Organizational Implementation of PQC, ZTA, and AI for Defending Information Security

Delgerekh Ariunbileg

Fall 2025

1 Executive Summary

Within the next 2 decades, with the arrival of quantum computers, organizations will integrate and harness the power of quantum computing to solve complex problems exponentially faster than classical computers. Conversely, adversaries will utilize quantum computers and Shor's algorithm to crack the prime factors of large numbers, compromising our most widely used asymmetric encryption method. High performing organizations should adopt post-quantum cryptography (PQC) algorithms while this threat is still forthcoming. Private and public organizations who fail to adopt these algorithms will face catastrophic unwanted outcomes and impacts after the first quantum computer is built. Some of these outcomes will include the breach of confidential data, such as customer information, intellectual property, and confidential repositories [2]. The consequences foresee catastrophic operational, financial, and safety impacts which can range from the inability to deliver products to major class action lawsuits as a result of harm. As Q-Day approaches, malicious actors are increasingly likely to utilize artificial intelligence to increase attacks, with hope of exfiltrating sensitive data today to decrypt in the future [21]. Without the implementation of PQC algorithms, organizations will find themselves in a reactive state, facing increased risks and inadequate ability to mitigate threats effectively.

To safeguard from these potential risk factors, organizational technology leaders can utilize a variety of public frameworks that have been laid out by public organizations like NIST or private foreseeing ones like IBM, Microsoft, or Cisco to help transition from classical cryptography to post-quantum cryptographic methods [6][14]. Financial leaders, including CFOs, should actively support and advocate for these initiatives by ensuring adequate protection through well informed cost-benefit analysis. Notably, early adopters may gain a competitive advantage within their sector as compliance thresholds evolve.

Organizations must also implement zero trust architecture (ZTA) to prevent adversaries from employing a "harvest now, decrypt later" strategy aimed at exploiting future advances in quantum computing [22]. ZTA places zero trust for any user, and ensures strict authentication for all access requests and assigns least privileged access [11][20]. To further diminish the risks, organizations must

also leverage AI and ML to learn from past attacks, automate pentesting to evaluate defenses, and continuously detect network abnormalities before they escalate into major incidents [12].

Q-Day will be a groundbreaking day for humanity, but will also unleash unprecedented cybersecurity risks. Without proactive adoption of PQC, ZTA, and AI driven threat detection, organizations risk catastrophic operational, financial, and reputational damage. The following report will illustrate the power of quantum computing, accompanying threats, and considerations to assess.

2 Background and Varying Considerations

2.1 An Introduction to Quantum Computing

The two-photon double-slit experiment, first conducted by Thomas Young in 1801, revealed that light particles can exist in superposition and go through both slits, concurrently. More oddly, researchers found that measurement or observation of these light particles collapsed superposition, forcing one outcome. This groundbreaking discovery of superposition is the fundamental basis of quantum computing, in which quantum bits, or qubits, can exist as 0 and 1 simultaneously, in different proportions, ultimately determined by amplitudes [23]. Unlike classical computers, which use binary bits and processes one combination of bits at a time, quantum computers permit all parallel states to process concurrently. As a result, certain processes can be conducted in an exponentially faster amount of time with quantum computers and offer a wide range of results [22]. One applicable example is the use of Shor's algorithm which is run in polynomial time to find the prime factors of large numbers, a current process that would take classical computers billions of years to compute for practical examples [23].

For many organizations, the development of quantum computers will aid in solving complex problems, and overall have a net positive on their impact and performance. On the other hand, adversaries with malicious intent will utilize the power of quantum computing and Shor's algorithm to decrypt currently "unbreakable" cryptographic methods [23]. With intent to "harvest now, decrypt later", adversaries may also use preexisting methods or leverage AI to exfiltrate sensitive information at increased rates. Their efforts aim to stockpile and accumulate a repository of stolen data in hope of leveraging Shor's algorithm to decrypt the information when the opportunity arises.

