Picture credit: AdobeStock

LOOK TO THE FUTURE

Daz Preuss *highlights the importance of building resilience for a post-quantum security landscape*

While large-scale quantum computing attacks may still be years away, the conditions enabling them to exist today

Quantum computing has often been viewed as a 'future technology' with little perceived impact on day-to-day security operations. For many organisations it still feels like a distant migration challenge; something to address only once practical quantum machines arrive. However, in reality it has already created a present-day data exposure problem.

Organisations are now just two years away from the first major milestone in the National Cyber Security Centre's (NCSC) roadmap towards full migration to post-quantum cryptography (PQC) by 2035. This marks a clear shift from theory to planning. Although quantum computers capable of breaking today's encryption do not exist yet, the conditions required for future exploitation are already in place. The question is no longer whether quantum computing will create a security risk, but when it will begin to affect the confidentiality, integrity and availability of data. As quantum-safe security gains momentum, organisations need a clear understanding of the scale of the challenge and awareness of the practical steps they can take today to reduce long-term risk.

Quantum computing is not yet an operational threat, but its implications are clear. Its potential risk stems from the technology's ability to evaluate vast numbers of possible solutions within a single computational cycle. Unlike classical computers, which process information using binary states, quantum computers use qubits – units that can represent both 0 and 1 simultaneously. This property, known as superposition, allows quantum systems to explore exponential combinations of possibilities and ultimately renders many current encryption methods obsolete. This represents a fundamental shift for systems that underpin modern cryptography. Encryption schemes that currently require years of computational effort to brute-force could eventually be broken much faster.

Given that encryption protects sensitive data, secures communication channels, underpins identity verification and enables organisations to operate securely at scale, it is the backbone of modern business operations. If these mechanisms fail, the consequences extend beyond security teams to core business functions and organisational trust.

The most immediate quantum-related risk does not depend on having a quantum computer today. The 'harvest now, decrypt later' (HNDL) model allows attackers to capture encrypted data now and store it until it becomes readable. The risk is simple: data stolen today can be decrypted tomorrow. Once quantum machines reach the required threshold, this encrypted material can be decrypted retrospectively. This is especially concerning for long-lived information such as intellectual property, financial records, customer data, and strategic communications.

Because so much information is sensitive and retains value for decades, early acquisition gives quantum-capable adversaries a significant future advantage, even if they cannot use the data right away. This leads to an uncomfortable reality. Organisations may believe their environments are secure because data remains encrypted. In practice, that same data may already be sitting in an attacker's archive, waiting for quantum decryption to become viable.

The consequences will only surface when quantum computing reaches the point where today's encryption can be broken. In this sense, quantum security is not just about preparing for the future, it is about protecting the present from future exploitation.

Quantum computing is emerging at a time when security teams are already operating under immense pressure within a highly distributed, heavily integrated landscape. With increasing reliance on external services, the current ecosystem further amplifies the potential impact of quantum-enabled attacks.

Few organisations today operate within a single, well-defined perimeter. Most rely on cloud platforms, SaaS providers, remote workforces, partner ecosystems and global supply chains. Sensitive data moves across multiple environments where control is shared and accountability is often unclear. A single weakness anywhere in this ecosystem can expose data across the entire chain.

APIs sit at the centre of this model. They enable system integration and data exchange, but they also rely heavily on cryptographic trust. If that trust weakens, the integrity of these connections is compromised.

This interconnectedness is also why cloud environments are a major focus of quantum-related concern. While often assumed to provide stronger security by default, cloud platforms are equally vulnerable to quantum risk, especially if attackers can compromise authentication layers or intercept encrypted traffic. At the same time, identity systems are becoming more complex and more exposed. Techniques such as synthetic identity creation and deepfakes are already emerging. Increased computational capability will only accelerate the scale and speed of these threats.

The combination of a growing attack surface and the challenges introduced by quantum computing means that data, one of the most valuable assets organisations hold, is becoming harder to protect across its lifecycle. From creation to storage, transfer and use, it encounters different risks at each stage. Traditional models address these risks by protecting data at rest, in transit and at runtime. These approaches remain useful, but all rely on cryptographic strength holding over long periods. An assumption that quantum computing directly threatens. However, it is important to note that quantum risk does not affect all data in the same way. It especially exposes two areas of vulnerability: data at rest and data in transit.

