



TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

The Encryption Crisis Nobody is Talking About: Why Pakistan Must Prepare for Post-Quantum Cybersecurity Now

A silent shift is underway in global cybersecurity — one that could render today's encryption archaic. The real risk is not the technology itself, but how unprepared we are for it.

By **Nimra Manzoor** | University of Agriculture Faisalabad | Published: September 2026

✉ nimramanzoor.tech@gmail.com | Position: Student Researcher

Introduction

Cyber Encryption is a silent backbone of our entire digital world and is used every time we execute a payment through electronic medium, access our computer, or send an email. Cyber Encryption is playing an increasingly vital role in facilitating secure electronic transactions in Pakistan, as banks, government agencies, and new companies are using electronic medium more than ever to conduct business. The problem is the lack of future viability with current Cyber Encryption Technology. Contemporary research indicates that the current common algorithms for Cyber Encryption such as RSA and ECC will have been rendered useless due to advancements in Quantum Computing, poised to radically change the environment of Cyber Security (Saeed & Alqahtani, 2026). The nature of this problem is compounded by the fact that the possibility of Cybercriminals exploiting Quantum Computing Technology as a means of compromising the current methods of Cyber Encryption already exists today.

"This is not hypothetical. It's an looming threat with a time delay."

For Pakistan, it's not just technology. It's the disconnection between global developments in cyber security and local capabilities - a growing, subtle, and deceptive gap.

The U.S. National Institute of Standards and Technology (NIST) states that advancements in quantum computing have the potential to disrupt currently established and common-use asymmetric encryption protocols, such as RSA and ECC, because an adequately powerful quantum computer will be able to solve the underlying mathematical problems at an exponentially faster rate than a classical computer would (NIST 2024). This potential has resulted in the fast-track development globally of Post-Quantum Cryptography (PQC) as the next generation cryptographic system which will be designed to remain secure from quantum attacks.

Technology Overview

Let's consider how encryption works today. Encryption systems such as RSA are based on problems that are hard for conventional computers to solve. There is evidence of this taking place around the globe today. As a result of the National Institute of Standards & Technology (NIST), PQC standardization is moving forward rapidly, including what will be the first sets of quantum-resistant cryptographic standards to be established at the end of 2024 (Areghan, 2025).



TABLE 1 — Traditional vs Post-Quantum Cryptography

Feature	Traditional Cryptography	Post-Quantum Cryptography
Common Algorithms	RSA, ECC	ML-KEM, Dilithium
Security Basis	Factorization problems	Lattice-based mathematics
Quantum Resistance	Vulnerable	Designed to resist quantum attacks
Current Adoption	Widely used globally	Early migration stage
Long-Term Security	Limited against quantum systems	Built for future resilience

In addition to this, the concepts associated with cybersecurity are also changing. The principle of trusting everything in a network has been replaced by the concept of implementing Zero Trust Architecture (ZTA), whereby every user, device and request must be authenticated. Together, these developments will result in an entirely new cybersecurity paradigm to include:

1. Quantum resistant encryption
2. Zero Trust principles
3. Crypto-agility (the ability to adapt quickly to new algorithms)

Indeed, the standardization process of PQC has picked up pace since the National Institute of Standards and Technology (NIST) decided on its first set of quantum-resistant cryptographic algorithms in 2024 (Aregban, 2025; Rustamova & Dutta, 2025)

Key Findings & Impact

One of the most critical findings in recent cybersecurity researches is the concept of:

“Harvest Now, Decrypt Later” (HNDL)

According to cybersecurity researchers, hackers could potentially have already begun gathering various encrypted financial documents, government comms as well as information that is stored in the cloud for future decryption once large scale quantum computing become available. This process is called Harvest Now, Decrypt Later (HNDL). Quantum computing has shifted from being considered a problem of the future to being a current and long-term security risk.

Rather than immediately breaking encryption, hackers are now stealing encrypted data with the hope that they can decrypt it at some point in the future with the help of quantum computers (Okika et al., 2025; Campbell, 2025; Kohli & Misra, 2025). This changes everything. This implies that data that is being sent today - financial data, user identities, and government data - could be compromised without the knowledge of the parties involved. A further insight is that the move to post-quantum systems is not equitable.