At the time of this report, quantum computers are still being developed by private firms and academic institutions. Extensive research and development within the realm of quantum physics is applied to applications in computing [24] There are various projections for when quantum computers will become available commercially, with some estimating as early as 2030 [10]. As organizations deliberate ways that they can utilize quantum computers in their operations or to solve problems that are currently computationally infeasible, research and investment is being continually funnelled across the sectors of academia, in-

dustry, and government. The following organizations have received significant private and governmental investment to boost their research efforts: IBM, MIT, Google, and NIST [28][29]. The coming decade will reveal which organizations will steer and lead the commercialization of quantum computers, as well as which organizations or stakeholders will recognize its value, either maliciously or nonmaliciously.

2.2 Quantum Threats to Cybersecurity

Encryption is fundamental to information security and scrambles confidential data in order to protect access or modification by unauthorized parties. Within the CIA framework, encryption provides confidentiality by ensuring that third parties are unable to intercept data and protects the integrity by preventing alterations in transit. Encryption is a powerful method that allows networks to safeguard the transmission of data, ensuring that only parties authorized to access the information are able to do so. Modern public key encryption techniques heavily rely on the difficulty of factoring a large number, such as Rivest, Shamir, and Adleman (RSA), one of the most popular encryption algorithms used today. RSA is an asymmetric cryptography method that relies on a set of private and public keys. A public key is shared in the communication channel between 2 devices, allowing the messenger to encrypt using that key. The recipient can only decrypt that message by using a private key. RSA works by multiplying two large prime numbers, p and q, to create a value n which forms the foundation of both the public and private keys. The algorithm then generates two linked numbers: a public exponent (e) and a private exponent (d). To encrypt a message, one would raise the message x to the e and multiply mod n to obtain c, the encrypted message. To decrypt the encrypted message, one would raise c to d and multiply by mod n [30].

Classical computers are capable of running algorithms that factor these large integers, but the current process takes billions of years to complete. However, quantum computers can leverage Shor's algorithm and superposition to evaluate all possible factors simultaneously, a process that reduces computation time to just a few hours or days [4]. The power of quantum interference can be leveraged, where the amplitudes from the parallel states tally or cancel out in a methodical way to highlight the correct answers and eliminate the incorrect ones. Consequently, since public key cryptography is widely used by organizations across all sectors, it is critical that leaders distinguish current and future risks to discern their stance.

Since Q-Day will be unprecedented, organizations should adopt PQC methods as early as realistically possible. In a hypothetical scenario, adversaries who have motive and access to quantum computers may harness Shor's algorithm to decrypt existing public key encryption as a means or opportunity. Additionally, as Q-Day approaches, the number of attacks striving to exfiltrate and stockpile data will increase exponentially.

Especially in the context of espionage and political adversaries, nation states are already leveraging AI to expedite the number of attacks on their enemies

[19][27]. Threat actors are harvesting data today from their adversaries, with the hope of eventually obtaining the means or opportunity to decrypt these files later.

2.3 Future of Cybersecurity in a Quantum Era

Implementation of PQC algorithms will aid in diminishing the future unwanted outcomes or consequences that could be experienced by organizations. Inability to obtain PQC algorithms will warrant tremendous consequences for organizations, depending on the type of data decrypted by adversaries. Data breaches and privacy lawsuits are considerations that have the ability to cause insurmountable amounts of damage to organizations, either financial and/or reputational.

In addition to implementing PQC algorithms, organization leaders should implement zero trust architecture (ZTA) to address the security risks associated with modern cloud environments. Doing so will reduce the attack surface of their organization and minimize future impact of breaches, especially against the imminent threats produced by the eventual Q-Day. ZTA is built on the fundamental practices of authenticating every single access request, assigning least privilege, and microsegmentation of the network just to list a few. Organizations should consider migrating to ZTA as early as possible, as the timeline can be lengthy and stakeholders may be reluctant to adopt and convert. In the later part of this paper, frameworks and standards for rolling implementing ZTA from recognized organizations will be showcased [12][16].

