Quantum risk: a new digital threat that should not be overlooke

(Published on 5 November 2025)

By the Information Technology Audit and Cyber Risk Supervision Department,
The Securities and Exchange Commission, Thailand (SEC)

Advances in quantum computing are drawing increasing attention to a growing challenge in the digital landscape—"**quantum risk**." Once viewed as a distant concern, quantum risk is becoming increasingly relevant, as it may undermine the cryptographic[1] systems used today to protect personal data. This risk applies to all types of information that rely on encryption, ranging from passwords used in investment applications to sensitive investment-related data. For **users**, the potential consequences include the exposure or theft of their personal information and wealth. For **service providers**, the implications may extend to reputational damage, erosion of trust, and financial losses that may be difficult to quantify. As a result, quantum risk represents a significant challenge for today's financial sector.

Given the capabilities of quantum computing, it may pose a threat by undermining public key cryptography mechanisms widely used by most organizations, such as RSA and ECC[2], which are central to secure internet transactions and the protection of sensitive information. Once quantum computing becomes commercially accessible, encryption using any algorithms that are not resilient to quantum-enabled decryption (quantum-resistant algorithms, also referred to as quantum-safe) will become vulnerable—no different from using a safe without closing its door.

Quantum risk is a global issue. International cybersecurity authorities have therefore prepared two main approaches to addressing it, as follows:

1. Post-quantum cryptography (PQC): a software-based protective approach that establishes new cryptographic systems based on mathematical principles that even quantum computing may

---

1 The encryption process uses a pair of keys: (1) a private key, which must be kept confidential and known only to its owner, and (2) a public key, which functions like a house number and is openly shared so that others can send information to us.

2 RSA and ECC are widely used public-key encryption methods. RSA (Rivest–Shamir–Adleman) is an older and more commonly used method, whereas ECC (Elliptic Curve Cryptography) is newer and offers greater efficiency.

require thousands of years to decrypt—for example, multivariate techniques that use highly complex multivariable equations;

2. Quantum key distribution (QKD): a hardware-based protective approach that applies principles of quantum physics to create a completely secure communication channel between a sender and a receiver. This enables QKD to immediately detect any attempt to intercept data. However, QKD requires specialized infrastructure and has distance limitations. It is therefore suitable for specific use cases that require the highest level of security.

"Geopolitical tension" and national security motivations are another **accelerating factor** that may cause quantum computing to arrive sooner than expected. Major countries are accelerating investment and intensifying efforts to develop this technology in order to gain an advantage. If any country develops quantum computing that can decrypt its competitors' data first, it will gain advantages across economic, security, and intelligence dimensions. This accelerating factor may cause the "future" to arrive faster than anticipated. Therefore, the pace at which quantum computing may arrive cannot be assessed based solely on commercial factors. Although many organizations view quantum computing as still confined to laboratories and not yet relevant, some note that it may take another 10 to 20 years before quantum computing is commercially ready.

Advances in AI also affect the development of quantum computing, as they help enhance the potential of this technology and accelerate its progress toward commercial use. One example is the launch of Microsoft's QPU (Quantum Processing Unit), known as Majorana 1, which is small in size but offers processing performance many times greater than that of supercomputers. Although this QPU model has not yet been deployed for actual commercial use, it reflects technological progress and developments that are emerging in the near term.

Against this backdrop, many organizations question **why attention to quantum risk is necessary at this stage, when quantum computing remains under development**. The answer lies in the concept known as **"Harvest now, decrypt later (HNDL)"**—collect encrypted data now and wait until quantum computing can decrypt it in the future. This means that data that is secure today—whether customer data, legal documents, historical financial transactions, or even passwords (key algorithm)—may no longer remain secure in the future. Organizations should therefore promptly

assess the risk and plan data protection starting today, rather than waiting until quantum computing is widely available for commercial use and only then beginning to act.

Moreover, **damage does not occur only on the day encrypted data is stolen**. Encrypted data may become like a book that can be opened and read five to ten years later. The key question that executives must understand is therefore not, "Has the organization's data been encrypted?" but rather, **"Is the encryption currently used by the organization sufficiently robust to withstand the future capabilities of quantum computing (quantum-safe)?"** If the answer is "no," that means all data believed to be secure may have an expiration date, because it may be decrypted in the future.

The transition to the quantum era may appear significant and concerning, comparable to the Y2K period. However, the most immediate and critical starting point is **data risk assessment**, with the "time" dimension as a key element. This should begin with understanding the data held and prioritizing it as follows:

1. Data Inventory: What data is being stored? Where is it stored? And how is it protected?

2. Security shelf-life assessment: Organizations should consider: "How long must each type of data remain confidential?" "If the data held by the company is expected to face the risk of being decrypted ten years from now, would that affect the organization?" "If the organization's data that was found to have been compromised in the past—even if it was encrypted—could be decrypted in the future, would that affect the organization and customers?" If the answer is "yes," that is the point at which a protective strategy should begin.

- Daily transaction data may present low risk from a time-based perspective, because it loses importance within a short period and may require security for only three to five years.
- Customers' personal data (Personally Identifiable Information - PII), KYC/CDD data, biometric data, or long-term financial contracts may require security for as long as 10 to 20 years, or for the customer's lifetime.

This prioritization of data will help organizations plan investments in post-quantum security systems effectively. Data with high time-based risk should be protected first with encryption systems that are resilient to quantum capabilities (quantum-safe), while data with lower risk may continue using existing systems for some time.

Through this article, the SEC aims to raise awareness that organizations should not wait until quantum technology arrives. Instead, they **should prepare a transition plan that enables them to manage risk while balancing investment in safeguards.** This will be an important factor in enabling organizations to survive and grow in the quantum era that is approaching.
