QUANTUM-SAFE SECURITY: THE TIME IS NOW!

THE BIG TEMPTATION WITH QUANTUM COMPUTING IS TO TREAT IT AS A PROBLEM TO BE TACKLED FURTHER DOWN THE LINE. THE ARITHMETIC SAYS OTHERWISE, WARNS AJ THOMPSON, NORTHDOOR'S CHIEF COMMERCIAL OFFICER, AND A RECOGNISED VOICE IN CYBER SECURITY, DATA GOVERNANCE AND CLOUD STRATEGY

What exactly is quantum computing and in what ways does it differ from traditional computing?

A conventional computer works through problems in an orderly manner, reducing everything to ones and zeros, and testing possibilities largely one after another.

A quantum computer works differently. Rather than checking each answer in turn, it can explore huge numbers of possibilities at once. For a narrow set of extremely hard mathematical problems, calculations that would take today's most powerful machines thousands of years could be completed in hours or days. One such problem sits at the heart of online security.



AJ Thompson, Northdoor Chief Commercial Officer

Why is quantum computing seen as a potential threat?

Almost everything digital is protected by encryption, much of it relying on mathematical puzzles today's computers cannot realistically solve. A large enough quantum computer could. The threat is already present. Hostile states and criminal groups are stealing and stockpiling encrypted data, expecting to unlock it later. This is known as 'harvest now, decrypt later'. Information needing to remain confidential for five or ten years is already at risk.

Many nations are investing heavily in quantum computing, with the day fast approaching when it is anticipated most traditional public key cryptography (PKC) algorithms currently in use will be highly vulnerable to attack. How worried should we be?

Concerned enough to act, but not so alarmed that we freeze. Countries investing heavily in quantum recognise its strategic value, and it would be naive to assume that is purely scientific. Whoever builds a machine capable of breaking current encryption is unlikely to announce it, so we must plan for the day to arrive without warning. The good news is that a solution already exists. In 2024, the US National Institute of Standards and Technology (NIST) published the first encryption standards designed to withstand quantum attack, and providers such as IBM, which helped develop several, are building them into products. The worry is that most organisations have not begun applying them, and that work takes years, rather than months.

Why has the post-quantum deadline changed and what is the impact in the UK?

Two things have happened in quick succession. First, science has moved faster than expected. In March 2026, Google announced it was bringing forward its deadline for making its systems quantum-safe to 2029, citing progress in hardware, error correction and estimates of the computing power needed. Researchers have shown that the machine required could be a fraction of the size previously assumed. Secondly, governments responded. In June 2026, the US government issued an Executive Order requiring federal departments and their suppliers to move sensitive systems to quantum-safe encryption by the end of 2030.

For UK organisations, the impact is twofold. Anyone selling to the US government, or in the supply chain of a business that does, now faces a firm deadline. More broadly, the UK's planning horizon, with the National Cyber Security Centre targeting full migration by 2035, suddenly looks generous.

Did earlier deadlines create complacency?

Undoubtedly. When a target date is ten or fifteen years away, it rarely reaches the top of a board agenda. Quantum risk was filed as 'important, but not urgent'. The date itself was misleading. What matters is not when a quantum computer arrives, but how long your data needs to stay secret and how long it will take to upgrade your systems. Was the pace of progress a failure to recognise the risk, or a genuine surprise? I would not call it a failure so much as a human reaction to uncertainty. Expert forecasts varied widely and hype around quantum made some leaders sceptical. Governments and standards bodies spent the last decade developing and testing replacement encryption, so demanding mass migration before those standards were finalised would have been premature.



IBM Quantum Lab, Yorktown Heights, New York. Credit: Connie Zhou for IBM.



IBM Quantum Hummingbird processor. Credit: Connie Zhou for IBM.

What has caught people out is recent progress, particularly in error correction, which makes quantum machines reliable enough for useful work. The lesson is that security planning should never be pinned to a single forecast. It must allow for the possibility of being wrong in the unfavourable direction.

How many businesses have yet to prepare for a post-quantum attack?

The honest answer is: the overwhelming majority. Gartner found that only 6% of CISOs had carried out a post-quantum risk assessment and just 8% had a clear view of where encryption is used. More than nine in ten organisations have therefore not taken even the first step of understanding their exposure, let alone addressing it.

Some larger organisations in financial services, telecoms and government are further ahead. Most mid-sized businesses, however, and many suppliers on which larger organisations depend, have barely started. An organisation is only as secure as the weakest link in its systems and partners.

What should organisations do to stay safe?

- First, find out what you have. Most organisations lack a complete picture of where encryption is used, and you cannot protect what you cannot see.
- Next, identify what matters most: data that must stay confidential for years and systems hardest to change.
- Then talk to suppliers about their quantum-safe plans, and build those expectations into contracts and procurement.
- Systems should also be designed for flexibility, so encryption can be replaced without rebuilding everything.
- Finally, make it a board-level issue with a named owner, budget and timetable. This is a business risk, not just an IT project.

How does the IBM Quantum Safe and Northdoor process work?

IBM's researchers helped develop several of the new standards published in 2024. IBM Quantum Safe brings together the tools and methodology to put them into practice. Northdoor's role is to make that capability work across a client's real-world estate. The process has four stages: discovery builds an inventory of encryption in use; assessment identifies and ranks the highest risks; remediation replaces vulnerable encryption without disrupting operations; and ongoing governance and monitoring maintain visibility as standards evolve. The aim is lasting resilience.

How long would an organisation starting from scratch need to prepare for 'Q-Day', when a quantum computer can break today's encryption?

For a large organisation starting from scratch, full migration typically takes three to five years, and longer for complex, regulated or legacy-dependent estates. Set that against Google's 2029 timetable and the US government's 2030 deadline, and the arith-metic is uncomfortable. There is still time, if organisations start now and prioritise sensibly. Nobody needs to make every system quantum-safe overnight. Protecting the most sensitive, longest-lived data first reduces risk early, and discovery can often be completed within months. Those waiting for certainty will struggle. By the time a code-breaking quantum computer is confirmed, it will be too late to begin.

Are there positives to a post-quantum world?

Certainly. Quantum computing promises benefits from new medicines and materials to better financial modelling and more efficient energy and transport networks. The security challenge is the price of those advances and one we know how to meet. The migration is also a valuable opportunity. For many organisations, it will be their first complete inventory of encryption, uncovering outdated protocols, expired certificates and forgotten systems that pose risks today.

Those that complete the journey will emerge with stronger security, better governance and systems built to adapt to whatever comes next. They can also show customers, regulators and partners that their data is in safe hands. In a world where trust is a competitive advantage, that is no small thing.

Further reading:
https://www.northdoor.co.uk/partners/ibm/ibm-security-solutions/post-quantum-cryptography/

For practical guidance on preparing for quantum threats, watch Northdoor's 26-minute on-demand webinar with Professor Andy Stanford-Clark, IBM Distinguished Engineer, and AJ Thompson, Chief Commercial Officer at Northdoor. They explain where encryption is at risk and how to build a quantum-safe plan. **Watch at:**
https://www.northdoor.co.uk/quantum-safe-webinar/on-demand/