Cyber chiefs unveil new roadmap for post-quantum cryptography migration

New guidance from the NCSC outlines a three-phase timeline for organisations to transition to quantum-resistant encryption methods by 2035.

- NCSC issues new guidance to help protect against future quantum computing threats.
- Advice outlines a three-phase timeline for key sectors and organisations to transition to quantum-resistant encryption methods by 2035.
- Adoption of post-quantum cryptography (PQC) is encouraged, as current encryption standards – used to protect banking, secure communications and other sensitive data – are vulnerable to power of quantum computers.

The UK's cyber security agency has today issued new guidance to help the nation prepare for and protect against threats posed by future developments in quantum computing.

The guidance, published by the National Cyber Security Centre (NCSC) – part of GCHQ – emphasises the importance of post-quantum cryptography (PQC), which is a new type of encryption designed to safeguard sensitive information from the future risks posed by quantum computers.

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.

Migrating to PQC will help organisations stay ahead of this threat by deploying quantum-resistant algorithms before would-be attackers have the chance to exploit vulnerabilities.

The new guidance encourages organisations to begin preparing for the transition now to allow for a smoother, more controlled migration that will reduce the risk of rushed implementations and related security gaps. It outlines three phases for migration:

- **To 2028** – identify cryptographic services needing upgrades and build a migration plan.
- **From 2028 to 2031** – execute high-priority upgrades and refine plans as PQC evolves.
- **From 2031 to 2035** – complete migration to PQC for all systems, services and products.

NCSC Chief Technical Officer Ollie Whitehouse said:

> “Quantum computing is set to revolutionise technology, but it also poses significant risks to current encryption methods.
>
> “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.
>
> “As quantum technology advances, upgrading our collective security is not just important – it’s essential.”

For many small and medium-sized businesses and organisations, migration to PQC will be routine, as service and technology providers will deliver it as part of their normal upgrades. However, for some larger organisations, PQC will require planning and significant investment.

By taking proactive steps now, the UK can ensure its digital infrastructure remains robust and secure in the face of quantum advancements.

PUBLISHED

20 March 2025

NEWS TYPE

General news