Developed countries are developing migration strategies, but many emerging developing nations are lagging behind due to a lack of resources, expertise and policy mechanisms (Ullah et al., 2025; Rustamova & Dutta, 2025). This poses significant danger for Pakistan Financial sector: confidentiality of data is very important in Banking and FinTech applications. Risk from Government: security of National Data Banks require decades of security to provide continued assurance to the public, on the ability of their data to remain secure. Startup risk: inconsistent policies and procedures for security can limit global confidence and growth. In addition, research has shown that encryption alone cannot prevent breaches. Without using Zero Trust Principles, systems remain susceptible to

insider and lateral network attacks (Nurhaliza & Darmawan, 2025). Therefore, the issue is not lack of awareness; the problem is outright failure to act.

'Harvest Now, Decrypt Later' (HNDL)

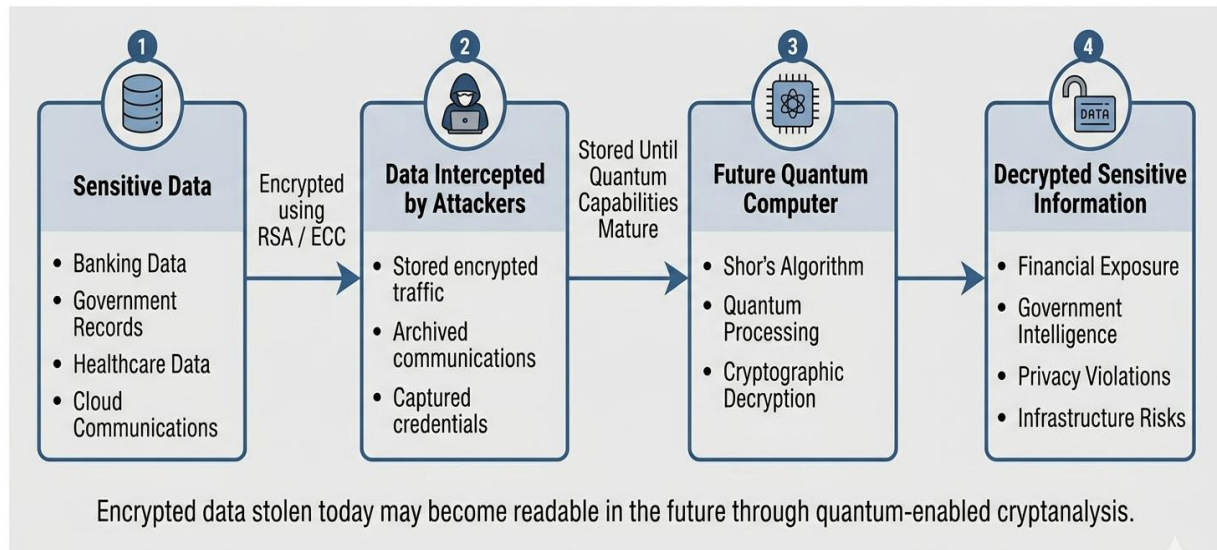


Figure 1: Illustration of the "Harvest Now, Decrypt Later" Threat model; where a cybercriminal steals encrypted data today, with the ability to decrypt it with future quantum computing capability.

Real-World Cybersecurity Lessons

The possibility of cybercriminals exploiting a company's reliance upon weak or antiquated cybersecurity systems has become a reality. In recent years, multiple high-profile cyber incidents from around the globe have proven that when organizations do not modernize their security practices, their digital infrastructure is subject to catastrophic failure.

One example is the WannaCry ransomware attack of 2017, which successfully infected more than 150 countries' networks and caused disruptions in the delivery of services to hospitals, banks, educational institutions, and governmental organizations. The attack utilized vulnerabilities in their legacy systems to demonstrate how easily critical infrastructures can be entirely incapacitated in a few short hours.

Another example is the SolarWinds cyberattack in December 2020, where various U.S. federal agencies were compromised because of a software supply chain vulnerability. The attack exposed the vulnerabilities of a newly developed digital ecosystem that was assumed to be sophisticated and secure from modern threats.

