

THE QUANTUM CLOCK IS TICKING: IS MALAYSIA READY FOR THE NEXT FRONTIER OF CYBER THREATS?

Opinion

**VIKNESWARAN
KUNASEGARAN**
PROFESSIONAL FELLOW

Vikneswaran currently serves as Sr. Vice President at FIRMUS where he leads a team of consultants delivering security assessment services across Malaysia and the broader Southeast Asian region.



Data is money. The more data an organisation has, the more leverage is accumulated. From the context of cybersecurity, encryption is a crucial part of the digital world. Encryption protects data from being easily accessible by those who are not authorized to view the data. However, a new type of machine is emerging that can impact the current digital locks that are being used: The Quantum Computer.

To understand the threat, the first thing that needs to be understood is what exactly is encryption. There are two types of encryption: Asymmetric and Symmetric. Asymmetric algorithms use a pair of keys (public and private key) where the public key is used to encrypt, while the private key is to decrypt. However, the Symmetric algorithm uses a single shared key for both encryption and decryption. The quantum problem hits harder on the Asymmetric algorithms as this is widely being used as a "handshake" to establish connection between two parties for almost all types of secure communication known.

The main concern is HTTPS (the green padlock on websites to prove the website's legitimacy) which will be severely affected once Quantum Computing has reached its maturity. If Quantum Computing could crack open these encryption methods, there would be a privacy disaster.

In a traditional methodology, a thief must pick the lock, with all the right combination, one by one, to open and access the house. This can be slow, manual, and a very linear process which may not be effective as technology has advanced so much now. On the other hand, Quantum Computing uses a slightly different method, called qubits. Qubits on its own are limited, but once the quantum information is in a state of superposition, it has the capability to try every possible combination, simultaneously (IBM, n.d.). It is faster than what can be imagined. Currently Quantum Computing is heavily used in industries such as pharmaceuticals to speed up research and development of new life-saving drugs. Chemistry is another area where

Quantum Computing is thriving mainly to discover solutions to mitigate dangerous or destructive chemical byproducts and obviously, machine learning which our Artificial Intelligence is heavily relying on (IBM, n.d.).

Quantum Computing seems like a leap in human productivity, but in the wrong hands, it can be exploited in a manner that could severely impact individuals, organizations and even countries. Much like AI which is a dual-use technology, Quantum Computing falls under the same bracket. Threat actors (also known as hackers) are already at the frontier, conducting research and attack techniques using Quantum Computing.

One of the most dreadful techniques that was discovered, is a term called Harvest Now, Decrypt Later (HNDL). The concept is straightforward: attackers collect encrypted data today to decrypt it once quantum capability matures. What hackers do is that they compromise an organization (hack), collect all the sensitive information (especially those encrypted files, data, documents) and archive it (Palo Alto Networks, n.d.). Then it becomes a waiting game. Once the relevant Quantum Computing is accessible, able to be used, then the old data is used that was collected and try to decrypt it using Quantum Computing. This entire process is built on patience and perseverance where it is a calculated bet that the right technology will arrive to assist with the decryption. Unlike ransomware groups, these hackers do not make noise, issue announcements or shame the organization on social media. It is a silent, surgical digital operation that happens with minimal to no alarms triggered. The type of organisations affected by these type of attacks are financial institutions who store transaction records, customer personal identifiable information or a government agency that stores diplomatic communications, classified archives, government top secrets; even healthcare providers, who stores and protects medical records, genetic data, research datasets, patient data, etc. (Palo Alto Networks, n.d.). For these sectors, a breach today is an incident delayed, not avoided.

As HNDL is the most popular threat discussed in the Quantum Computing context, there is a lesser-discussed but more dangerous threat than HNDL out there.

It is called "Trust Now, Forge Later (TNFL)". If HNDL impacts the confidentiality of data stolen from an organization, TNFL impacts trust and integrity which is the fundamental principle of digital security.

How exactly can hackers forge? The mechanism is already available publicly. With the nature of Asymmetric algorithms, the public key is already available for users to use, store, trust and bookmark. It is mathematically impossible to forge today but with the rise of quantum computing, in the very near future, it is possible, using Shor's algorithm (Aditi Goel, 2026).

To put this into a daily context, the use of a smartphone OS update can put it into laymen's terms. Every time there is an update, there will be a message showing that a download may be installed and updated.. Behind the scenes, the smartphone and the server that pushes the update will perform a "digital handshake" before any installation happens. Each of these updates will have its own signature which will be verified before the installation happens. If the digital signature can be forged by an attacker, and the attacker sends a malicious OS update notification to the smartphone, the chances the notification would cast doubt would be minimal given the digital signature appears valid. The same scenario can happen to a personal digital signature as well. If that can be forged by an attacker, important documents may be signed: wills and loans that would be endangering without the knowledge of the original person. It would be very difficult and almost impossible to prove that the documents signed would not be from the actual authority as the digital signature would cement any doubts. This leads to identity theft which is getting more and more popular with all these eKYC (e-Know Your Customer) registration in place. All of this is made possible with the relevant quantum computing technology.