Furthermore, artificial intelligence should be implemented along with PQC algorithms and ZTA, as machine learning can aid organizations in identifying behavioral patterns, various anomalies, and trends from data. An initial use case includes using AI to make classical encryption methods more resilient against standard decryption methods and brute force attacks. AI can also be used to develop algorithms or improve BB84 (a quantum key distribution protocol) to become increasingly resistant to quantum computers [9].

Without the implementation of PQC algorithms to safekeep the confidentiality of information, ZTA to protect against increased attacks, and implementation of AI to predict anomalies, organizations place themselves in a vulnerable and reactionary position. Early adoption and migration is crucial for organizations, as it can offer security advantages but increases challenges for leaders and stakeholders in terms of cost, technical expertise, and codependencies with legacy systems.

2.4 Frameworks and Standards for Transitioning to PQC for Security

Timely implementation of these frameworks and standards are crucial for organization leaders to ensure operational resilience and readiness. NIST's "NCCoE Migration to Post-Quantum Cryptography" project offers an introductory document to aid organizations in preparing for the transition of commonly used

encryption algorithms to PQC. The initial draft section outlines the tools that help streamline understanding of existing cryptographic methods. Implementation of such methods will enable organizations in verifying risks and determine the suitable PQC algorithms to consider. Overall, the framework provides guidance on measuring performance, understanding interdependencies, and permits organizations the ability to align with compliance expectations, since private and regulatory entities often use these same standards to assess benchmarks [13].

The subsequent section offers a structured test strategy that presents a subset of discovery tools that can be utilized to establish a benchline for performance. Additionally, the paper presents real life use cases developed in collaboration with leader organizations. High level architecture examples are provided along with methods for discovery and continued evaluation of potential threats. All these steps offer organizations guidance and demonstrate a proactive migration strategy [16].

Last but not least, the last section provides an approach for assessing and preparing for PQC adoption. Migration from current to QPC algorithm requires tools and processes in assessing compatibility matters, and NIST provides methods to resolve such issues in a controlled environment. Performance and risk evaluation is critical, and the document further offers guidance to ensure a stronghold transition [16]. This framework is a resourceful tool, but not a complete outline that IT leaders, security architects, and system administrators can use to administer their migration plan.

Beyond publicly available frameworks, private firms such as IBM and Microsoft offer enterprise solutions focused on migration efforts. For example, IBM provides commercial services that assess an organization's quantum readiness through its Quantum-Safe Readiness Index (QSRI) [7]. The company also offers end-to-end solutions designed to help their clients build the infrastructure and capabilities needed to achieve cryptographic agility in order to aid the shift in moving beyond a purely anticipatory approach [8].

Similarly, Microsoft has introduced PQC tools for both Windows and Linux operating systems, built on NIST standardized algorithms. These tools allow organizations to begin testing and adopting PQC methods in ways that best fit their operational needs. Rather than offering directly compiled solutions, Microsoft focuses on enabling a hybrid approach that incorporates both classical and PQC techniques [29].

Organizations ultimately have autonomy in determining an approach that aligns with their operational goals, risk tolerance, and financial constraints. While some may choose to partner with large providers that offer comprehensive enterprise scaled PQC migration services, others may rely on NIST's guidance and supplement support from smaller specialized firms. To reiterate, the appropriate path is dependent on each organization's technical environment, cost considerations, and support from leaders to adopt PQC solutions.

2.5 Challenges in Implementing ZTA and Countermeasures

Considering that threat actors can collect encrypted data today and decrypt it later using quantum computers in the near future, security engineers and IT leaders must take several considerations into account. Successful implementation or elevation of ZTA requires organization wide commitment. A common misconception persists that ZTA is only suitable for large enterprises, that it diminishes productivity, and that it does not warrant prioritization particularly among leadership. Many organizations also struggle to clearly understand their current architectural framework, including asset inventories and current user based credential roles. They are unclear on how their stakeholders, assets, and systems are connected with one another, and their susceptibility to exposures and potential threats. Technical blockages and challenges further complicate the process, particularly when working with legacy systems, fragmented infrastructures, and the absence of shared terminology or consistent assessment practices.