ORGANISATIONS SHOULD IDENTIFY DATA THAT WILL REMAIN SENSITIVE FOR A DECADE OR MORE

Data at rest includes information stored in databases, file systems and backups. It carries the risk of the most significant long-term exposure. Aligned with the HNDL model, it targets large volumes of long-lived data, which organisations retain and cannot easily be re-encrypted due to scale, fragmentation or legacy constraints.

As with the nature of the model, if this data has already been copied by an attacker, future quantum capability could make it readable regardless of stronger protections applied later. Once stolen, long-lived data cannot be secured again.

Data in transit faces a different risk. Transactions, API calls and authentication flows depend on cryptographic mechanisms such as key establishment and digital signatures. These are expected to be among the first elements to weaken as quantum capability matures.

Attackers could compromise key exchanges, forge identities or intercept communications at speed. While temporary measures may offer short-term resilience, they do not remove the reliance on algorithms that are likely to become vulnerable.

A common strategic mistake is treating quantum security as a single challenge – it is important to understand that these risks demand different responses. Treating these issues as a single problem leads to poor prioritisation. Data at rest and data in transit require tailored strategies and timelines. Both depend on encryption remaining secure over time and quantum computing places increasing pressure on that assumption.

Awareness of quantum-safe security is increasing and Google's recent acceleration in PQC development appears likely to play an important role in that momentum. However, most organisations remain in the early stages of readiness.

One of the biggest barriers is that quantum technology does not follow a single, predictable trajectory. This makes it difficult for businesses to plan effectively for a threat that's shape, timing and operational impact remain uncertain. Although quantum-resistant cryptographic proposals are emerging, none have yet been fully validated across real-world business environments.

On the other hand, security teams are already under pressure from ransomware, supply chain vulnerabilities, insider threats, regulatory change and rapid technology adoption. This often means that quantum risk becomes 'important, but not urgent'.

Many organisations still operate complex landscapes of legacy systems, undocumented dependencies and inconsistent cryptographic practices. As a result, simply understanding where and how encryption is used is often more challenging than expected. Another common assumption is that cloud providers will 'handle the quantum problem'. While platforms will update their own cryptographic standards, this alone does not protect the full lifecycle of a customer's data.

DATA AT REST AND DATA IN TRANSIT REQUIRE TAILORED STRATEGIES AND TIMELINES

Quantum-safe readiness is not just a technical challenge. It requires broader organisational awareness and alignment. At an executive level, quantum computing must be understood as a strategic risk affecting resilience and trust. At the same time, technical teams need to understand how quantum developments intersect with encryption, identity, authentication and system design.

More broadly, organisations must shift how they think about risk. Quantum introduces threats that develop gradually and only become apparent later. Building awareness now makes future transitions more manageable.

That said, organisations do not need to implement full quantum-safe cryptography immediately. But there are meaningful steps they can take now to reduce future exposure. The first is gaining a clear understanding of where encryption is used across applications, devices, databases and integrations. Without this visibility, planning any future migration becomes difficult.

Organisations should also identify data that will remain sensitive for a decade or more, as these long-lived assets require early attention. Strengthening key management practices is another important foundation.

Better ownership, rotation and usage processes reduce current risk and make later transitions easier. Authentication systems should also be reviewed, particularly those relying on biometrics or static factors that may contain tolerances an advanced adversary could exploit.

It is equally important to understand how suppliers and technology partners are approaching quantum-safe security and to ensure that future procurement decisions include clear expectations around readiness. Quantum risk should also be embedded within the wider enterprise risk framework, so it is visible to compliance, governance and operational teams as well as security specialists. None of this requires waiting for new standards or fully matured technology. These actions can be taken now using existing capabilities, helping organisations move from awareness to practical preparation.

Quantum computing is advancing steadily. While large-scale attacks may still be years away, the conditions enabling them to exist today. Strategies focused only on current threats will not protect organisations from risks that evolve over long timelines. The transition to quantum-safe security requires planning and preparation well before quantum machines become powerful enough to break today's defences.

Organisations that begin this work now will be best positioned to protect their data, maintain trust and remain resilient in a post-quantum world. Those that wait may discover that the breach which undermines them happened long before the decryption ever began ●

Darren Preuss (known as 'Daz'), Chief Operating Officer, CybExer UK, brings nearly 28 years of Defence industry experience, spanning telecommunications engineering, global solutions architecture, capability development and cyber training.

While often assumed to provide stronger security by default, cloud platforms are equally vulnerable to quantum risk

Picture credit: Getty