How to achieve crypto agility ready for a post-quantum world

An action plan for protecting your data before and after Q-Day

Foreword

The quantum clock is ticking… and we don't know how long we've got left until Q-Day, when a quantum computer cracks the world of encryption wide open, putting vast amounts of data at risk.

I know many decision-makers won't even blink at that statement because the concept of quantum computing has been around for a while now, and it hasn't yet shaken their operating world. But this 'blindness' to its relevance is dangerous and could have significant consequences.

The quantum field is moving fast – perhaps faster than many realise. Seismic change is coming – and could be just around the corner.

Preparing for Q-Day must be a critical focus, but it's also important to grasp that the quantum transformation will reach far beyond data security. Just as classical computing is now a core part of every business, quantum computing will have the power to bring change to every aspect of an organisation - and society beyond.

Quantum's ability to compute differently, accelerate Artificial Intelligence (AI) and machine learning, and understand things at a molecular level will open avenues we're only now beginning to imagine. From near-instant and individualised logistical plans for vast global fleets to the rapid creation of personalised medication – the potential is eye-opening.

This is why quantum computing is everyone's business. Although security and IT decision-makers are on the frontline and may take the lead as the departments facing the most imminent risk, everyone needs to upskill themselves on the subject. A broad understanding of quantum computing's potential must run through the organisation so the C-suite can formulate a strategy that covers all possibilities.

We've put this paper together to get this whole-business conversation started and to share practical guidance as to what organisations should do next.

Together, we can prepare for Q-Day and lay the foundations for a successful quantum future.

Lee Stephens
Director, Security Advisory Services

Contents

What is quantum computing?

In many ways, it's easier to grasp quantum computing by outlining what it's not. It's not a supercomputer or a bigger, faster version of what we use now. Quantum technology is a whole new approach to computing.

With classical computing, data is processed in a binary space, where information is stored in bits that are represented by either a 0 (meaning 'off') or a 1 (meaning 'on'). This binary restriction limits the volume of data classical computing can handle and the decisions it can produce.

Quantum opens up new mathematical vistas

With quantum computing, qubits are the basic unit of information, and each qubit has a probability of being both 1 and O. When a quantum computer is working, the probabilities of multiple qubits interact and can be entangled into multi-qubit states – like ripples in water would bump and mingle if you were to tap two places on the water surface at the same time.

Quantum computers run algorithms based on the probability of a qubit's state before it's measured. Instead of trying all the options (which is the classical approach), a quantum computer watches those probability ripples interacting and finds the most likely answer.

For an unusual, but effective, way of understanding quantum computing, check out this link.

“If quantum mechanics hasn’t profoundly shocked you, you haven’t understood it yet.”

Niels Bohr, Nobel Prize-winning physicist

Grasp quantum's potential

Since quantum computing is a completely different way of running computations, it opens up new mathematical approaches to complex tasks that are beyond the scope of current computing.

A specialism of quantum computing is finding structure within tonnes of data. This means it'll be able to better predict the way nature behaves at a molecular scale. Together with its ability to accelerate analysis, quantum computing will revolutionise many fields of exploration.

Here's just a taste of its potential:

Faster AI and machine learning

Delivering accelerated automation and task optimisation at scale, especially with unstructured data sets.

Advanced financial modelling

Rapid insights into investments and securities at scale, providing a better understanding of the global trends and movements.

Optimised routing

Harnessing real-time data to individually plan routes for whole fleets across transportation structures and supply chains.

Accelerated product development

Delivering more accurate and realistic prototyping and testing, speeding up time to market and reducing costs.

Insight at a molecular level

Better models for how atoms interact will accelerate drug and chemical research, potentially driving bespoke medicine.

Next-generation batteries

A deeper understanding of lithium compounds and battery chemistry will advance battery manufacturing and increase battery capacity.

Quantum's potential is vast and inspiring, but the sweeping changes the quantum world will bring also open up new avenues of threat.

Broken encryption: The initial risk frontier

Encryption is the bedrock of most cyber security measures – and quantum computing threatens that security.

A hostile actor who could read encrypted information travelling digitally would have access to a world of critically sensitive information. From personal information such as medical records or bank account and credit card numbers to cutting-edge commercial research and classified national security information, all security and privacy guarantees would be void.

The problem: current encryption assumes only classical computing exists

Today, asymmetric encryption is the most commonly used form to protect data transactions worldwide. It works by multiplying two huge prime numbers to create large products using an algorithm such as RSA or Diffie Hellman. This type of algorithm generates a key pair, one public and one private, that is used to encrypt and decrypt data.