Despite these challenges, ZTA can be tailored to suit an organization's operations needs and risk tolerance. Leaders must evaluate trade offs and between increased security and its potential impacts on efficiency. Economists and leaders must work together to conduct cost-benefit analysis of these evaluations in order to determine the appropriate balance [25].

The lack of a fusion center or a security operations center (SOC) leads to challenges in contextualizing the current architecture of modern organizations. Both are essential for integration of cybersecurity tools, processes, and frameworks. Without these centers, documentation often remains obsolete for organizations, communication suffers, and leaves the organization without a clear, coordinated picture of its information operations. As the Software Engineering Institute (SEI) articulates, fusion centers centralize and unify diverse technical and nontechnical stakeholders within an organization, and permits for a proactive approach in addressing cybersecurity needs [5].

Lastly, organizations are not alone in navigating ZTA adoption. NIST highlights twenty four technology providers that offer tools and architectures to support ZTA integration and adherence. Implementation begins with a baseline architecture, with additional capabilities layered on to meet changing requirements and needs for varying organizations [16].

2.6 Challenges in Implementing AI and Considerations

The application of artificial intelligence for cybersecurity is an emerging field that continues to be actively researched and standardized. Machine learning and AI can be used to detect anomalies and suspicious behaviors by modeling off of historical data from events that occurred. Additionally, AI has the potential to enhance current PQC algorithms, create leeway for increase in resilience, even as quantum computing evolves.

However, the integration of AI into cybersecurity comes with several challenges. Firstly, AI systems require continuous training using reliable and high

quality data. This resource may be limited, particularly for organizations that have previously never encountered significant cyber incidents. In countering these limitations, organizations may consider participating in collective information sharing to strengthen their available threat intelligence. Next, often referred to as the "privacy paradox", data privacy is another point of concern as highly effective AI training requires access to personal or sensitive information to analyze threats or past incidents [9]. While this paradox proposes a challenge, organizations could employ synthetic data generation to generate artificial datasets or agents that can be used to train models.

Furthermore, ethical and regulatory considerations are critical. Human guidance is essential and necessary in defining moral and ethical boundaries for AI decision making. Current regulations and legal frameworks are slow to develop, leaving wide gaps in accountability and guidance. For example, should an AI respond to a cyber incident by prioritizing a network shutdown in order to prevent a major cyberattack, potentially disrupting services for many users, or should it risk continuing operations in order to maintain operational continuity? These broader ethical questions should be actively discussed between all relevant stakeholders.

Despite these challenges, the continued exploration and responsible implementation of AI in cybersecurity is crucial and necessary for staying ahead of emerging threats [15].

2.7 Adequate Planning for Anticipatory

For business leaders, the implementation of the mentioned solutions are dependent on the complexity and size of their organization. As an example, large enterprises and government agencies have legacy systems with complex cryptographic systems and architecture. These organizations should be aware of substantial codebase modifications, increased assessments, and extended testing periods. Some firms will struggle with computational resources, within sectors where system downtime is often believed to be more important than enhanced security. This challenge is especially apparent within the finance, aerospace, and healthcare industries and requires additional planning and anticipation [1].

Businesses in regulated sectors like financial, health and telecommunication are required to adhere to federal requirements such as HIPAA, GLBA, and FCC rules [3]. As these regulations evolve to account for quantum computing and threats, firms will need to begin adjusting their operations to comply. Failure to adhere to such changes can result in penalties and increased operational costs.