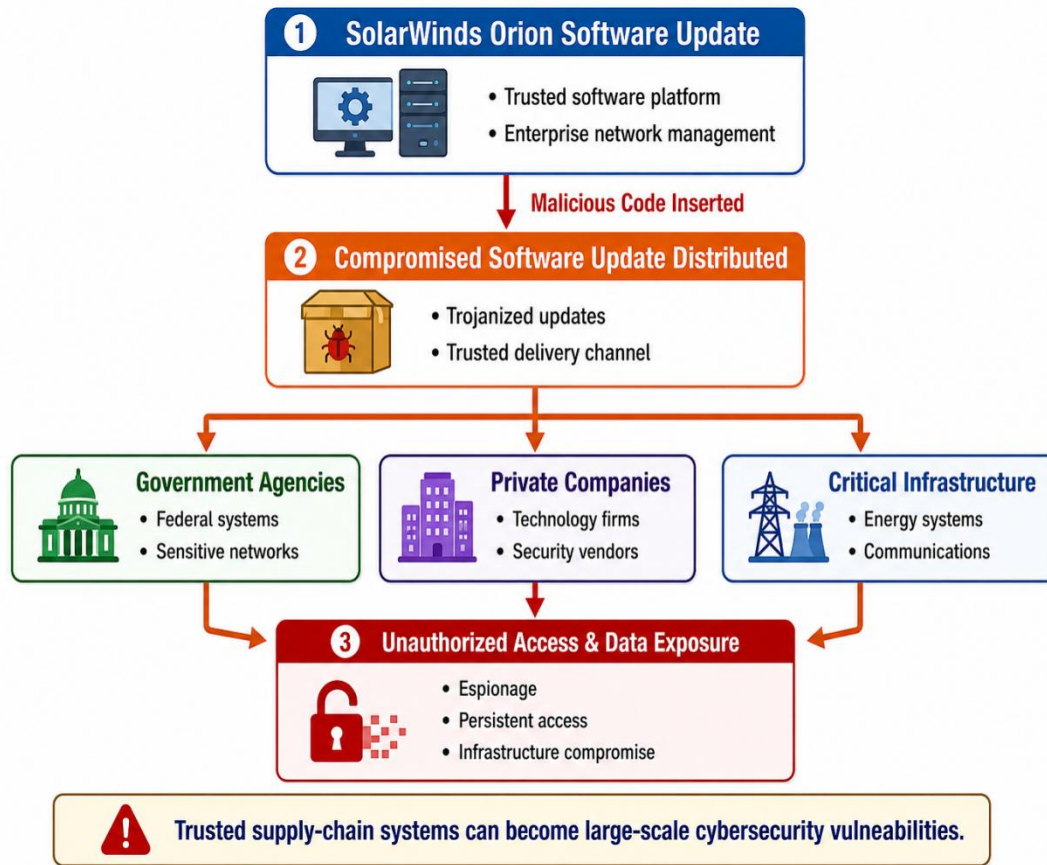


Figure 3: SolarWinds cyber-attack demonstrated how advanced intrusions can breach trusted digital ecosystems due to vulnerabilities in the software supply chain.

Pakistan has also faced an increased security risk due to several recent cybersecurity breaches. Among the most recent, in 2024, sensitive data belonging to Pakistani citizens and their associated SIM registration records were found posted to underground forums, creating concern regarding data governance, as well as the potential long-term risks of digital privacy and security.

Security analysts have consistently reiterated that emerging digital economies characterized by limited capabilities to recover from cyber incidents will be desirable and attractive targets for future data collection and theft campaigns.

Experts have also stated that the rise of quantum computing could subsequently cause these risks to become even more elevated, because when it becomes possible to utilize quantum-assisted attacks on data that is retrieved now, that data will also become accessible in the future.

Pakistan's Readiness Gap

The digital transition of Pakistan is continuing to grow at a rapid rate, as evidenced by developments in such areas as online banking, mobile wallets, cloud computing platforms and electronic governance systems. The data shows that there were over five billion digital retail transactions processed by the State Bank of Pakistan (SBP) in fiscal year 2023-24, indicating that Pakistan's reliance upon secure digital financial infrastructure increases every day. Presently, however, cybersecurity readiness has not developed at a comparable rate. As a result, many



institutions are still operating on legacy systems that were never designed to protect against the new emerging threat posed by quantum computing. Furthermore, many sectors still lack an adequate understanding of crypto-agility and post-quantum migration planning.

