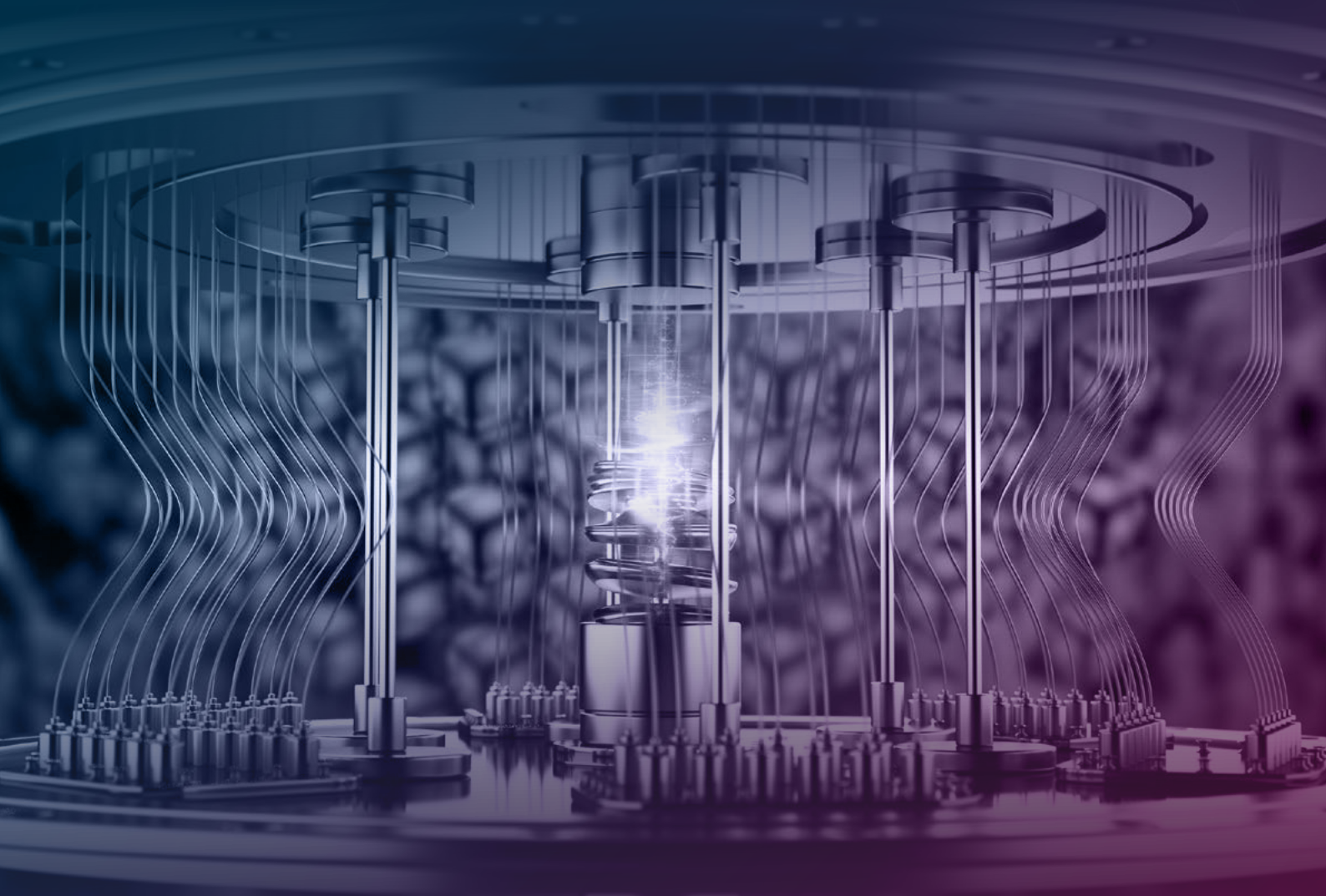
THE CHANNEL CO.

computing

– APRIL 2026 –

Is the UK ready for Q-Day



Exclusive research from Computing

By John Leonard, Research Director, Computing

Q-Day is the day when quantum computers become powerful enough to break public-key cryptography, which secures most online activities and data.

In the latest research from Computing, Research Director John Leonard looked at developments in quantum computing and cryptography, whether UK IT leaders believe the risk is real and what actions they are taking.

