TOSHIBA | BT

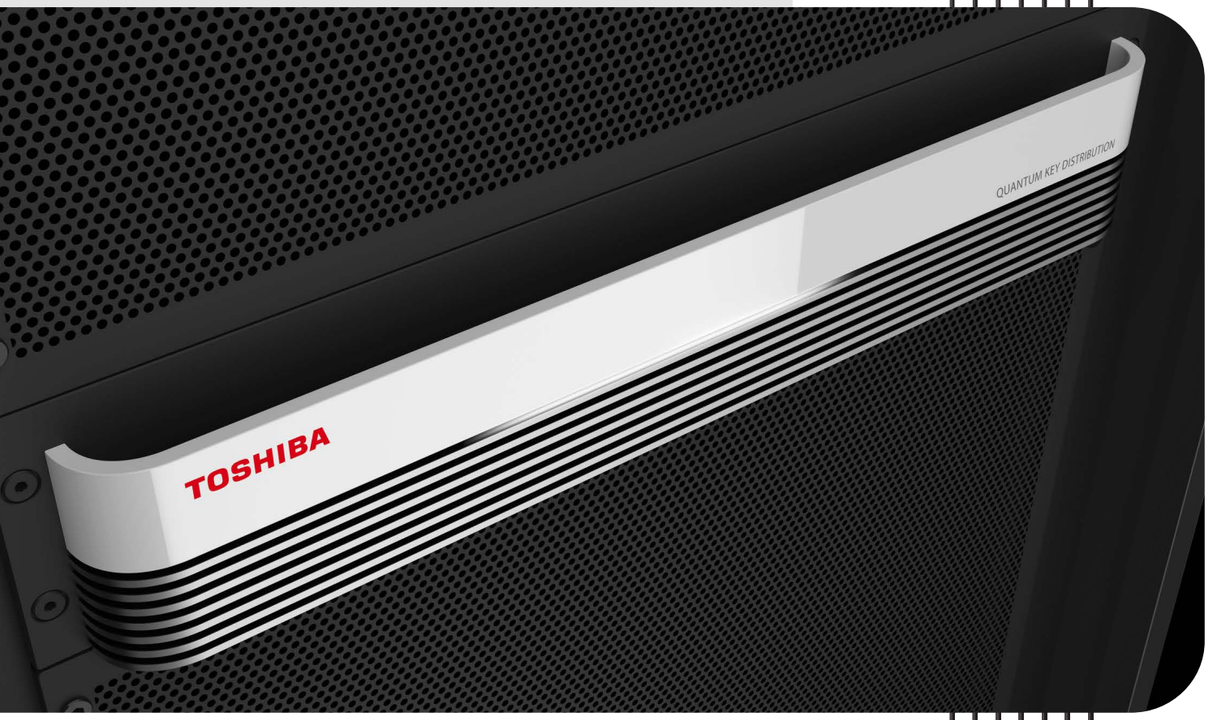
Securing the future quantum economy, today

Introduction

Building the quantum-secure economy

The arrival of powerful quantum computers at some point in the near future promises to be a milestone moment with the potential to disrupt computing as we know it.

One key effect will be the introduction of huge concern and uncertainty in the market as many fundamental principles of cybersecurity are undermined. A world in which quantum computers exist as practical devices will be one that immediately calls into question the security of standards such as **Public Key Cryptography (PKC)**, whose security underpins today's digital economy.



And yet there is a real and current danger to today's data – an attacker might collect it with the expectation of being able to decrypt the most valuable using a future quantum computer. This is called *harvest now, decrypt later*, a technique which many experts and government officials have warned is almost certainly being employed by attackers today. With large sums of money being invested in the field and development accelerating rapidly, this means that tomorrow's cyberattacks are being planned today without anyone being able to detect when this is happening. As US Secretary of Homeland Security Alejandro Mayorkas told the RSA conference in 2021:

> "We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future."

For these reasons, it is imperative that the industry develops security technologies able to resist threats today as well as in the future. Currently, the world is at the beginning of a transitional period where technologies to re-establish security in the age of quantum computing are being tested and assessed. Chief among these is **Quantum Key Distribution (QKD)**, a quantum-secure technology which is already being trialled by commercial users in the UK.

