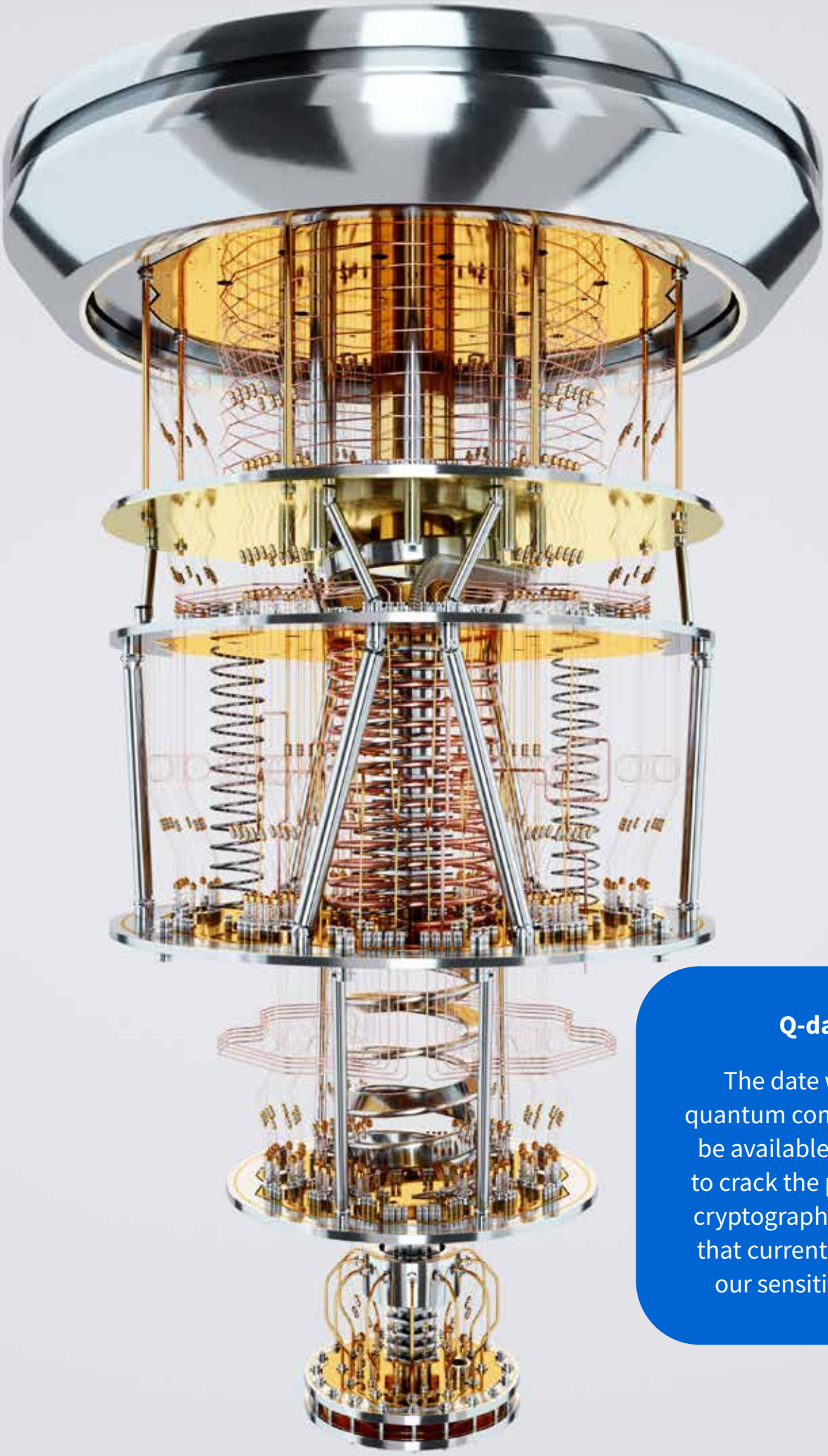
TOSHIBA

# Defence-in-Depth Solutions Today for a Quantum-Safe Tomorrow

Get ahead of the imminent quantum threat with a quantum-safe and crypto-agile hybrid QKD + PQC solution



**Q-day**

The date when a quantum computer will be available and able to crack the public key cryptography systems that currently protect our sensitive data.

01

# Introduction: The quantum threat

Whitfield Diffie and Martin Hellman published their milestone paper on Public Key Cryptography in 1976.