Cracking asymmetric encryption involves factoring large integers – a form of 'reverse multiplication' - to work out what prime numbers were used. However, with classical computing, there's no known way to do this due to the time it would take.

Once it's broken, it's broken

This picture shifted in 1994 when Shor's Factoring Algorithm arrived. As a strong algorithm for factorisation, it meant that, given enough advancements in quantum computing, it would be able to factor numbers in reasonable timeframes and break any asymmetric encryption.

Q-Day became an inevitability, recognised as the point when large quantum computers will be able to perform Shor's Factoring Algorithm to allow unauthorised access to any data in transit.

Once cracked, current asymmetric algorithms will be permanently broken, and the world will need alternatives.

How serious will Q-Day be?

On Q-Day, all networks secured using traditional encryption methods will be vulnerable to compromise. This goes further than it may first appear. In reality, any data that's been compromised up to that point, whether encrypted or not, could become readable. This will include any data that's been obtained on a 'store today, crack later' basis, so the implications spread far and wide, and are hard to quantify.

Could this be Y2K again?

The digital world has faced a similar situation before in the run-up to the year 2000. There were significant fears that the change of the century would obliterate computing and data security.

The term Y2K (short for the Year 2000) became shorthand for a problem stemming from the clash of the upcoming Year 2000 and the two-digit year format used by early coders to minimise the use of computer memory.

It was feared that computers would interpret the '00' in 2000 as 1900, creating chaos ranging from wildly incorrect calculations to large-scale blackouts and infrastructure damage.

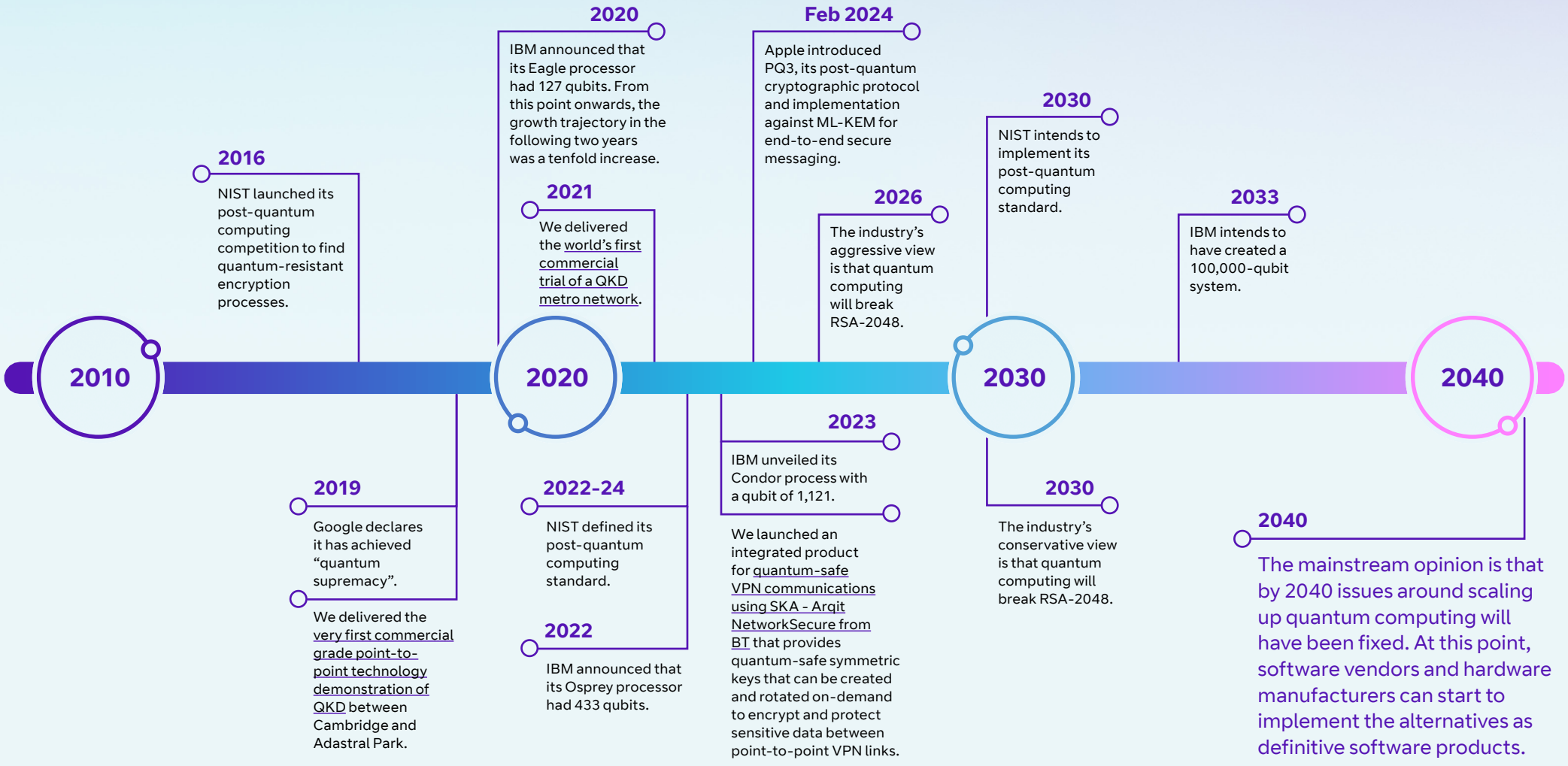
In the end, as the century turned, nothing serious happened and it felt like an anti-climax. However, what the general public didn't realise is that Y2K was only a 'non-event' because of the vast amounts of work done behind the scenes by specialists in the decade running up to the year 2000.