One such company is EY (Ernst & Young), which in 2022 became the launch customer for the **Quantum-Secured Metro Network (QSMN)**, the first commercial QKD network built using Toshiba QKD hardware and key management software across BT's fibre network. Connecting two of its offices at sites in London Bridge and Canary Wharf, the QSMN allows EY to fully assess QKD's ability to resist the possibility of harvest now, decrypt later eavesdropping attacks on secure keys.

The threat that quantum computing poses to traditional cybersecurity methods has such widespread economic and technological ramifications that organisations need to take action now to mitigate risks. However, building quantum-secure networks will be a complex undertaking requiring a re-examination and reconfiguration of security in ways that could take years to mature. QKD and emerging encryption standards such as Post-Quantum Cryptography (PQC) will be central to this future. The QSMN offers the perfect testbed to explore the deployment dynamics behind future security systems before the need to use them becomes critical.

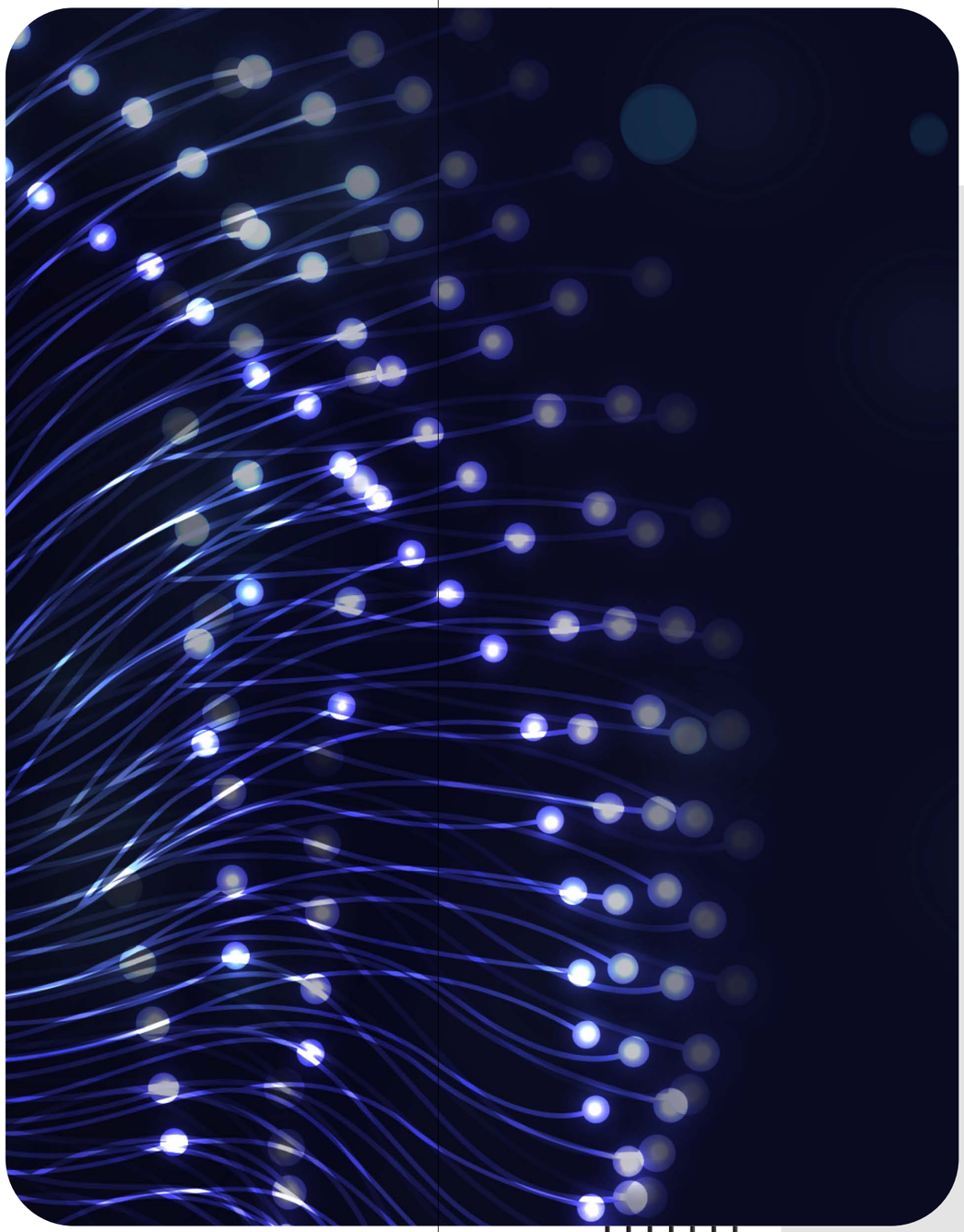
01

The quantum threat to today's world

Ever since they were first proposed, experts have worried that quantum computers have the potential to threaten today's encryption standards. The most vulnerable to this is PKC implemented using algorithms such as RSA, which forms the security bedrock of applications as diverse as email, HTTPS web communication, and cryptocurrencies.

RSA and similar algorithms have been successful so far because certain computations, such as factoring very large numbers, have proven challenging for current technology. In theory, it is possible for a classical system to crack PKC, given enough time. But even for today's most powerful supercomputers, the key lengths used in current cryptographic systems render the process wholly impractical due to how long it would actually take to break the encryption.

During the 1990s, an algorithm developed by mathematician Peter Shor was the first to demonstrate that the underlying physics of quantum computers meant they could exploit novel mathematics to perform this task many orders of magnitude faster than a classical system. At that point, the industry realised it would have to replace today's standards with a new generation of algorithms and security designs resistant to quantum computers.



Harvest now, decrypt later