Since then, Diffie-Hellman-based public key cryptography has acted as a high security fence protecting the vast amounts of data that are transmitted and shared every day.

Public key cryptography's 'one-way' mathematical functions are almost impossible to break, even using the most powerful supercomputers and this has kept our sensitive information secure.

But this era of safety is about to come to an end. Thanks to heavy investment and advances in quantum computing, in a short space of time, "Q-day" has accelerated from a distant possibility to an imminent reality.

In fact, The Financial Times reported in March 2025 that the National Cyber Security Centre (a branch of GCHQ) had issued a warning that: **"the risks posed by the rapid development of quantum computers were not being taken seriously enough and called for organisations to begin preparing now."**

Current public key cryptography methods (such as RSA and Elliptic Curve Cryptography) which were previously difficult to break even by the most powerful supercomputers, could theoretically be rendered insecure by quantum computers.

As such, if bad actors are able to access the power of quantum computers, they will quickly compromise the encryption techniques which protect much of our internet traffic today and our sensitive data will be exposed.

## Building a quantum-safe plan

Telecommunications providers, governments and enterprises are well aware of the threat of quantum computers, but many still don't have a practical plan in place for creating their quantum-safe infrastructure.

How should telecom operators – and other organisations in high-risk industries – start this process? Crucially, where should they invest to future-proof their networks against the quantum threat?

According to the European Quantum Industry Consortium, which advises the EU on quantum strategy, two technology areas offer the most promising solution: **"PQC and QKD are the two main approaches to quantum-secure cryptography, providing cryptographic solutions that resist attacks from large-scale quantum computers."**

Quantum Key Distribution (QKD), which uses quantum hardware integrated into existing telecommunication networks, is 'information theoretically secure' (ITS). The gold-standard for security, this means that QKD-protected data is immune to attacks by a quantum computer, or indeed any other powerful computing resource, now and in the future.

Post-Quantum Cryptography (PQC) meanwhile, is a software-based technology which uses an algorithmic approach and is considered more resistant to quantum attack than traditionally employed forms of public key cryptography.

For organisations planning their next steps, it can be difficult to identify where investment is best placed. As the European Quantum Industry Consortium notes: **"The two approaches each have their own merits and can complement each other."**

In line with this, Toshiba has created a third option: a hybrid solution which combines the software-based PQC technology with QKD hardware. By integrating newly standardised PQC algorithms, Toshiba's hybrid QKD solution promises customers 'defence-in-depth' – two lines of defence against the quantum threat, combined.

02

# Planning your quantum-safe future

Forward-thinking telecoms or network operators are aware of the threat that quantum computing poses to their existing business model. As a result, many are in the process of evaluating their options for building a quantum-safe future.

However, few have translated an overarching strategy into a step-by-step implementation plan. Without going through this exercise, many organisations overlook the timescales and operational issues which may be involved in preparing for readiness. The following questions are aimed to aid the creation of a quantum-safe network strategy.

Today we are at an essential inflection point. Until recently, telecoms operators could consider quantum to be an iceberg on the horizon, but the threat has evolved faster than previously anticipated.

## Prompts for building your quantum-safe strategy

1. Do you have a strategy for quantum, and has this been communicated to key stakeholders?
2. Do you have an overall time-scale you're working towards to become quantum-safe?
3. Do you have a network wide cryptographic assessment? (A list of all systems and applications that use cryptography, and which ones may be vulnerable to attack by quantum computers.)
4. Have you prioritised key data, systems and network segments? (Focusing first on which data systems will be most affected by harvest now decrypt later attacks.)
5. Have you considered adopting a hybrid solution for flexibility and defence in depth?
6. Do you understand the technical, operational and timescale requirements to implement quantum-safe networking through your entire estate?
7. Do you have a phased implementation plan? To protect your most sensitive areas first or to begin earlier on areas which may take longer.
8. Which individuals and teams will be involved in executing your plan and deploying new technology? Do you have the right team on board to manage this?
9. What compliance issues or internal complexities do you envision having to overcome and how long would this take?

## Quantum Key Distribution: Your ‘ITS’ answer to quantum-safe

Toshiba began scientific research into quantum cryptography in 1999. Over the last 25+ years, it has demonstrated a number of notable world firsts and became a global leader in quantum-safe technology. The result of that journey enables the most secure communications known today, Quantum Key Distribution technology.