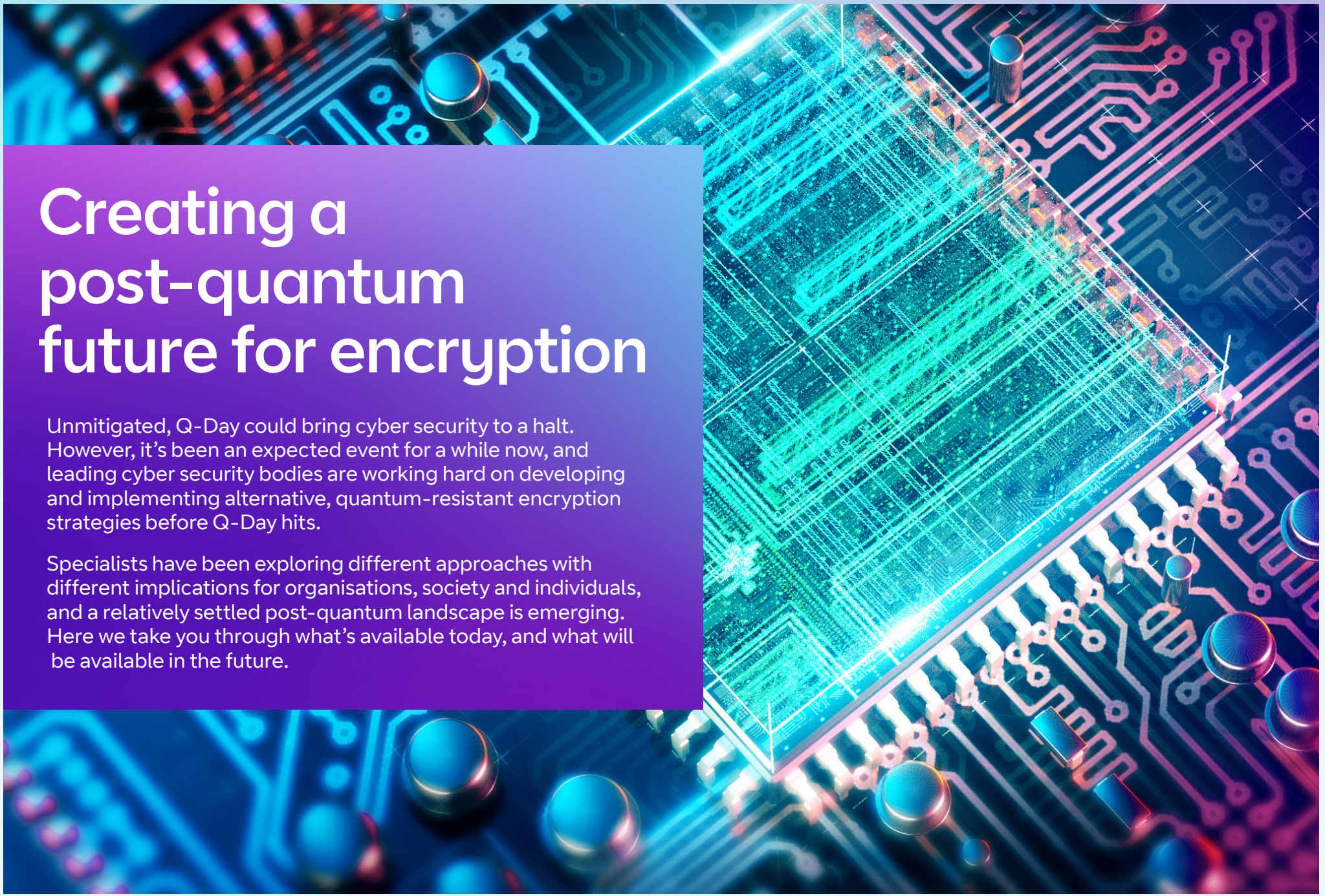
The ambition of the cyber security community is that Q-Day will be a re-run of this scenario, where careful and timely preparation neutralises the impact of quantum computing breaking current encryption algorithms.