Experts soon identified a second fear – the existence of future quantum computers also put at risk the security of data being stored today. It followed that an attacker could collect large amounts of encrypted data today and store it until a quantum computer became available to unlock it, an attack called *harvest now, decrypt later (or hack now, crack later)*. This exploits the fact that data such as financial information or military secrets age slowly, and could therefore remain useful to an attacker for many years.

The level of threat posed by *harvest now, decrypt later* still depends on the type of data captured. For most web traffic, the risk is low because the value of that data is time-limited or of low value. However, the same is not true for sensitive financial and personal data, which remain sensitive for years or decades.

Although it is impossible to know whether harvest now, decrypt later attacks have been carried out – such attacks can't be distinguished from any other form of data interception – its use would be entirely logical. Gathering data today that can be used as an exploitable resource in the future, such as sensitive data from the likes of financial companies or public entities, holds a benefit for malicious actors. Meanwhile, investment in quantum computing continues to rise exponentially as companies and nations race one another to develop the first device capable of performing advanced computing tasks, including the ability to undermine PKC.

The risk for organisations isn't simply that the point at which quantum computers are able to break PKC is drawing near, but that if such a breakthrough was made this might not be made public in order to achieve an invisible advantage. Even the unconfirmed possibility that this has happened could prove destabilising to the financial sector as organisations, shareholders and regulators all scramble to find out if supposedly secure sensitive data is still really safe. The key defence against this uncertainty is to invest in quantum-safe technologies well in advance of such a breakthrough being made.

02

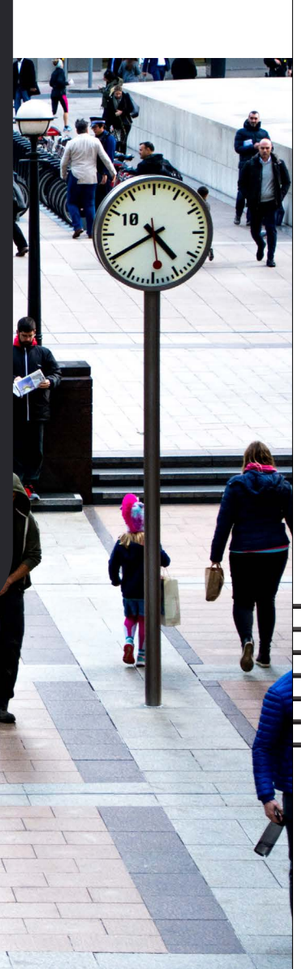
The transition to quantum safety

Addressing quantum risk requires progress on two fronts, starting with the development of new encryption algorithms able to resist quantum computers. This is already happening through the development of new Post-Quantum Cryptography (PQC) algorithms under the auspices of the National Institute of Standards and Technology (NIST).