Quantum Key Distribution (QKD) takes advantage of the laws of quantum physics to protect sensitive data. It uses particles of light to distribute secure encryption keys across optical networks. Individual photons are transmitted between parties which are encoded with secret key information, enabling the parties to establish secure, ‘quantum-safe’ encryption keys which can be used to encrypt their sensitive data. The process of creating and distributing the quantum-safe encryption keys is immune to attack from today’s computing or future quantum computing.

The power of QKD in today’s landscape is that it is ITS. This guarantees protection against all current computational attack methods, and crucially provides resistance against future developments in high-performance or quantum computing.

### What is ITS

A cryptosystem is considered to have Information-Theoretical Security, if it is secure against bad actors armed with unlimited computing resources and time.

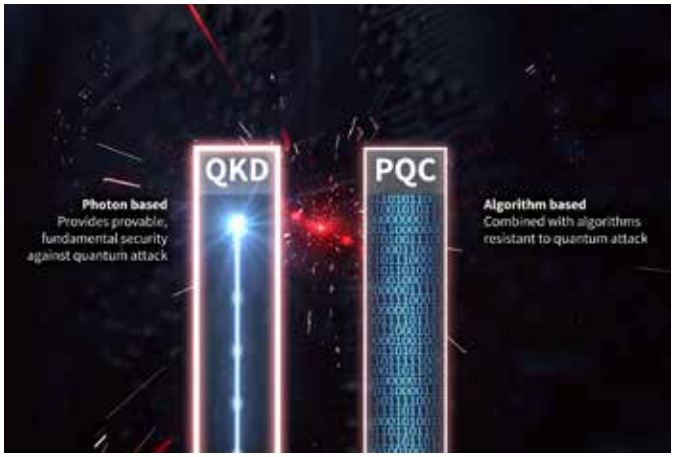
QKD is a hardware-based technology and is typically deployed over optical fibre networks, today, thanks to multiplexing technology, operators can easily and quickly overlay QKD on existing fibre networks and co-existing with their existing data services.

## PQC: Quantum-resilience

We've established that commonly used public key encryption is not safe from the impending threat of quantum computers, but that doesn't mean that all forms of public key cryptography are equally vulnerable. Post-Quantum Cryptography refers to a new category of algorithms for public key cryptography which are believed to be more resistant to quantum attack.

Several factors have made PQC a potential option for organisations which require a quantum-safe future.

- **Perceived lower barrier for implementation:** PQC can be deployed as a software solution to upgrade current public key cryptography methods e.g. RSA and ECC-based cryptography. This makes it appealing to organisations as software-based upgrades may be perceived as simpler than the physical installation of QKD technology.
- **Standardisation:** Meanwhile, following evaluation, the US-based National Institute for Standards and Technology (NIST) released standards defining the first set of PQC algorithms in 2024, bolstering the credibility of the technology.




## Limitations of PQC

While these factors make PQC an attractive proposition, there are some important limitations to consider.

- **Evolving threat landscape:** The security of PQC is still based on computational assumptions which assert that certain mathematical problems are too hard for even a quantum computer to solve. However, as quantum computers continue to advance, it's entirely possible that new methods of attack could be developed that would overcome PQC algorithms. In addition, PQC could prove vulnerable to new types of computational attack developed for use with classical computers. This means that the efficacy of PQC algorithms will need to be continually reviewed and will likely require new algorithms to be developed and deployed on an ongoing basis.
- **Implementation challenges:** While PQC's software-based nature does mean that it is easier to deploy in some ways when compared to hardware-based solutions, there are still several important considerations. For example, PQC algorithms may require more memory and processing power in order to operate efficiently. Therefore, network audits and refreshes may be required. Typically, this is not a quick process, and can take years and concerted financial investment to carry out.

  For those considering their quantum-safe business transition, PQC may seem like a quicker, cheaper and easier fix instead of using hardware-based solution like QKD. However, the continually evolving threat landscape, combined with the fact that deployment still involves notable organisational investment, does require careful evaluation of all benefits and challenges.

03

# A powerful future-proof hybrid solution

Addressing these evolutions in the market, Toshiba has implemented a hybrid QKD and PQC system that takes advantage of the benefits – and mitigates against the limitations – of QKD and PQC technology to deliver a ‘best of both’ solution.