So, how long do we have left before Q-Day?

The expected timeline for Q-Day

The key takeaway here is that the majority of experts believe that Q-Day will take place by 2030. As a consequence, research and development into quantum computing and post-quantum cryptography is on an accelerated trajectory.





Creating a post-quantum future for encryption

Unmitigated, Q-Day could bring cyber security to a halt. However, it's been an expected event for a while now, and leading cyber security bodies are working hard on developing and implementing alternative, quantum-resistant encryption strategies before Q-Day hits.

Specialists have been exploring different approaches with different implications for organisations, society and individuals, and a relatively settled post-quantum landscape is emerging. Here we take you through what's available today, and what will be available in the future.

The leading solution for most post-quantum encryption

The leading contender for a global solution is using symmetric encryption, which appears to be quantum-resistant. This uses only one secret key to both encrypt and decrypt electronic data. To work, both parties need the key to scramble and unscramble the data, but securely exchanging the key is the biggest problem.

NIST is taking the lead in finding a solution

The US National Institute of Standards and Technology (NIST), an eminent body in global cyber security governance and structure, is leading the search and implementation of a new, quantum-resistant algorithm to protect this key exchange and also digital signature processes (used to underpin proof-of-identity and trust on a network). This involves finding a new mathematical problem (not the factorisation of prime numbers) that neither classical nor quantum computers can solve and basing key encryption on that.

In their Federal Information Processing Standards (FIPS) 203, NIST sets out draft post-quantum cryptography standards for how encryption solutions should adopt a key-encapsulation mechanism (or KEM) that can be used with symmetric-key cryptographic algorithms. The FIPS 203 Standard specifies a KEM called ML-KEM that's centred on the extreme computational difficulty of Module Lattice problems. The agency selected four algorithms, designed to withstand attack by quantum computers, to standardise for widespread use.

> "Our post-quantum cryptography program has leveraged the top minds in cryptography - worldwide - to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."
>
> **Laurie E. Locascio**
> NIST Director

The significance of FIPS 203

Although the global cyber security community has known that NIST has been working on post-quantum cryptography solutions and standards since 2016, there was no collective agreement or certainty until FIPS 203 was published in August 2023. This marked the final step before the new quantum-safe mathematical tools would be available for global organisations to integrate into their encryption. It's expected that the standards will become the global benchmark for quantum-resistant cyber security across the world in 2024/5.

Apple joins the journey to quantum-safe cryptography

In February 2024, Apple announced "the most significant cryptographic security upgrade in iMessage history with the introduction of PQ3, a ground-breaking post-quantum cryptographic protocol that advances the state of the art of end-to-end secure messaging".

Apple's development uses post-quantum cryptography to secure both the initial key establishment and the ongoing message exchange. And should a key be compromised, Apple's system will automatically and rapidly restore the cryptographic security of a conversation. The protocol for iMessage also protects messages against 'store now, decrypt later' attacks and future quantum computers.

"We're getting close to the light at the end of the tunnel, where people will have standards they can use in practice."