Quantum Key Distribution (QKD)

Quantum-secure encryption security depends on two things. First, the algorithms used to generate the keys must be resistant to being cracked by a quantum computer, making the data itself hard to decrypt. Second, the keys must then be distributed in a secure manner across a network, which could include insecure public networks. QKD is an example of the latter, and can be used today to distribute ultra-secure encryption keys. Organisations should note:

- QKD security is underpinned by fundamental physical laws in which each bit of key material is encoded using a sequence of photons in random states or qubits. Due to the nature of measuring quantum systems, any attempt to intercept these photons disturbs the encoding of their states. This alteration reveals the eavesdropping, discards the current key, and restricts a new key from being successfully created until the eavesdropping stops.
- Toshiba's QKD is a solution to the problem of *harvest now, decrypt later* attacks. Because it is based on physical laws rather than mathematics, it is proven to be immune to future eavesdropping attacks on a communication channel by quantum computers.



The Quantum-Secure Metro Network (QSMN)

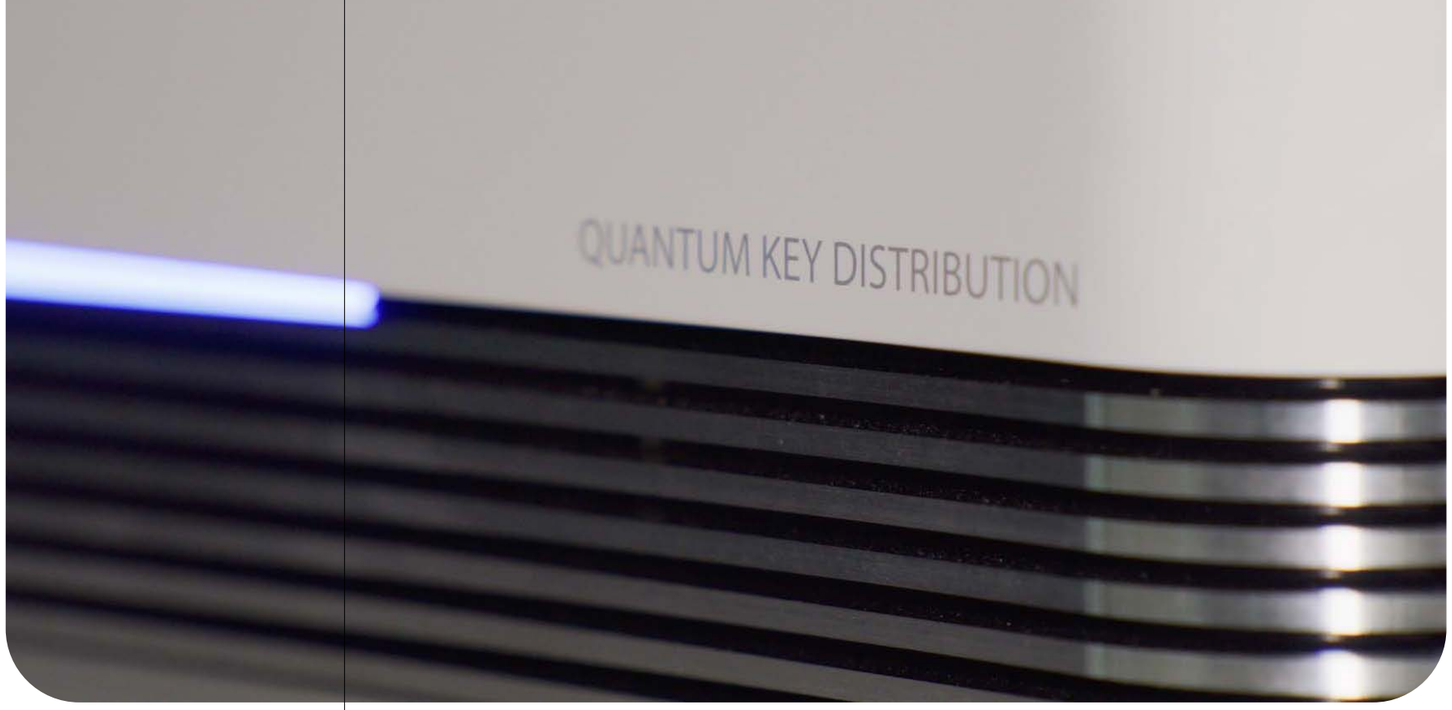
Based on technology developed by Toshiba and BT's fibre infrastructure, QKD is accessible today through the QSMN, the world's first metro scale network designed to trial quantum-secure services. Deployed across the City and West of London, the QSMN covers a large metropolitan area of potential BT customers in sectors such as financial services.