There is a threat that is closely related to Quantum Computing known as Cyber Kinetic Risk. By definition, it is the intersection between cybersecurity and physical safety. The threats discussed before are more focused on data loss, data theft, identity theft, unauthorized monetary transactions etc. Cyber Kinetic Risk, however, takes it one step higher. It can harm human life.

Human use of the power grid, water plant, nuclear power plant are all operating using Operational Technology (OT). Unlike a laptop or smartphone which can be changed every 1-2 years, OT assets are the opposite — built for longevity, often running for decades without replacement. It is placed with longevity in mind and usually the life span will cross 1-2 decades if not more. If an outdated OT asset is being attacked by hackers using quantum computing and are able to break the asymmetric algorithm of an industrial controller today, a mere password was not stolen, a privilege where malicious commands can be sent was accessed, thus making the scope to be harmful to humans or the environment viable. This may sound far-fetched — but it has already happened. In 2010, a famous computer worm named Stuxnet was found to infiltrate Iran's uranium enrichment facility at Natanz, causing the centrifuges to spin at incorrect speeds — physically destroying them while reporting normal readings to operators (Kaspersky, n.d.). One of the steps taken by the attacker was to ensure installation of files that were successful on the affected assets. The method used by stealing private keys to digitally sign the driver so it does not raise any suspicion or alerts where it denies the installation (Marco De Falco, 2012). With quantum computing, the hacker does not have to steal anymore, all that is needed is a public key and quantum computing capability: being able to crack a private key and using it to perform sophisticated and potentially undetected attacks. Routine attacks then become normal due to quantum computing capabilities.

The question remains whether or not there is protection from the threats that Quantum Computing poses. One of the major enhancements that needs to be done is the adoption of Post Quantum Cryptography (PQC). As the classic asymmetric algorithms can be broken, it is important to ensure the environment can support PQC. One of the preferred cryptography types under PQC is called Lattice-based cryptography due to its balance on strong security and efficient performance. It is also indicated that this particular cryptography is impossible to be broken by both classical and quantum computers for now (Palo Alto Networks, What Is Post-Quantum Cryptography (PQC)? A Complete Guide, n.d.). Other than PQC adoption, organizations have to start planning for the future and enforce PQC-supported

hardware and software before procuring. This is called cryptography agility. This means that vendors must start producing technologies (hardware, software and/or cloud environments) that can support swapping of encryption algorithms as and when required. This is also stated in the National Institute of Standards and Technology (NIST) whereby this agility mechanism will help organizations to exchange cryptographic algorithms without disrupting the infrastructure setup or infrastructure overhaul which can be costly (Palo Alto Networks, Cryptographic Agility: The Key to Quantum Readiness, n.d.). If there is an issue with any of the algorithms being used in the asset, a simple swap capability must be there to change the problematic algorithm and it should not disrupt the usage of the asset and the change must be seamless. Other methods such as hybrid cryptography can help in combating Quantum Computing threats. The concept is simple, wrap the classic algorithm within the post-quantum algorithm to create double-layer protection. This ensures if one of the algorithms is vulnerable (asymmetric algorithm), the other non-vulnerable algorithm will still be able to protect the encrypted data. This ensures interoperability and easy adoption to quantum cryptography which allows legacy systems to be secured while the full adoption is still in progress (Palo Alto Networks, What Is Hybrid Cryptography? | The Bridge to Post-Quantum Security, n.d.).

How can we prepare ourselves to face Q-Day (Quantum Day)? It is estimated that the Q-Day will materialize somewhere around 2029-2035 (Palo Alto Networks, Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat, n.d.). This is when quantum computing will be powerful enough to break the encryption algorithms available. This means there are less than 9 years to ensure technologies and protocols are quantum-proof (at least for the time being). The most fundamental step that needs to be taken is to create a Cryptography Bill of Materials (CBOM). As Software Bill of Materials (SBOM) intends to collect all of the software in use in an organization, CBOM focuses on collecting all cryptographic assets within the organization's ecosystem. This means that all symmetric and asymmetric algorithms, digital signatures, key exchange protocols in use, which may include third-party services, Software as a Service platforms and even cloud environments, must be identified.

This process allows an organization to have a complete list of the assets and its corresponding cryptographic information which can assist in performing a thorough risk assessment. The risk assessment will help the organization to prioritize critical assets that need to be upgraded to PQC first, identify vendors and clarify if their product will support PQC in future and decide if a shift in vendor and their technology is necessary, which asset/application cannot upgrade to PQC algorithm and what are the compensating controls for that situation. This is a very long process thus it is advisable for organizations to start now to avoid missing the PQC train (Rob Shapland, 2025).