Dustin Moody, NIST mathematician and project lead

Prepare for a permanent shift in encryption

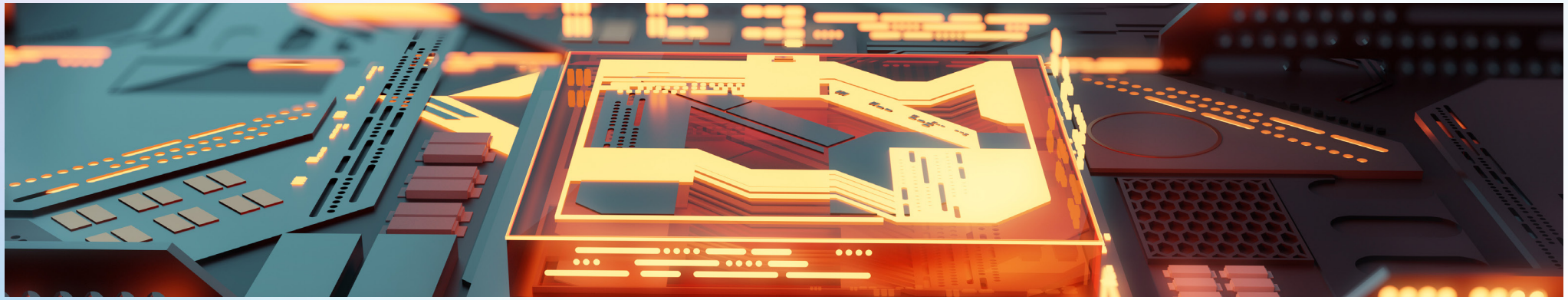
Post-quantum cryptography demands a new approach to securing data in transit. It will never be a case of finding a quantum-safe algorithm and relying on that indefinitely.

Global organisations will have to find ways to live with the fact that algorithms will be broken and replaced, repeatedly. The answer is to embrace crypto agility, where systems are ready to swap in new algorithms whenever necessary.

NIST has been very open about this future, launching a Post-Quantum Cryptography Standardisation Project to collaboratively develop robust cryptographic standards capable of withstanding the challenges posed by quantum computers.

As part of this, NIST is exploring replacements for algorithms at risk. These replacements are based on different mathematical problems than the first set to offer alternative defence methods should one of today's algorithms show a weakness.

This highlights the need for organisations to build agility into their systems so that they're ready to swap in new algorithms whenever necessary.



An overview of global progress

Post-quantum security is a priority for many nations, and significant investment and innovation is going into developing suitably robust forms of encryption.

Progress in China
China has an operational integrated space-to-ground quantum communication network over 4,600 kilometres with 700 terrestrial fibre Quantum Key Distribution (QKD) links. It claims it has 150+ users across four quantum metro networks and two QKD satellite-ground connections.

Progress in South Korea
South Korea's focus is on delivering QKD over 5G, applying QKD to its LTE network as a world first in 2016. It has subsequently applied QKD over a 330km section of its 5G backbone network.

A smartphone with Quantum Random Number Generation (QRNG) is available.

Progress in Europe
The EU began building a Europe-wide quantum network (known as EU-QCI) in 2023. It will interconnect 18 individual national quantum networks as they are constructed, with the intention that all 27 member states will join eventually.

Quantum-safe cryptography solutions available today

The ‘store now, decrypt later’ strategy employed by nation-states and cyber adversaries means some organisations need to take steps now to protect their data against the future cryptography-cracking potential of quantum computing.

To prevent cyber criminals from stockpiling their encrypted data today, they don’t want to wait for the completion of the NIST approach, so they’re opting to use quantum-safe VPN ‘tunnels’ to transmit data or investing in QKD.

There are currently two options:

1. Introducing our quantum-safe VPN solution

In partnership with Arqit, a leader in quantum-safe encryption, and Fortinet, a global leader in cyber security solutions and services, we’ve launched a quantum-safe VPN communications service using a symmetric key agreement. The service combines Arqit’s cloud-based software into Fortinet firewalls within our managed service, forming an add-on capability to our Managed Firewall service called Quantum-safe VPN Encryption.

At the core of the solution is the ability to create and rotate symmetric keys on demand to encrypt and protect sensitive data between point-to-point VPN links. This not only protects against future quantum threats, but it also defends data in transit from ‘store now, decrypt later’ attacks.

2. Using quantum itself to secure encryption

The ultimate route for protecting encrypted data against the capabilities of quantum computing is to use quantum technology itself to protect key transfer. This approach offers robust cyber security but requires significant network investment. However, it’s deployable today and may be considered the best option for organisations that need the highest levels of security assurance.

The power of Quantum Key Distribution (QKD)

QKD is a method of distributing quantum-safe encryption keys between parties, and it's the backbone of quantum-secure networks. Rather than relying on mathematics, it uses the quantum properties of light to generate secure random keys for encrypting and decrypting data, meaning that QKD-protected transmissions can never be intercepted and decrypted by adversaries. This makes QKD the most secure key establishment technology available today - other than using a physical courier to move keys.

