techUK

10 St Bride Street
London EC4A 4AD

techUK.org | @techUK

Media Contacts
Margherita Certo
T: (+44) 07462107214
E: margherita.certo@techUK.org

Press release

FOR RELEASE: 4 September at 00:01 AM

techUK's new report sheds light on how businesses can become quantum resilient

- *Businesses need to prepare for the potential threat of quantum, says techUK*
- *The report shares practical recommendations for business and government to navigate the challenges posed by quantum technologies, while recognising the opportunities quantum could bring*

LONDON, 5 September 2024: Businesses need to begin to prepare for the potential cyber security threats of quantum, says technology trade association techUK, in a new paper published today.

Titled "**Industry Perspective: Preparing for Quantum Resilience**", the report provides insights into the security challenges posed by quantum technologies and offers a practical overview for businesses and governments alike.

As the UK strives to position itself as a global leader in quantum technologies, it is imperative to ensure that quantum deployment is safe and secure. Alongside the opportunities quantum technologies may bring, they also pose significant cyber threats. Quantum computers could potentially breach encryption keys safeguarding sensitive data, compromising the integrity of digital documents, financial transactions, and personal information.

techUK states that an enhanced use of post-quantum cryptography sits at the heart of quantum safety. As quantum technologies develop, it is possible they will break cryptography in the years to come. While we cannot predict how or when this will happen, it is important that businesses take this seriously and are empowered to prepare for quantum resilience.

The potential solutions

The quantum and cryptography communities have been preparing for the quantum threat through defining and standardising quantum-resistant solutions, including post-quantum cryptography (PQC). Following the long-awaited guidance from NIST, techUK sets out the current state of play and what this means for businesses. It also explores and myth busts quantum random number generation (QRNG), and quantum key distribution (QKD).

Businesses are facing cultural, organisational and technical challenges that hinder the move towards quantum resilience. Consulting its members, techUK has found that the tech sector is currently facing barriers such as:

- skills shortfalls across both the cyber security and quantum domains;
- the infancy of quantum technologies and unclear timelines for becoming quantum secure;
- a lack of understanding around where, why and how businesses are currently using cryptography;
- a lack of understanding around when and how businesses should invest in quantum-security measures; and

difficulty in conveying why investment is needed when budgets are tight and the quantum threat remains intangible to most C-suite executives.

How the UK Government can support

While the government has already provided support to businesses to face the cyber security challenges posed by quantum technologies, such as the National Quantum Strategy and the '*Next steps in preparing for post-quantum cryptography*' guidance published by the National Cyber Security Centre (NCSC), the UK cannot be complacent. As quantum technologies advance and other nations invest robustly in cyber resilience, techUK calls on government to collaborate with industry to:

- **Deliver guidance:** government should continue to prioritise the publication of guidance from the National Protective Security Authority (NPSA) and the NCSC on how all organisations should prepare for the quantum transition, including clear steps for raising awareness of the challenges as well as more technical 'how-to' security guidance for companies; and
- **Develop a Quantum Resilience Taskforce:** government and industry should convene a workstream or forum to come together to collaborate on the challenges of quantum technologies at the earliest opportunity, developing key metrics for success and strategy.

By fostering collaboration between government, industry, and academia, the UK can maintain its position as a global leader in quantum innovation while safeguarding against emerging cyber threats.

Next steps for businesses

In the report, techUK also sets out the following recommendations for businesses working towards quantum resiliency:

- **Ensure access to key skills:** the sooner organisations start seeking the appropriate guidance or talent, the better. A key starting point could be agreeing who within an organisation is responsible for the quantum transition.
- **Review current security measures and develop a Cryptographic Inventory:** organisations should assess where, why, and how they are using cryptography. This

should include a risk register, assessing the potential impacts of failure on key parts of the business in the event of a breach.

- **Create a roadmap towards adoption of quantum safe technologies:** once the Cryptographic Inventory is complete, businesses should develop a plan for upgrading cryptography in the most appropriate and timely way, following guidance from government institutions and the cyber security community
- **Engage with the quantum and cyber security communities:** as part of a quantum resiliency roadmap, any business should engage early with the quantum and cyber security communities to develop knowledge, understanding, and the partnerships needed to address cryptographic threats from quantum computing.

Laura Foster, Associate Director for Tech and Innovation at techUK, said:
"Quantum technologies will unlock many benefits across financial services, life sciences, transportation and other key industries. But we cannot shy away from the security threats they also pose.

"It is imperative for organisations to prepare for the quantum future, including preparing for quantum resiliency. Our report, written in collaboration with techUK's quantum and cyber security members, provides practical insights to help businesses navigate the complexities of quantum security."

Zygmunt Lozinski, Senior Technical Staff Member and Quantum Ambassador, IBM Research:
"IBM aims to bring useful quantum computing to the world, and to make the world quantum safe. And while quantum computing has great potential for science and innovation, it could lead to increased risk to the security of our most sensitive data and systems. The publication of NIST's post-quantum cryptography standards means that UK organisations also have the agreed standards they need to plan and build a quantum-safe future, and to implement the National Cyber Security Center guidance on PQC migration. The techUK report gives executives and leaders a good overview of how the UK is addressing quantum risk alongside the UK's National Quantum Strategy."

-ENDS-

Notes to Editors

Cryptography:
Cryptography underpins the security of our digital infrastructure. The confidentiality of communications (such as WhatsApp or other signal messages) is ensured by encryption. The confidentiality of personal data (such as used in banking or healthcare) is also ensured by encryption. Encryption provides the non-repudiation of card payments and on-line transactions. The integrity of software updates (needed in devices from Electric Vehicles to phones) is guaranteed by digital signatures to prevent malware. Authentication confirms who is using a passport, or accessing an IT system. Public Key Cryptography is the technology deployed.

Post-Quantum Cryptography (PQC):

Sometimes referred to as quantum-safe cryptography, PQC simply refers to cryptography that is resistant to attack by quantum computers.

Symmetric encryption methods:
Symmetric cryptography is already quantum resistant, meaning this is a solution that can be implemented right now and can be used for both encryption and key exchange.

Quantum Random Number Generation (QRNG):
random number generation forms the bedrock of any cryptography system.

Quantum Key Distribution (QKD):
Refers to the sharing of quantum-safe encryption keys. Rather than the mathematical approach that cryptography uses, QKD relies on quantum properties of light to generate secure random keys for encrypting and decrypting data.

The full report can be downloaded here.

Contact details: Margherita Certo, E: margherita.certo@techuk.org, M: (+44) 07462107214

techUK's Innovation Hub

About techUK

techUK is the technology trade association that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve.

With over 1000 members (the majority of which are SMEs) across the UK, techUK creates a network for innovation and collaboration across business, government and stakeholders to provide a better future for people, society, the economy and the planet.

By providing expertise and insight, we support members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.