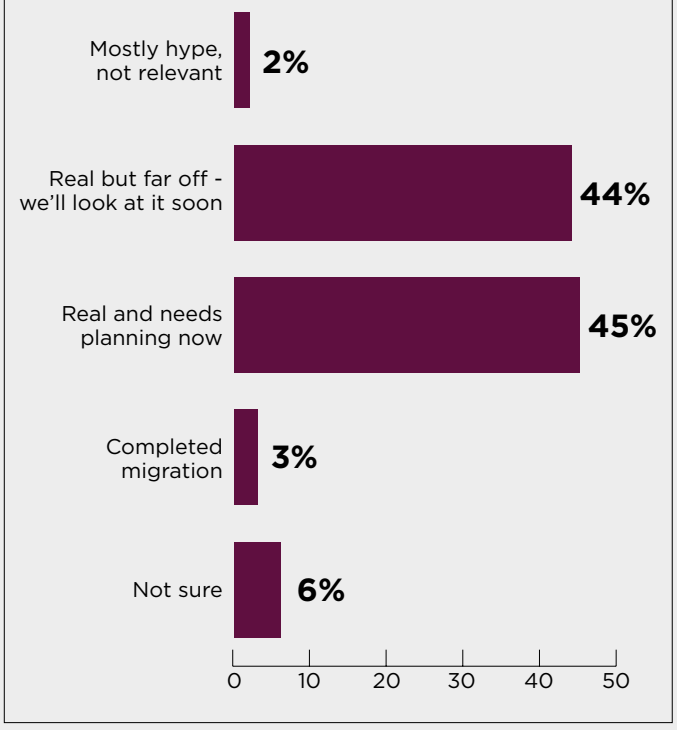
Key Research Findings:

- **Most people agree there's a risk of quantum computing cracking cryptography, but they're split on whether it's urgent**
- **Almost all expect to have migrated to quantum-safe cryptography by the NCSC's suggested deadline of 2035**
- **But most have not started yet, raising a big question mark**
- **Cost and competing priorities are the biggest blockers**

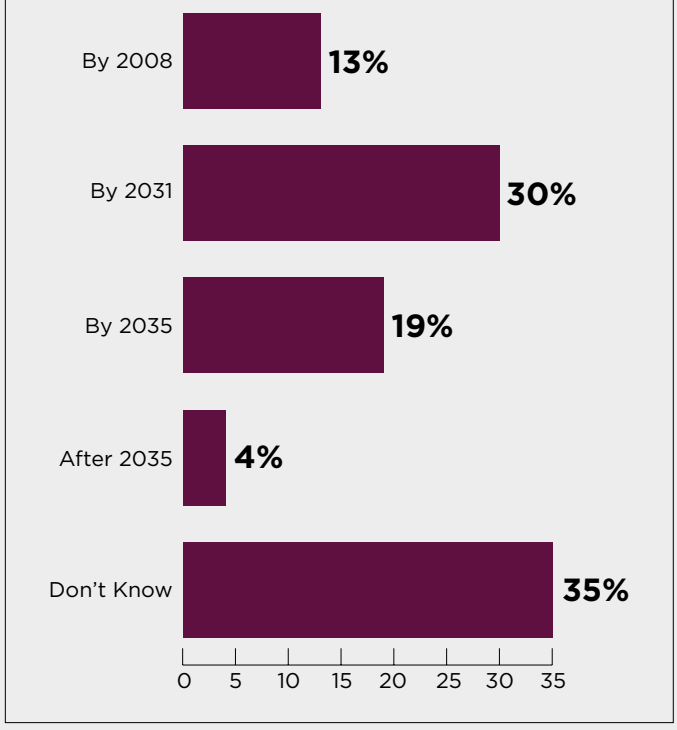
The research was carried out on 100 UK IT leaders roughly split between large and small-to-medium sized organisations and with 26% in the public sector. 37% describe their industry as highly regulated (e.g. finance, healthcare, government), and the same proportion said they must keep some sensitive data for 7 years or more.