Among its many positives, QKD - provided it is set up properly – ensures the keys used in public-key infrastructure are constantly refreshed, making it impossible to hack into the key. It's also capable of detecting and mitigating eavesdropping attacks, and it's likely to remain quantum-safe on a long-term basis.

However, QKD has technical limitations, and is only a partial solution at the moment. It doesn't currently provide a means to authenticate the QKD transmission source, and securing and validating QKD is a significant challenge. It also requires special hardware-based equipment and can't be implemented in software or as a service on a network, or easily integrated into existing network equipment.

Innovating for a QKD future

Our QKD work started with establishing the UK's ultra-secure Quantum Network Link (UKQNtel). In collaboration with the government and industry, we opened a commercial-grade quantum test network link between the BT Labs in Suffolk and Cambridge University in 2019.

This link forms part of the UK Quantum Network (UKQN) built by the Quantum Communications Hub and is used for testing and demonstrating new quantum technologies, such as QKD.

Our investigations include trials of how these technologies can be used to secure critical and sensitive data across vertical industry sectors such as healthcare, financial services, defence and logistics.

Introducing our Quantum Secure Network

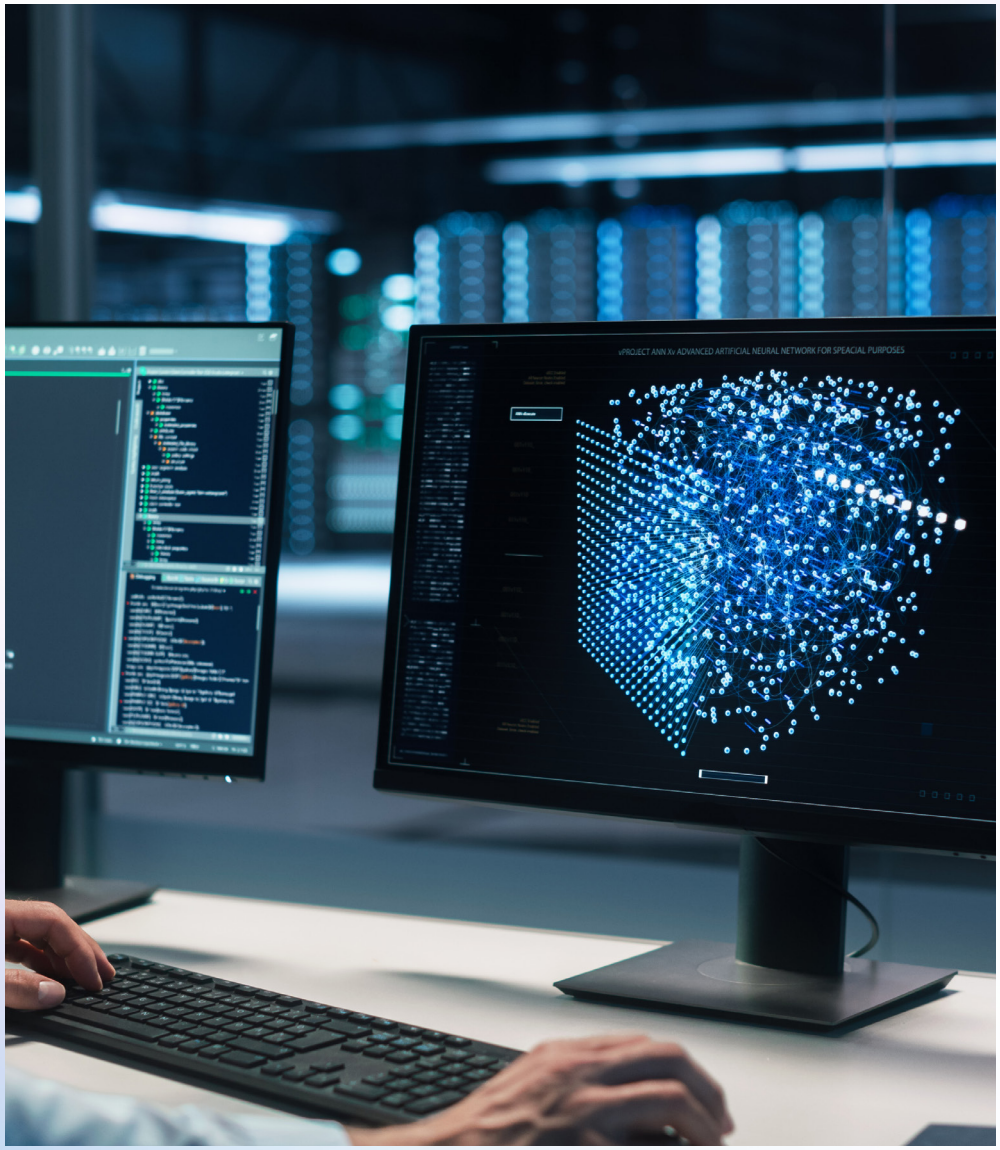
In partnership with Toshiba Europe Ltd, we built an industrial quantum-secure network between the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS), near Bristol, using BT Openreach's 'standard' fibre optic infrastructure.