The QSMN in short:

- The BT and Toshiba Quantum-Secure Metro Network offers sectors a way to test their use of the technology and start assessing how to implement it as part of their security strategy.
- The technology can be deployed over existing fibre networks. It will also work with future encryption algorithms such as PQC and provides a mechanism to evaluate in parallel.
- Toshiba's QKD is a mature technology that is the result of two decades of research and development, including testing the technology in conjunction with BT since 2014.
- The QSMN offers a range of quantum-secured services including dedicated high bandwidth end-to-end encrypted links over a large metropolitan area of potential customers.
- QKD is a specialised, high-end technology designed to provide a future-proof solution in sectors that depend on being able to guarantee security (while not, of course, mitigating separate cybersecurity problems such as malware, software vulnerabilities, or insider threats).

03

The Quantum Secure Metro Network in action: EY



"The future is already here, it's just not evenly distributed," says EY's technology risk partner, Piers Clinton-Tarestad, discussing what quantum technologies exist today in the real world by way of quoting science fiction writer William Gibson.

It's a provocative way to introduce QKD, but also the possibility that attackers might be harvesting encrypted data today with the expectation they will soon be able to decrypt it on the quiet. It's a concerning prognosis that tomorrow's data breaches are being set up in today's world, right now.

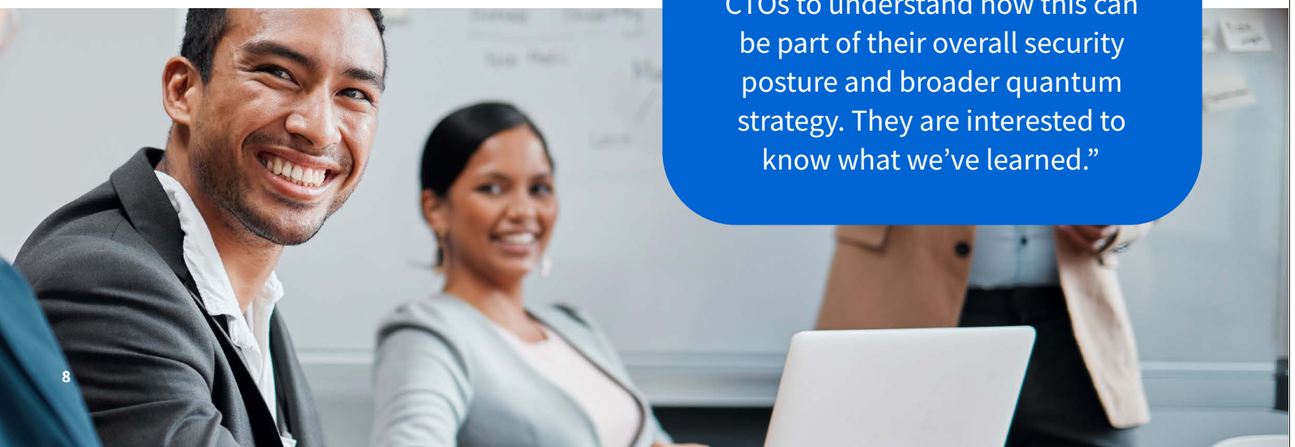
For customers, this can be a lot to take in, which is why one of the biggest challenges is simply knowing where to start. Expertise is difficult to acquire and the learning that exists is often based on lab results or early trials. What is becoming invaluable is feedback from a customer such as EY that's actually experienced the system in practice.