Leaders should also invest in fusion centers and recognize the value of cyber intelligence operations. According to the SEI, fusion centers help diminish information siloing of organizations, enabling information sharing and lead to proactive planning of cybersecurity solutions [5]. A mature fusion center often incorporates a security operation center (SOC) and is composed of stakeholders with diverse skill sets. These centers allow for a physical or virtual space where stakeholders can formulate preventive and anticipatory measures to protect their

organization. The SOC may focus on detection, response, and maintaining current operations [5].

Ultimately, business leaders are responsible and must govern in making the strategic investments necessary to prepare their organizations. They must fully recognize the importance of adopting PQC, embracing ZTA, and leveraging AI to strengthen their cybersecurity posture.

Fortunately, early adoption also presents advantages from an economic stance. Firms that implement PQC ahead of competitors can position themselves as market leaders in quantum safe security, enhancing customer trust and demonstrating a strong commitment to data protection. This differentiation may be particularly valuable for financial and healthcare organizations, where security maturity is often a key competitive factor.

3 Secure the Future with Urgency

Q-Day will inevitably impact organizations across every sector, by presenting the unprecedented ability to break classical encryption. The commercialization of quantum computers will be an incredible breakthrough for humanity. However, threat actors will harness their abilities by utilizing Shor's algorithm to compromise our current asymmetric cryptographic systems. Organizations that delay to implement PQC, ZTA, and employ AI defenses will face increased risks, including exposure of data, operational disruption, regulatory penalties, and reputational damage [26].

Organizational leaders should not wait as the window to prepare is narrowing and strategies to implement change are already available. Public frameworks and offerings from industry leaders are already available. In many cases, leaders must attain proactive investment, well informed decision making, and overcome challenging considerations to create meaningful progress.

Zero trust architecture is vital in countering "harvest now, decrypt later" attacks, as well as leveraging AI and ML tools to detect, respond, and evolve to threats. Such measures are not optional any longer, but rather foundational for resilience [21].

Q-Day will be a landmark achievement for society, but also a moment that will test organizational preparedness. Leaders who act now will safeguard their systems, preserve customer trust, and position their organizations for competitive advantage [18]. Those who hesitate will face consequences that are both avoidable and potentially catastrophic. Clear proactive adoption of PQC, ZTA, and AI driven threat detection is the path forward and essential in securing the future.

Works Cited

[1] Business Wire. "Post-Quantum Cryptography (PQC) Market Report 2025-2035." www.businesswire.com, www.businesswire.com/news/home/20250829766116/en/Post-Quantum-Cryptography-PQC-Market-Report-2025-2035-Legacy-Systems-Complexity-Challenges-PQC-Implementation---ResearchAndMarkets.com .

[2] CISA. "Post-Quantum Considerations for Operational Technology." CISA, www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf.

[3] Cryptopedia Staff. "What Is Blockchain Technology?" Buy, Sell & Trade Bitcoin, Solana, & Other Cryptos with Gemini's Best-in-class Platform | Gemini, www.gemini.com/cryptopedia/blockchain-technology-explained.

[4] Emerging Technology from the arXiv. "How a Quantum Computer Could Break 2048-bit RSA Encryption in 8 Hours." MIT Technology Review, 30 May 2019, www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

[5] Ettinger, Jared, et al. "Cyber Intelligence Tradecraft Report." Software Engineering Institute, www.sei.cmu.edu/documents/2846/2019_300_001_546590.pdf.

[6] Federal Register. "Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard." Federal Register, 14 Aug. 2024, www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based.

[7] IBM. "Quantum Safe Transformation Services." IBM, www.ibm.com/services/quantum-safe.

[8] —. "The Quantum-safe Clock is Ticking." IBM, www.ibm.com/thought-leadership/institute-business-value/report/quantum-safe.

[9] Li, Fangshu. "Application and Challenges of Artificial Intelligence in Cybersecurity." School of Electronic Engineering and Computer Science, Queen Mary University of London, (PDF) Application and challenges of artificial intelligence in cybersecurity.

[10] McKinsey and Company. "What is quantum computing?" www.mckinsey.com, www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing.