Organizations in Malaysia are also putting in a lot of effort in relation to Quantum Computing. Starting from the government's effort, a total of RM 30 Million is allocated in the recent Belanjawan Madani 2026 under the umbrella of cybersecurity. One part of the allocation will be used to develop advanced cryptographic security services to protect individuals, businesses and national infrastructure (Ministry of Digital, Allocations In Belanjawan Madani 2026 Set To Spur Malaysia's Digital Transformation, 2025). This demonstrates that the government is aware of the upcoming threat in the digital space, and is making an effort to spearhead this program to ensure we are not left behind. Other than that, there is a homegrown product in relation to quantum computing named KAZ-SIGN, which is the country's first locally developed quantum-resistant digital signature technology (Muhammad Nur Syazwan Wafiy Mohd Aseri, 2025). Apart from that, CyberSecurity Malaysia has developed and published a document named "POST-QUANTUM CRYPTOGRAPHY MIGRATION FRAMEWORK" which helps organizations to understand what PQC is all about and how to structurally plan for the migration from classic to PQC enabled environment. It is quite comprehensive, touching on multiple different principles starting from the basics of PQC and moving towards the technicalities such as technical considerations, security considerations, regulatory and compliance considerations and many more (Cyber Security Malaysia, Post Quantum Cryptography Migration Framework, 2024). With all these efforts and significant investment on cybersecurity and quantum computing, it shows how Malaysia is moving beyond simple awareness, towards practical and tangible results in this field.

PQC is inevitable. Google is targeting to be PQC ready by 2029 (Jose Antonio Lanz, 2026) and the Q-Day is predicted to be somewhere around 2029 - 2035. This is a race between users and hackers to see who gets caught off guard. The cybersecurity community has witnessed many revolutionary threats, including WannaCry ransomware, EternalBlue exploitation, Log4J, Spectre and Meltdown (a critical hardware-based vulnerability which can be exploited) and many more. These were massive worldwide phenomena that happened which shook the cybersecurity industry. However, the Quantum Computing threat is different. It resets the whole digital world that we have been living on and building so far for decades. Looking at Malaysia's effort in keeping up with this technological threat is also promising that a top-down approach when it comes to cybersecurity in general is taken seriously. Now, it's no longer a question of "if" but a question of "when".

What happens when Q-Day arrives? The value of data will shift. It shifts from the hands of those who rightfully own it, to threat actors who patiently waited for Q-Day to crack that encryption. Every organisation that has chosen to delay its quantum readiness is risking its entire data estate — and the longer the delay, the costlier the migration will be. This is not an IT project as simple as plugging a new device into a network and watching it work. It is a process, and a hard decision that needs to be made by organisational leaders, governments, and security practitioners before the threat becomes visible.

References

IBM, Josh Schneider, Ian Smalley, (n.d.) What is quantum computing?, from <https://www.ibm.com/think/topics/quantum-computing>.

Palo Alto Networks, (n.d.), Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat, from <http://paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl>

Aditi Goel, 2026, Your Guide to Understand Trust Now Forge Later attack, from <https://www.encryptionconsulting.com/trust-now-forge-later-attack/#:~:text=If%20a%20hacker%20cracks%20a,so%20the%20hardware%20installs%20it>

Kaspersky, (n.d.), Stuxnet explained: What it is, who created it and how it works, from <https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet>

Marco De Falco, 2012, Stuxnet Facts Report: A Technical and Strategic Analysis, from http://ccdcocoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Palo Alto Networks, (n.d.), What Is Post-Quantum Cryptography (PQC)? A Complete Guide, from <http://paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc>

Palo Alto Networks, (n.d.), Cryptographic Agility: The Key to Quantum Readiness, from <https://www.paloaltonetworks.com/cyberpedia/what-is-cryptographic-agility>

Palo Alto Networks, (n.d.), What Is Hybrid Cryptography? | The Bridge to Post-Quantum Security, from <https://www.paloaltonetworks.com/cyberpedia/what-is-hybrid-cryptography>

Rob Shapland, 2025, How to create a CBOM for quantum readiness, from https://www.techtarget.com/searchsecurity/tip/How-to-create-a-CBOM#:~:text=CBOMs%20are%20especially%20useful%20when%20planning%20a%20Licenses%20*%20Cryptographic%20algorithms%20and%20key%20lengths

Ministry of Digital, Allocations In Belanjawan Madani 2026 Set To Spur Malaysia's Digital Transformation, 2025, from <https://www.digital.gov.my/en-GB/siaran/Peruntukan-Dalam-Belanjawan-Madani-2026-Akan-Merangsang-Transformasi-Digital-Malaysia>

Muhammad Nur Syazwan Wafiy Mohd Aseri, UPM Develops KAZ-SIGN, Pioneers Malaysia's Post-Quantum Digital Security, 2025, from https://upm.edu.my/news/upm_develops_kaz_sign_pioneers_malaysias_post_quantum_digital_security-90027

Cyber Security Malaysia, Post Quantum Cryptography Migration Framework, 2024, from <https://mykripto.cybersecurity.my/index.php/services/post-quantum-cryptography-initiatives/documents>

Jose Antonio Lanz, Google Sets 2029 Deadline to Deal With Quantum Threat—Is It a Problem for Bitcoin?, 2026, from <https://decrypt.co/362356/google-2029-deadline-quantum-threat-problem-bitcoin>