The motivation for EY to install QKD was twofold. First, the company wanted to test the viability of securing sensitive phone and video traffic such as that connected to its M&A business communications. Second, with interest among financial sector companies in QKD security growing, EY decided it had to learn more about the technology in order to consider it as part of wider consultancy it offers in quantum technologies and business transformation.

"We wanted to learn how we could use it but also how QKD could be integrated into our future products and services and used by our clients," confirms Clinton-Tarestad.

Although QKD and the QSMN are still emerging in the security space, he believes that UK organisations have entered the learning phase with a number within financial services reaching out to EY for advice.

> "Our clients also need to understand the use cases. We are already helping multiple CIOs and CTOs to understand how this can be part of their overall security posture and broader quantum strategy. They are interested to know what we've learned."



Currently, the network testbed is a point-to-point fibre connection linking to EY's internal Ethernet network, and as well as QKD, it utilises a classical encryptor based on AES 256 symmetric keys (replaced every minute). EY is sending test data over the network to gain insight into its real-world throughput and latency.

According to Clinton-Tarestad, the biggest issue EY's consultancy customers face is less the technology itself than understanding the QKD business case in terms of risk management. This requires that organisations first identify the most sensitive data they might want to secure, a daunting undertaking if you've never done it before, but a fundamental part of many security approaches.

"You need to understand your data and its risk and lifetime. With that completed, it's possible to work out where the business case makes sense," he says. Because few organisations have carried out such an exercise, this will take time. Having advisers to give guidance on this process is essential.

The risks QKD addresses might seem a way off, but the possibility of harvesting attacks makes it important that organisations start planning now for the impact advancements in quantum technology will have.

> "EY helps clients build this into their broader quantum strategy, including what they should be considering in the coming years."

04

How should organisations respond?

At the current rate of development, the point where quantum computers undermine data security is probably 5-10 years in the future. While it might sound like the risk is still some way away, it's one that requires action now.

The transition to quantum-secure technologies such as QKD and PQC will be a complex process taking years to implement. The technologies need to be tested under real-world conditions and organisations need to build teams with a new set of skills in order to deploy them effectively. For this reason, it is important that organisations in those sectors that will be most affected, such as finance and government, start addressing this transition as soon as possible even while understanding it will be a long-term challenge.

How can this be achieved in practical terms?

Identify data and encryption vulnerability

An organisation's vulnerability to harvest now, decrypt later attacks is a result of the time sensitivity of the data they store, and the strength of the cryptographic technologies used to secure them, of which there are numerous variations. Mitigating this risk requires identifying and classifying critical data with a long shelf life and protecting these accordingly, including by employing quantum-secure technologies such as QKD and PQC.

Enter the learning curve

Understandably, awareness of the quantum threat remains low. This means that financial sector companies whose data is at risk will have to build awareness throughout their technology and management teams. Similarly, the skills needed to use quantum-secure technologies are not easy to find. Networks such as the QSMN not only offer a vital platform for real-world learning, but a hub around which financial organisations can build quantum-aware teams.

Avoiding lock-in

As with any emerging technology, customers worry about being locked into designs they later have to abandon or upgrade. Among QSMN's key strengths is that it is available as a service and easy to integrate without specialist interfaces or the need for any significant changes. It runs across standard BT fibre and is installed on the customer's premises as a standard 2U rack-mounted appliance. And, because it presents as an encrypted Ethernet or IP link, though backed up by QKD, it is straightforward to implement. This allows organisations to assess its capabilities without having to alter their own networks or buy and later upgrade expensive equipment.