These have created significant long-term risks because records of financial transactions, databases containing information about citizens, systems responsible for providing essential healthcare, and strategic governmental information often need to be kept confidential for decades, not just years.

In contrast to other countries such as the United States, the European Union, and China, all of which have begun discussions about transitioning to a post-quantum cybersecurity environment, Pakistan currently does not possess any publicly available national roadmap outlining how to plan for a transition to a quantum-safe cybersecurity infrastructure.

Sector	Current Challenge	Potential Risk
Banking	Legacy encryption systems	Long-term financial exposure
Government Databases	Limited PQC planning	Sensitive national data risks
Universities	Limited advanced PQC research	Innovation gap
Startups	Inconsistent cybersecurity standards	Reduced global trust
Workforce	Shortage of PQC specialists	Slow migration readiness

What's Next?

This presents a problem that can be addressed; however, it will require both timeliness and urgency to address it. The recognition of quantum-resistant security as an issue that is immediate rather than one that is on the horizon. Companies must implement crypto-agile architectures that can switch to the most current cryptographic algorithms as they are developed (Jena, 2015).

Step 2 is to create a strategy for seamless migration. A hybrid approach of using traditional and post-quantum encryption allows for advancement without large-scale changes to a business' current environment. Step 3, develop Pakistan's cybersecurity capacity as such includes: Update education curriculum Development of strategic alliances to advance national cybersecurity strategy. This brings us to the final step: An opportunity exists for Pakistan to build system designs incorporating Zero Trust and post-quantum secure methods rather than retrofitting existing systems to address the crisis in encryption technology. Although it is not evident today, the issue regarding encryption will dictate the evolution of trust. When will it happen? The question is WHEN!

Many major tech companies are currently making significant investments in transitioning existing security solutions into post-quantum securities. For instance, Google has been testing hybrid post-quantum encryption methods within both Chrome and TLS communication protocols. Doing so will allow for the preparation of internet traffic that can eventually facilitate quantum safe communications in the future. Moreover, Google has also stated "that to maintain long-term confidentiality, organizations should begin preparing to migrate their existing infrastructure years before the first large-scale quantum computers become commercially viable".

Quantum-Safe Transition Roadmap

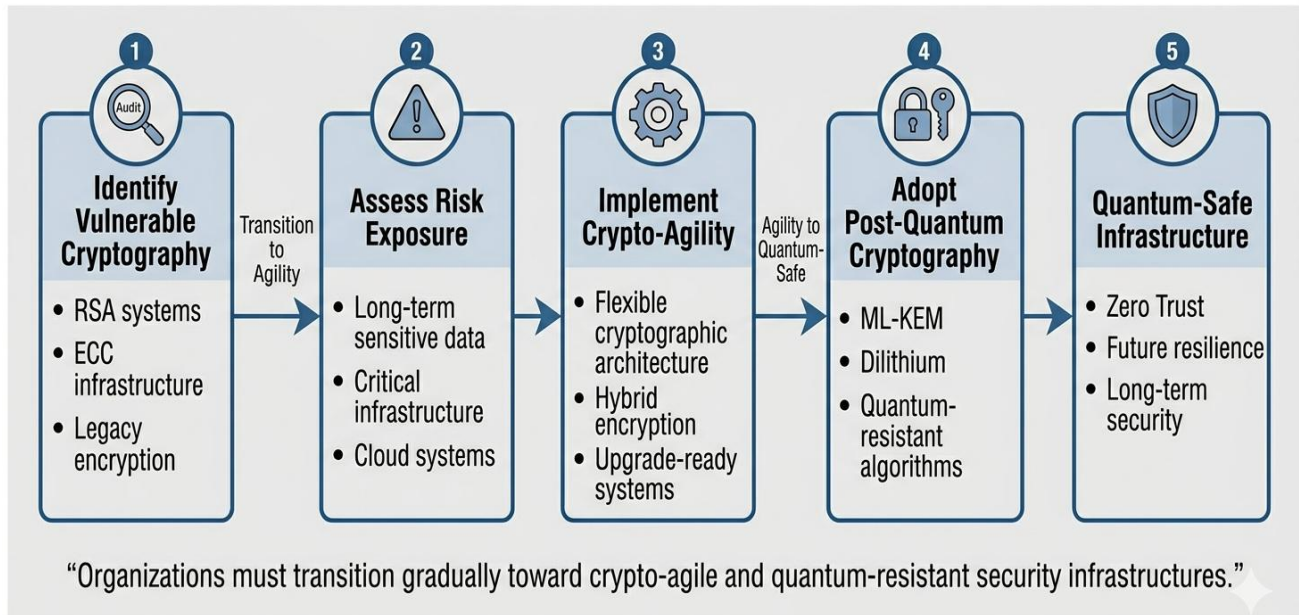


Figure 2: Organizational migration framework to crypto-agile and quantum-safe cyber security infrastructure.