The NCC was able to use QKD in combination with a standard classical algorithm for dual resilience during the trial, to transfer sensitive data relevant to the design and performance of a large-scale industrial component. It proved the suitability of QKD for real-world manufacturing applications, accelerating the shift to smart factories.

In April 2022, continuing our partnership with Toshiba Europe Ltd, we launched the London Quantum Secure Network - a trial London Metronet area network able to deliver key material to customer sites, incorporating high-speed, high-performance encryption and data transmission.

EY became our first commercial customer to connect quantum secure data transmission between its major London offices. The Metronet is demonstrating how data secured using QKD can move between sites, in a way that's future-proofed against the threat of an adversary equipped with a quantum computer.

This commercial trial is ongoing and is open to new organisations who wish to get involved.



Crypto agility is critical to post-quantum security

After Q-Day, secure encryption will become a much more fluid state, needing constant monitoring and adjustment. All organisations will need to make a shift in their approach to actively adopt crypto agility – the ability to quickly react to cryptographic threats by implementing alternative methods of encryption.

> "We need to be preparing now so that even the data we have today is quantum proof tomorrow."
>
> **Matt Scholl**
> Chief of the Computer Security Division, NIST

Practical steps to prepare for Q-Day

Achieving crypto agility isn't like flipping a switch by purchasing a new solution that fixes the issue. Instead, organisations will need to move along a pathway to reach the end goal of post-quantum readiness through crypto agility.

Our security experts break this down into a four-step process:

1. Raising awareness of risk

Up until recently, understanding the implications of Q-Day has been limited to practitioners within the security world. And even though security teams will need to take the lead, it needs to become an issue for the whole senior leadership team.

This starts with the security team doing a deep dive into the topic so they're prepared to answer any senior leadership questions and can frame this information in the context of what it means for the whole organisation.

A key part of this will be thinking carefully about who needs to be included in conversations about post-quantum encryption, and championing the issue so that it gets their attention.

2. Understanding your organisation's use of encrypted communication

A vital step towards crypto agility is understanding how your organisation could be affected by Q-Day. This involves preparing a comprehensive inventory of your cryptography, so you know exactly where and how cryptography is used throughout your IT environment. It's only at this point that you'll be able to make conscious and informed decisions about how and what to update.

This may be a new exercise for your teams since, historically, implementing cryptography has simply been a case of ticking a yes / no box in response to a standard question of 'Do you want this to be secure?'. However, it's essential to implementing post-quantum cryptography.

It's important to remember that ensuring security post-Q-Day won't necessarily be a simple matter of swapping classical algorithms for quantum-safe alternatives. In some cases, you may need to layer quantum-safe updates on top of existing classical security measures. In others, you may need to modify your whole cryptographic architecture. But you can't make these decisions without a detailed understanding of your cryptography estate.

3. Assessing your organisation's risk profile

Pairing a detailed inventory of your current encryption of data at rest and in transit with a broad risk assessment will allow you to prioritise actions and move to protect your most critical assets first. As part of this, you'll gain visibility into any obsolete or weak encryption systems you have, and be able to find, classify and analyse risks in real time.

These core questions will guide your assessment:

- Where are your most pressing risks that need tackling first?
- What intermediate steps might you need to take on the way to Q-Day preparation?
- What data would benefit from the additional protection of layered encryption systems?

4. Creating a road map to post-quantum encryption methodologies

Armed with a deep understanding of your organisation's current encryption position and risks, you'll be able to formulate a road map to mitigate the effects of Q-Day.