The system now natively incorporates the latest Post-Quantum Cryptography (PQC) standard, allowing Toshiba’s QKD solution to provide and distribute both QKD and PQC keys.

04

# Benefits of Toshiba's hybrid QKD and PQC system

## Defence-in-depth

A hybrid approach offers a layered approach to security that achieves defence-in-depth. An eavesdropper would need to break both layers of security in order to obtain the secret encryption key. Therefore, even if the PQC level was compromised by a quantum computer, QKD provides an ITS fundamental line of defence that ensures the key distribution remains secure.

Creating multiple lines of defence in this way offers a 'belt and braces' approach to cryptographic security that demonstrates a compelling migration strategy to auditors, regulators and other stakeholders. But more importantly, a hybrid solution helps organisations achieve crypto-agility.

**Defence-in-depth**

The ability to efficiently layer your security according to your requirements. Defence-in-depth refers to deploying one or more different techniques of security intervention to one problem.

## Crypto-agility

Toshiba is able to quickly and easily implement new PQC algorithms as they emerge into its QKD solution. It's this 'crypto-agility' that allows telecoms operators to be flexible as and when they implement cryptographic solutions, as well as being assured that an investment made today would remain future-proof as PQC technology evolves.

## Tiered security in challenging environments

While the addition of PQC adds more flexibility, it's essential for operators to ensure that strategic parts of their networks are fundamentally secure via QKD.

With a hybrid architecture, organisations and operators can invest sparingly, deploying fibre-based QKD to their most secure locations. Meanwhile, they can still transmit a PQC key from these hubs to other sites, over the conventional network. For scenarios in which network-wide fibre access isn't possible, a tiered, hybrid solution offers the most secure second option.

## Lowering the barrier for transition

Many industry organisations are in the process of formulating their plan for a quantum-safe future. The move towards QKD can feel like a high barrier, as it requires implementation of technology on certain parts of the network.

As PQC operates using existing algorithm-based approaches, it potentially offers a way to introduce a level of quantum resistance into the network.

Meanwhile, as PQC is now a globally recognised standard recommended by NSIT, hybrid approaches that integrate PQC can lower the barrier for adoption of quantum-safe innovation by reducing the perceived risk amongst stakeholders.

## System failure mitigation

With a multi-layered solution, if an error or unexpected issue occurs on one layer of solution, a second layer of defence offers a level of system failure mitigation. This can give telecoms operators – and the organisations they serve – a greater sense of confidence.

**Crypto-agility**

The concept of designing systems with the flexibility to adapt in future without complete overhaul.

05

# How does it work?


A QKD system is comprised of two hardware appliances, a transmitter “Alice” and a receiver “Bob”, connected via fibre. QKD keys are established at Alice and Bob and these quantum-safe keys can then be used to encrypt sensitive information.

Toshiba has implemented the current PQC algorithm (called ML-KEM) within its QKD system, which gives it the ability to also establish PQC keys at Alice and Bob which can also be used to encrypt information.

With a Toshiba QKD network, any Alice can establish QKD and / or PQC keys with any Bob. Furthermore, a combination (hybrid) QKD + PQC key can be created at any Alice and any Bob enabling a defence in depth implementation.

The Toshiba QKD system can also easily implement new PQC algorithms when they are standardised.

This approach enables a crypto-agile, layered security approach which provides defence-in-depth protection.

06

# Conclusion

Quantum computing is advancing rapidly, and it may take significant time (in fact, several years) and resources to update today's networks to be quantum-safe.

To add to this, bad actors can collect and store our secret data today and decrypt it when quantum computers are available.