Similarly, IBM has initiated their 'Quantum Safe' program, which will allow organizations to identify areas in which their cryptographic infrastructure is vulnerable and migrate towards more quantum-resilient solutions. IBM's researchers have also stated ***"that organizations should begin documenting their complete inventory of cryptographic assets now, as enterprise-wide migration may take many years to complete"***.

All the above show that the transition to post-quantum cybersecurity is not just a topic for future consideration but is now an urgent global security concern.

Conclusion

Rapidly evolving from breakthrough to delivering serious challenges to cybersecurity, quantum computing will become a major force in the development of our future. The advent of quantum technologies and the increased pace of innovation being achieved by both industry and government will likely render traditional encryption systems (RSA/ECC) ineffective at providing long-term protection of digital sensitive information.

The move toward ***"Harvest Now, Decrypt Later"*** illustrates that the transition to post-quantum encryption is not something down the road, but rather an emergent global security issue and growing concern that is already shaping the direction of cybersecurity strategies around the world. To respond to this challenge, organisations such as NIST, IBM, Google, and CISA are developing quantum-resistant encryption standards, migration frameworks, and crypto-agility security models.

From the perspective of Pakistan, the need to address this issue is immediate and strategic. In light of the increasing popularity and proliferation of digital banking, e-governance and cloud computing services, it is critical that organizations prioritize efforts to bolster their cybersecurity infrastructure. If preparation is not undertaken now, the risks associated with using outdated encryption systems could expose Pakistan's critical, national, fiscal and citizen data to significant risk soon.



In conclusion, preparing for the post-quantum era is not simply about a technological refresh but an investment in the future of digital trust, resilience, and national security.

About the Author

Nimra Manzoor is an IT student at University of Agriculture, passionate about cyber security and how technology can be made more secure. She can be reached at nimramanzoor.tech@gmail.com.

Keywords: Cybersecurity; Post-Quantum Cryptography; Encryption; Zero Trust; Quantum Computing; Pakistan

References

- [1] IBM. Quantum Safe Cryptography. <https://www.ibm.com/quantum/quantum-safe>
- [2] NIST. (2024). Post-Quantum Cryptography Project. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- [3] Google Security Blog. Experimenting with Post-Quantum Cryptography. <https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html>
- [4] CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a>
- [5] Okika, N., Nwatuze, G. A., & Olarinoye, H. S. (2025). Post-Quantum Cryptographic Systems and Zero Trust Security. https://www.researchgate.net/...Zero_Trust_S.pdf
- [6] Aregban, E. (2025). Emerging Frontiers in Cybersecurity. <https://www.academia.edu/download/123326076/ijatcse031432025.pdf>
- [7] Saeed, M. M., & Alqahtani, F. (2026). AI and Post-Quantum Cryptography for IoT Systems. <https://peerj.com/articles/cs-3502.pdf>
- [8] Inakollu, M. V. (2026). Implications of Quantum Computing for Cybersecurity. <http://pspac.info/index.php/dlbh/article/download/281/225>
- [9] Campbell, R. (2025). Enterprise Migration to Post-Quantum Cryptography. <https://www.mdpi.com/2073-431X/15/1/9>
- [10] Ullah, M., Ali, A., & Jadoon, A. K. (2025). Quantum Computing and Cryptographic Vulnerabilities. https://mpira.ub.uni-muenchen.de/127528/1/MPRA_paper_127528.pdf
- [11] Nurhaliza, N., & Darmawan, A. (2025). Zero Trust Adaptation for Post-Quantum Systems. <https://jetbis.al-makkipublisher.com/index.php/al/article/download/201/323>
- [12] Kohli, V., & Misra, S. (2025). PQC Integration in Zero Trust Architecture. <https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.176591845.57793075>