# NCSC warns businesses of quantum computing threats to cybersecurity



The UK’s National Cyber Security Centre (NCSC) has issued a comprehensive warning aiming at businesses and government entities about the imminent threats posed by quantum computing, particularly in relation to cyber security. The agency highlighted the urgent necessity for organisations to prepare their systems against possible quantum hacking by the year 2035, amidst fears that advancements in quantum technology could fundamentally compromise current digital encryption methods.

In guidance released on Thursday, the NCSC recommended that critical infrastructure sectors, such as energy and transport, implement “post-quantum cryptography” to safeguard themselves from future quantum-enabled threats. The agency noted that quantum computers, which are still largely experimental, possess the capability to unravel the complex mathematical problems that form the basis of asymmetric public key cryptography. This form of encryption is widely used to protect sensitive information in various applications, including mobile phone communications and online banking transactions.

The NCSC explained, “While today’s encryption methods – used to protect everything from banking to secure communications – rely on mathematical problems that current-generation computers struggle to solve, quantum computers have the potential to solve them much faster, making current encryption methods insecure.” In light of this potential, the agency has urged organisations to take proactive measures to upgrade their systems by setting deadlines for implementation: services needing an upgrade should be identified by 2028, with significant changes expected by 2031 and complete migrations to new encryption systems by 2035.

Ollie Whitehouse, the NCSC's chief technical officer, commented on the importance of the agency's guidance, stating, “Our new guidance on post-quantum cryptography provides a clear roadmap for organisations to safeguard their data against these future threats, helping to ensure that today’s confidential information remains secure in years to come.”

Quantum computers differ fundamentally from traditional computers, which process information in binary bits represented as 0s and 1s. Quantum machines utilise qubits, capable of representing multiple states simultaneously, thereby enabling them to perform calculations at speeds previously unattainable. While current quantum technology is facing difficulties, such as vulnerability to environmental disturbances, significant investments continue to drive its development.

In addition to the risks associated with quantum computing, the NCSC has emphasised the need for organisations to begin preparations now rather than wait until quantum hacking becomes a tangible threat. The guidelines issued are intended to mitigate the potential chaos that might ensue from a hurried transition when quantum computing becomes more viable.

The Financial Times also reported that the NCSC underscored the necessity of awareness among organisations regarding the impending risks. It cautioned against underestimating the evolving threat landscape as quantum computing technology advances. A spokesperson from the NCSC noted that their timeline for migration to stronger encryption methods is more about ensuring readiness for mature technical solutions rather than predicting the regularisation of quantum hacking.

Global efforts are underway to establish robust encryption standards that can withstand quantum computing threats, with the US National Institute of Standards and Technology having already published approved security algorithms that can be adopted by organisations to secure their data. The NCSC's proactive approach aims to prevent a potential crisis due to insufficient preparation, advocating for a methodical transition to new security protocols rather than a rushed response to the advent of powerful quantum computers.

Moreover, concerns from various authorities, including Europol, highlight that quantum computing, alongside other emerging technologies such as artificial intelligence and blockchain, could enhance the capabilities of criminal operations, intensifying the urgency for organisations to act against potential vulnerabilities in their systems.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.techuk.org/resource/quantum-safe-symmetric-key-agreement-solutions.html> - This URL supports the claim that quantum computing poses a significant threat to current encryption methods and highlights the importance of transitioning to quantum-safe symmetric key agreement solutions.
* <https://thequantuminsider.com/2024/05/24/white-house-advisor-says-nist-to-release-post-quantum-cryptographic-algorithms-in-coming-weeks/> - This URL corroborates the information about global efforts to establish robust encryption standards, specifically mentioning NIST's role in releasing post-quantum cryptographic algorithms.
* <https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-post-quantum-cryptography> - This URL provides additional context on the need for post-quantum cryptography due to the potential of quantum computers to decrypt current encryption methods.
* <https://www.noahwire.com> - This URL is the source of the original article, providing context on the NCSC's warnings and recommendations regarding quantum computing threats.
* <https://www.justice.gov/archives/sco/file/1373816/dl?inline=> - This URL does not directly support the claims about quantum computing but is included as it was part of the search results; however, it is not relevant to the topic of quantum computing threats.
* <https://www.mass.gov/guide-to-evidence/article-xi-miscellaneous> - This URL does not support any claims related to quantum computing and is not relevant to the topic.