[11] Microsoft Security. "What Is Zero Trust Architecture? | Microsoft Security." www.microsoft.com, www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture.

[12] MIT Technology Review Insights. "Reimagining Cybersecurity in the Era of AI and Quantum." MIT Technology Review, 10 Nov. 2025, www.technologyreview.com/2025/11/10/1127774/reimagining-cybersecurity-in-the-era-of-ai-and-quantum/.

[13] Newhouse et. al, William, et al. "Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography." NIST Computer Security Resource Center | CSRC, 19 Dec. 2023, csrc.nist.gov/pubs/sp/1800/38/iprd-%281%29.

[14] NextGov. "NIST Selects 12 Companies for Implementing Post-Quantum Cryptography." Nextgov.com, 18 July 2022, www.nextgov.com/cybersecurity/2022/07/nist-selects-12-companies-implementing-post-quantum-cryptography/374601/.

[15] NIST. "Cybersecurity and AI: Integrating and Building on Existing NIST Guidelines." NIST, 22 May 2025, www.nist.gov/blogs/cybersecurity-insights/cybersecurity-and-ai-integrating-and-building-existing-nist-guidelines.

[16] —. "Mappings of Migration to PQC Project Capabilities to NIST Cybersecurity Framework 2.0 and to Security and Privacy

Controls for Information Systems and Organizations." NIST Technical Series Publications, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.48.ipd.pdf.

[17] Pfleeger, Charles P., et al. Security in Computing, 6th ed., Pearson, 2025.

[18] Quantumize. "The Benefits of Adopting Post-Quantum Cryptography." Quantumize, 3 Sept. 2024, www.quantumize.com/the-benefits-of-adopting-post-quantum-cryptography/.

[19] Radanliev, Petar. "Artificial Intelligence and Quantum Cryptography." Journal of Analytical Science and Technology, vol. 15, no. 4, 2024, https://doi.org/10.1186/s40543-024-00416-6.

[20] Rose, Scott W., et al. "Zero Trust Architecture." www.nist.gov, 10 Aug. 2020, www.nist.gov/publications/zero-trust-architecture.

[21] RSI Security. "Post-Quantum Cryptography & AI-Powered Cryptanalysis." RSI Security, 27 June 2025, blog.rsisecurity.com/post-quantum-cryptography-and-ai-powered-cryptanalysis/.

[22] Schneider, Josh, and Ian Smalley. "What Is Quantum Computing?" IBM - United States, www.ibm.com/think/topics/quantum-computing.

[23] Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." arXiv, 25 Jan. 1996, arxiv.org/abs/quant-ph/9508027.

[24] SpinQuantra. "How Many Quantum Computers Are There in 2025?" www.spinquanta.com, www.spinquanta.com/news-detail/how-many-quantum-computers-are-there.

[25] Stackpole, Beth. "Quantum Computing: What Leaders Need to Know Now." MIT Sloan, 11 Jan. 2024, mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now.

[26] Stanham, Lucia. "The Role of AI in Cybersecurity." www.crowdstrike.com,

www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/.

[27] Stöcker, Carsten. "Q-Day and Agentic AI: The Ultimate Nightmare in Cybersecurity." Spherity, 15 Sept. 2025, www.spherity.com/post/q-day-and-agentic-ai-the-ultimate-nightmare-in-cybersecurity.

[28] Swayne, Matt. "18 Leading Quantum Computing Research Institutions in 2024." The Quantum Insider, 25 Aug. 2024, thequantuminsider.com/2022/05/16/quantum-research/.

[29] —. "Microsoft Brings Post-Quantum Cryptography to Windows and Linux in Early Access Rollout." The Quantum Insider, 21 May 2025, thequantuminsider.com/2025/05/21/microsoft-brings-post-quantum-cryptography-to-windows-and-linux-in-early-access-rollout/.

[30] Wickramasinghe, Shanika. "RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained." Splunk, www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html.