Research Results

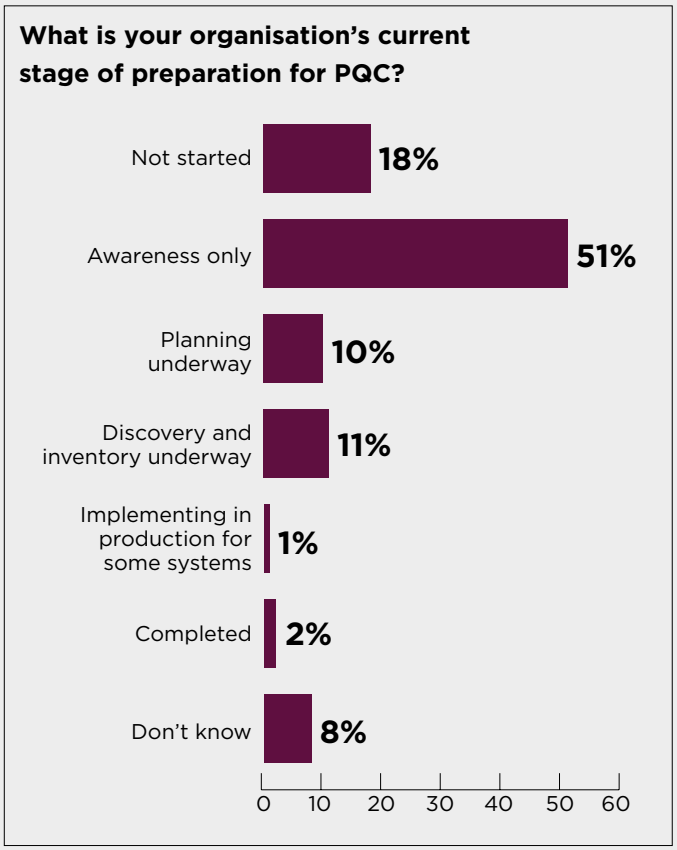
Which best matches your current view of the threat of quantum computing to encryption?

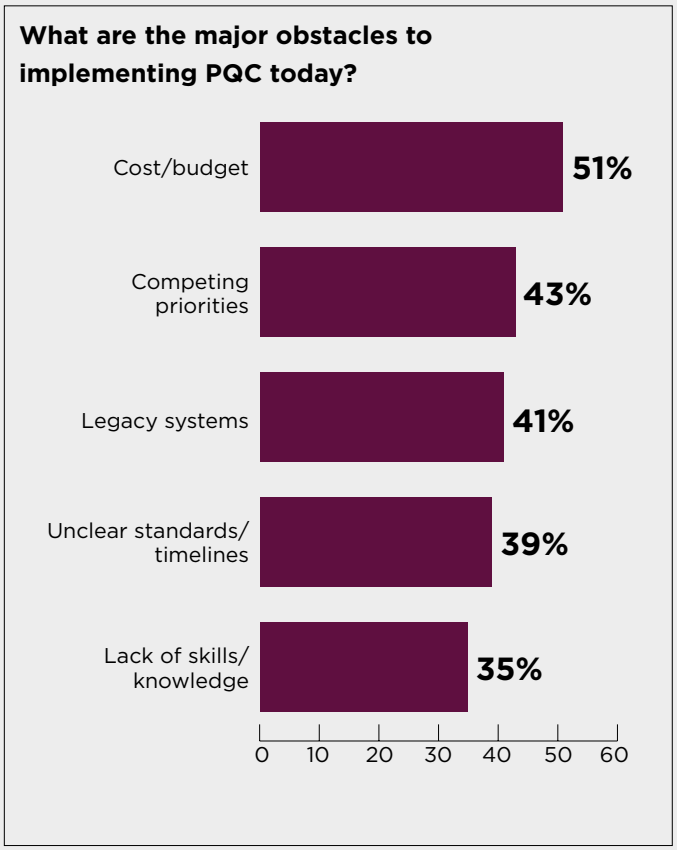


By which year do you expect your organisation to migrate fully to PQC?



Research conducted March 2026





Research conducted March 2026

What Does This Mean

Two per cent think the quantum risk is mostly hype, which is a perfectly defensible position. It's certainly not inevitable that quantum computers and software will be able to scale up as envisaged, and there are plenty of experts in the field who are sceptical that the formidable technical barriers will be overcome. Most respondents believe that quantum is a threat to encryption, but they're split almost exactly down the middle on whether the threat is urgent.

On paper, intentions look encouraging. 13% expect to move to post-quantum cryptography by 2028, 30% by 2031 and 19% by 2035.

But, in addition to the large number of "Don't knows", there is some cause for doubt.

Only a small minority are in the discovery or implementation phases, each of which could potentially take two or three years. Most are aware of the issue but not yet taking action, or are at the planning stage. Several respondents said they are waiting to be led by their vendors.

The biggest barrier cited is "cost", followed closely by "competing priorities". Most IT leaders have more security issues than they can effectively handle, so an additional problem with a nebulous timeline will not gain their full attention. 39% percent mentioned unclear standards and timelines. The timeline may be uncertain - although the NCSC and others are been clear about where organisations should be. But there are now approved standards to follow, so waiting for clarity may not be a defensible strategy.