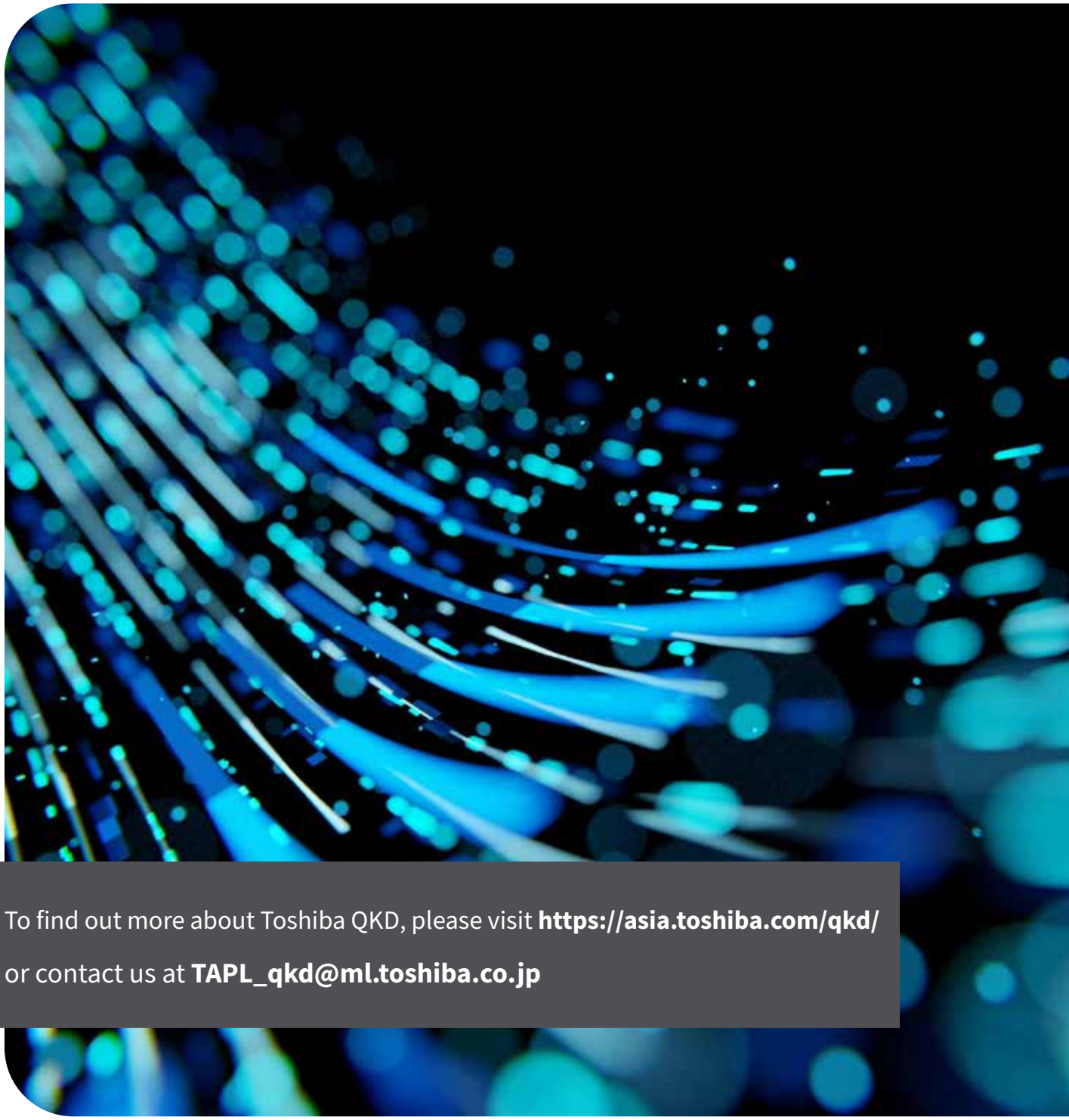
This means that organisations need to take action now to protect their communications against quantum computing-based attacks.

For telecom operators creating their quantum migration strategy, the price of true quantum-safety is the investment into QKD technology, which offers an ITS solution that promises to protect data against decryption, now and in the future. QKD provides the most secure method to put shareholders, auditors and customers' minds at rest.

Toshiba is the global leader in quantum-safe networking and has created cost effective QKD technology with market leading performance for absolute protection. Thanks to Toshiba's ongoing innovation, Toshiba now has the ability to augment its QKD solution with PQC. This hybrid solution offers additional value through defence-in-depth, and the ability to take a crypto-agile approach by implementing your quantum-safe strategy flexibly.

**Speak to Toshiba about a QKD or hybrid solution,** to plan your practical migration to a quantum-safe future.

TOSHIBA



To find out more about Toshiba QKD, please visit **https://asia.toshiba.com/qkd/**

or contact us at **TAPL_qkd@ml.toshiba.co.jp**

**Toshiba Asia Pacific Pte. Ltd.** | 20 Pasir Panjang Road, #12-25/26 Mapletree Business City, Singapore 117439