Conclusion

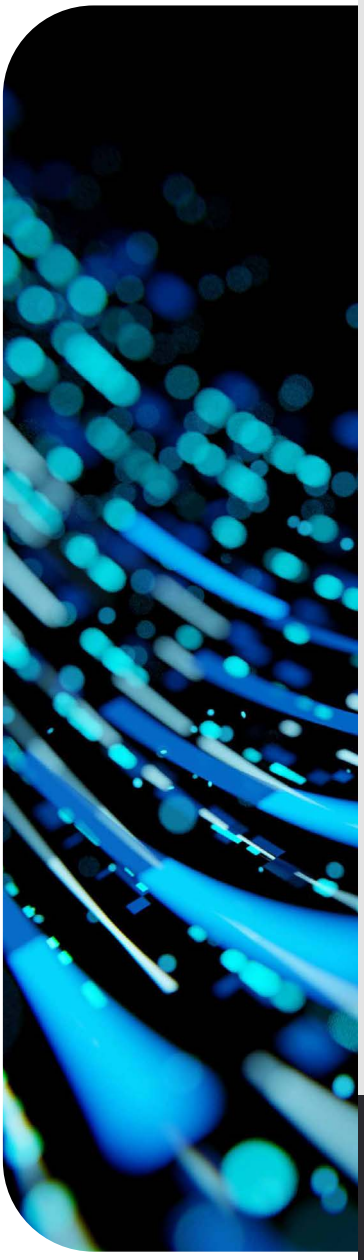
The need to act

The good news is that, unlike most big changes in computing history, the advent of quantum computing is a revolution whose benefits and risks can be assessed in advance. Historically, new opportunities in computing – the arrival of the personal computer or the Internet, say – often tend to be under-estimated initially, leading to wasted time and misdirected investment.

The era of quantum computing, by contrast, will be a revolution foretold. This gives organisations time to prepare. It follows from this that organisations in key sectors, like finance, must start to adapt to the coming quantum era as soon as possible. From a data security standpoint, the first challenge is simply to understand the risks. This is a lot of work in itself. As with any emerging technology, the skills and knowledge to understand quantum systems are not yet mainstream.

This paper has examined the certainty that the quantum era is fast approaching. It remains true that nobody knows how this new era might begin. It is often speculated that it might occur through a single breakthrough that calls into question today's encryption protocols. It's equally possible that the shift to the quantum era may come through a gradual series of discoveries and developments.

That will make it incredibly difficult for organisations to assess how and when to invest. In the early 2020s, enterprises face huge challenges from risks arising from the rise of cybercrime. Losing access to the certainty of encryption would be far worse still. While advanced technologies such as QKD are specialised today, this will not always be so. At some point, QKD, PQC, and other quantum-safe technologies will need to be integrated as a standard part of everyday security. It is imperative that organisations take the lead and engage with this post-quantum future now.



About Toshiba

Toshiba Corporation leads a global group of companies that combines knowledge and capabilities from over 145 years of experience in a wide range of businesses – from energy and social infrastructure to electronic devices – with world-class capabilities in information processing, digital and AI technologies. These distinctive strengths support Toshiba's continued evolution toward becoming an Infrastructure Services Company that promotes data utilization and digitization, and one of the world's leading cyber-physical-systems technology companies. Guided by the Basic Commitment of the Toshiba Group, "Committed to People, Committed to the Future," Toshiba contributes to society's positive development with services and solutions that lead to a better world. The Group and its 120,000 employees worldwide secured annual sales of 3.3 trillion yen (US$27.4 billion) in fiscal year 2021.

About BT

BT Group is the UK's leading provider of fixed and mobile telecommunications and related secure digital products, solutions and services. We also provide managed telecommunications, security and network and IT infrastructure services to customers across 180 countries.

BT Group consists of three customer-facing units: Consumer serves individuals and families in the UK; BT Business* covers companies and public services in the UK and internationally; Openreach is an independently governed, wholly owned subsidiary wholesaling fixed access infrastructure services to its customers - over 650 communication providers across the UK.

British Telecommunications plc is a wholly owned subsidiary of BT Group plc and encompasses virtually all businesses and assets of the BT Group. BT Group plc is listed on the London Stock Exchange.

For more information, visit **www.bt.com/about**

To learn more about protecting your data from the risk posed by quantum computers, contact **quantum@toshiba.eu** or **www.bt.com/media-enquiries**

Find out more about Toshiba at
www.global.toshiba/ww/outline/corporate.html