather than sector-specific (Jiang & Wang, 2024; Tiwo et al., 2025; Xiong et al., 2025).

Implications

The findings contribute to cybersecurity research by empirically validating awareness and governance support as key predictors of organizational readiness for PQC adoption. The findings also highlight the limitation of perceived vulnerability as a driver of action, suggesting that risk awareness must be supported by institutional capacity and strategic planning. These results reinforce prior studies that emphasize the importance of organizational knowledge and governance structures in facilitating cybersecurity transitions (Liu & Moody, 2024; Lin & Lin, 2025).

From a practical perspective, organizations should prioritize increasing PQC awareness through training and engagement with emerging standards, particularly those developed by the National Institute of Standards and Technology (Alagic et al., 2025). Strengthening governance frameworks, allocating resources, and developing structured migration strategies are also essential for improving readiness

(Baseri et al., 2024; Dobias et al., 2025). The absence of significant sector differences suggests that broad, coordinated approaches to PQC adoption may be more effective than isolated, industry-specific efforts.

Limitations

This study has several limitations that should be considered when interpreting the findings. First, the use of a non-probability convenience sampling method limits the generalizability of the results, as the sample may not fully represent the broader population of cybersecurity professionals. Additionally, the relatively small sample size (N = 43) reduces statistical power and may have limited the ability to detect significant differences across industry sectors.

Second, the study relies on self-reported survey data, which introduces the potential for response bias, including social desirability and subjective interpretation. Participants' responses may not accurately reflect actual organizational practices or readiness levels. Furthermore, the policy and governance support construct demonstrates low internal consistency reliability ($\alpha = .49$), which may affect the precision of findings related to this variable.

Third, the cross-sectional design captures perceptions at a single point in time and does not account for changes as quantum technologies evolve or as standards from the National Institute of Standards and Technology continue to develop (Alagic et al., 2025). Additionally, the study does not include other potentially influential variables, such as organizational size, budget, cybersecurity maturity, or leadership commitment, which may also impact readiness.

Conclusion

This study examines the extent to which perceived vulnerability, awareness of PQC, and policy/governance support predict organizational readiness for quantum-resistant encryption. The findings demonstrate that awareness and governance support are significant positive predictors, while perceived vulnerability is negatively associated with readiness.

The findings of Dam et al. and Liu and Moody suggest that quantum-enabled cyberattacks are no longer theoretical concerns but emerging threats with realistic timelines. Their research supports the concept of perceived vulnerability by emphasizing that current encryption methods may become obsolete as quantum computing capabilities continue to advance, reinforcing the need for organizations to prepare for post-quantum security challenges.

Despite widespread recognition of quantum computing threats, organizational readiness remains low, highlighting a critical gap between risk awareness and implementation capability. As quantum computing advances and threatens existing cryptographic systems (Li et al., 2023; Gheorghiu & Mosca, 2025), organizations must move beyond recognizing the threat and take concrete steps toward preparedness.

Strengthening governance frameworks, investing in workforce development, and aligning with emerging standards, such as those from the National Institute of Standards and Technology (Alagic et al., 2025), are essential to ensuring cybersecurity resilience. This study contributes quantitative evidence to support strategic decision-making and highlights the urgency of transitioning to quantum-safe encryption.

According to Lin and Lin (2025), organizations with strong governance structures and leadership support are better positioned to adopt and implement quantum-safe cryptographic systems, highlighting the importance of organizational policy and strategic leadership in post-quantum cybersecurity preparedness.

Baseri et al. (2024) further emphasized that many legacy network infrastructures are not adequately equipped to meet the computational requirements of quantum-safe cryptographic protocols. This limitation underscores the growing need for organizations to modernize existing systems to ensure long-term cybersecurity resilience as they transition to post-quantum security standards.

Recommendations for Future Research

Future research should expand this study by using larger and more diverse samples to improve generalizability and statistical robustness. Including participants from multiple geographic regions and organizational contexts would provide a more comprehensive understanding of global PQC readiness. Longitudinal studies are also recommended to examine how organizational readiness evolves over time as quantum computing capabilities advance and PQC standards mature (Alagic et al., 2025).

Additionally, future studies should refine and validate the policy and governance construct to improve measurement reliability and incorporate additional variables such as organizational size, cybersecurity maturity, budget allocation, and leadership commitment (Baseri et al., 2024; Dobias et al., 2025). Mixed-methods or qualitative approaches could provide deeper insight into organizational barriers and decision-making processes, while comparative international studies would help evaluate how different regulatory environments influence PQC adoption.

References

Aikata, A., Mert, A. C., Imran, M., Pagliarini, S., & Roy, S. S. (2022). KaLi: A crystal for post-quantum security using Kyber and Dilithium. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *70*(2), 747–758. https://doi.org/10.1109/TCSI.2022.3219555

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2025). *Status report on the fourth round of the NIST post-quantum cryptography standardization process* (NIST IR 8545). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8545/final

Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security*, *142,* 103883. https://doi.org/10.1016/j.cose.2024.103883

Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. *Cryptography*, *7*(3), 40. https://doi.org/10.3390/cryptography7030040

Dobias, P., Malina, L., & Hajny, J. (2025). Efficient unified architecture for post-quantum cryptography: combining Dilithium and Kyber. *PeerJ Computer Science*, *11*, e2746. https://doi.org/10.7717/peerj-cs.2746

Gheorghiu, V., & Mosca, M. (2025). Quantum resource estimation for large scale quantum algorithms. *Future Generation Computer Systems*, *162*, 107480. https://doi.org/10.1016/j.future.2024.107480

Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Jiang, J., & Wang, D. (2024). Qpase: Quantum-resistant password-authenticated searchable encryption for cloud storage. *IEEE Transactions on Information Forensics and Security, 19,* 4231–4246. https://doi.org/10.1109/TIFS.2024.3372804

Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., Liang, W., & Xiong, N. (2023). Post-quantum security: Opportunities and challenges. *Sensors*, *23*(21), 8744. https://doi.org/10.3390/s23218744

Lin, Y., & Lin, Y. (2025). NSEA: A resilient ERP framework integrating quantum-safe cryptography and neuro-symbolic reasoning for industrial adaptability. *IEEE Access, 13,* 77686-77695. https://doi.org/10.1109/ACCESS.2025.3562739

Liu, Y. K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. *Physical Review Applied*, *21*(4), 040501. https://doi.org/10.1103/physrevapplied.21.040501

Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. *IEEE Access, 13,* 89003–89024. https://doi.org/10.1109/ACCESS.2025.3571307

Stratton, S. J. (2021). Population research: convenience sampling strategies. *Prehospital and disaster Medicine*, *36*(4), 373–374. https://doi.org/10.1017/S1049023X21000649

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data. *Asian Journal of Research in Computer Science*, *18*(4), 187-208. https://doi.org/10.9734/ajrcos/2025/v18i4615

Xiong, J., Shen, L., Liu, Y., & Fang, X. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports*, *15*(1), 3. https://doi.org/10.1038/s41598-024-84427-8

Appendix A

Instrument

Quantum-Resistant Encryption Survey

Informed Consent Statement

Thank you for your participation in this survey on quantum-resistant encryption technologies. Your input will help us better understand perceptions, awareness, and organizational readiness around these emerging technologies.

Participation is voluntary, and you may skip any question or stop at any time. Responses are confidential, and no personally identifiable information will be collected. Survey data will be stored securely on a password-protected computer accessible only to the researcher and will be retained for three (3) years following completion of the study, after which it will be securely destroyed. The survey should take about 10 to 15 minutes to complete.

To participate, you must be 18 years of age or older. Minors are not permitted to participate in this study.

The instrument for this study was adapted from Liu and Moody (2024) and Dam et al. (2023).

Perceived Vulnerability of Classical Encryption Construct (Defines awareness of the risks associated with current cryptographic systems such as RSA and ECC).

If you have any questions, please contact Oscar Gonzalez at oscar.gonzalez@mga.edu. By clicking "Continue," you confirm that you have read this information and agree to participate.

Demographic Questions

1. What is your age?
   - 18–24
   - 25–34
   - 35–44
   - 45–54
   - 55+

2. What is your highest level of education completed?
   - High school diploma or equivalent
   - Associate degree
   - Bachelor's degree
   - Master's degree
   - Doctorate
   - Other (please specify) ☐

3. How many years of experience do you have in IT or cybersecurity?
   - Less than 1 year
   - 1–3 years
   - 4–6 years
   - 7–10 years
   - More than 10 years

4. Which sector best describes your organization?
    - Government
    - Healthcare
    - Finance
    - Education
    - Technology
    - Other (please specify) [ ]

Questions 5 through 22 use the following selection criteria
Likert Scale Questions. 1 (Strongly Disagree) to 7 (Strongly Agree)

- Strongly disagree
- Disagree
- Somewhat disagree
- Neutral
- Somewhat agree
- Agree
- Strongly agree

Perceived Vulnerability of Classical Encryption Construct (Questions 5-8)
(Defines awareness of the risks associated with current cryptographic systems such as RSA and ECC)

Awareness of Post-Quantum Cryptography Construct (Questions 9-13)
(Defines understanding of post-quantum cryptographic technologies, research progress, and potential benefits)

Organizational Readiness for PQC Adoption Construct (Questions 14-18)
(Defines preparedness, planning, and resource allocation toward adopting quantum-resistant encryption)

Policy and Governance Support for Quantum Security Construct (Questions 19-22)
(Defines regulatory, institutional, and leadership support for PQC adoption and coordination)

5. I am concerned that current encryption methods (e.g., RSA, ECC) will become ineffective once quantum computers are available.
6. I believe that existing digital infrastructure is vulnerable to quantum-based attacks.
7. I am aware that quantum algorithms such as Shor's algorithm can break current encryption systems.
8. I think organizations are underestimating the risks posed by quantum computing to current cybersecurity systems.
9. I am familiar with post-quantum cryptography (PQC) and its purpose in cybersecurity.
10. I understand that lattice-based algorithms (e.g., Kyber, Dilithium) are being developed as quantum-resistant encryption methods.
11. I follow developments from organizations such as NIST regarding post-quantum encryption standards.
12. I believe that implementing PQC is essential for ensuring long-term cybersecurity.
13. I think post-quantum encryption will significantly reduce data vulnerability to quantum-based attacks.
14. My organization is actively planning for the transition to post-quantum encryption.
15. My organization has sufficient technical expertise to implement PQC systems.
16. Adequate resources and funding are allocated for cybersecurity modernization in preparation for quantum threats.
17. My organization has a timeline or roadmap for adopting quantum-resistant encryption.
18. Employees in my organization receive training or information on quantum cybersecurity readiness.
19. National and international cybersecurity policies adequately address quantum computing threats.
20. Governments should play a stronger role in facilitating quantum-resistant encryption adoption across industries.
21. My organization's leadership supports developing policies to transition to quantum-safe systems.
22. Collaboration between public and private sectors is essential for implementing post-quantum cybersecurity solutions.