Your quantum partner

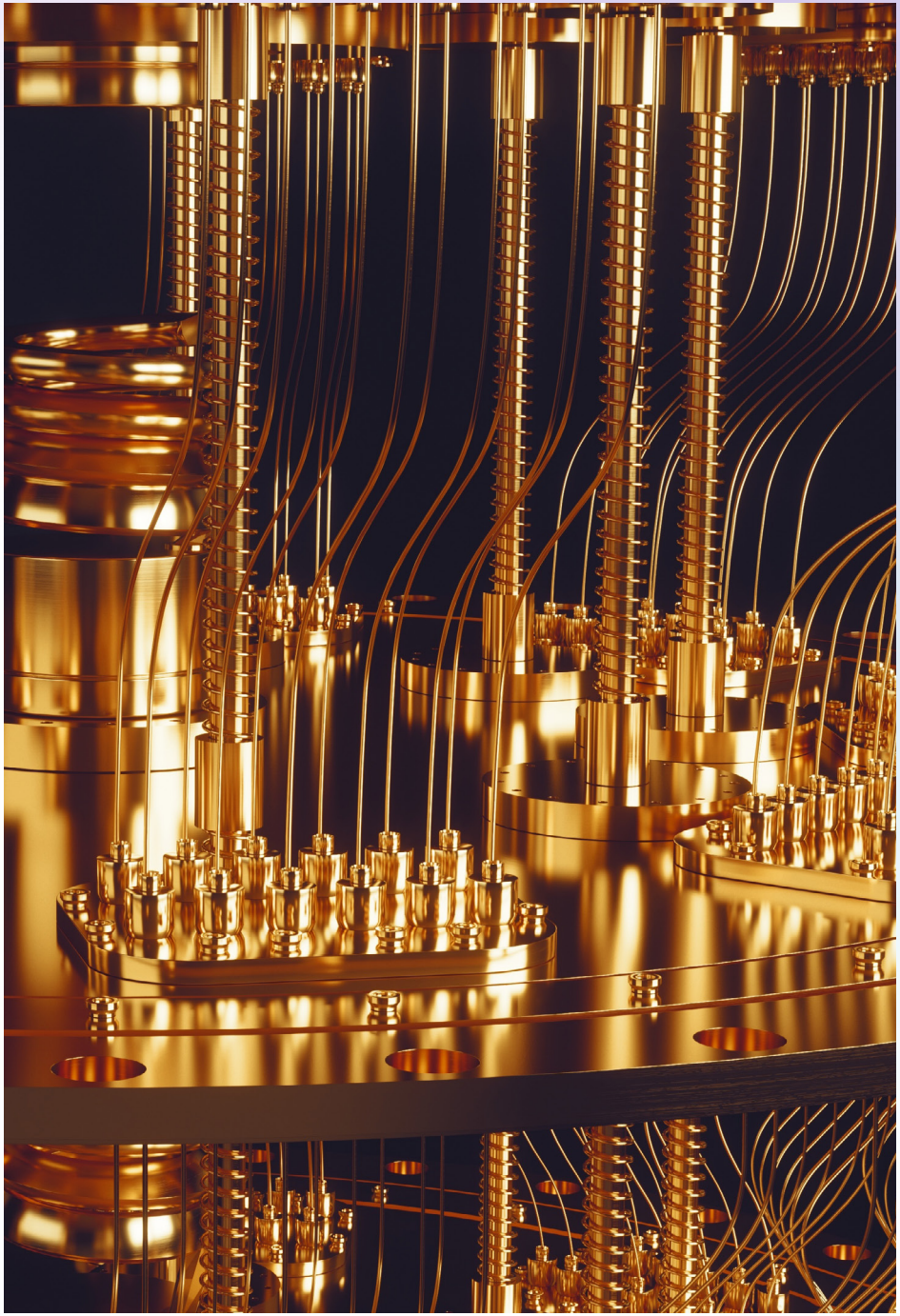
As a trusted advisor to governments and global organisations, we're actively extending our role into the quantum world and have been involved in quantum computing and quantum-safe encryption for some considerable time.

Part of our global watching brief includes scanning the horizon for emerging technological advancements and shifts, so we're closely monitoring any developments in the standardisation of post-quantum cryptography. We also continue to liaise with global bodies to further the debate and find viable solutions.

At the core of Q-Day preparations

We're part of a rich, UK quantum ecosystem that stretches across academia, start-ups, scale-ups, inward investors as well as governmental and publicly funded bodies:

- founding member of the UK Quantum Group
- member of the National Quantum Technologies Programme
- member of the National Quantum Computing Centre Technical Advisory Group
- partner with the National Physical Laboratory (NPL), a body that's playing a critical role in achieving the Government's quantum ambition. We support thinking around the standardisation, central testing and measurement services that will be critical for suppliers to bring quantum products to market.



Get post-quantum ready

To work out the implications of Q-Day for your organisation, get in touch to set up a discussion with our Security Advisory Services team.

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

May 2024