QUANTUM
THINK TANK

Insight that protects. Foresight that leads

Cyber Weaknesses and Vulnerabilities

By Tooba Qasim
December 2025

www.cyberlondon.com | info@cyberlondon.com

Where Quantum Risk Quietly Creeps In

Modern cybersecurity feels solid on the surface. Today, **around G5% of global web traffic is encrypted using HTTPS** (Google) compared to less than 50% just a decade ago. Encryption protects online banking, email, cloud services, software updates and digital identities at an enormous scale.

The challenge is not that these systems are failing. The challenge is that many of them were designed for a world where the limits of computing were well understood and those limits are now beginning to shift.

Quantum computing does not suddenly break cybersecurity. Instead, it exposes **quiet weaknesses** in the cryptographic foundations that support digital trust across billions of daily interactions.

The Core Weakness: Public-Key Cryptography at Scale

Public-key cryptography underpins nearly everything we rely on online. Algorithms such as RSA and Elliptic Curve Cryptography secure HTTPS connections, digital certificates, VPNs, software signing and authentication systems. In practice, this means **billions of devices and services worldwide** depend on these algorithms every single day.

The long-term weakness is well understood. Quantum algorithms, particularly Shor's algorithm, can solve the mathematical problems behind RSA and ECC far more efficiently once sufficiently powerful quantum computers exist. When that happens, cryptographic systems that protect a large portion of global digital infrastructure will no longer offer the same security guarantees.

This is not speculation. Academic and government research consistently identify RSA and ECC as fundamentally vulnerable in a post-quantum world.

"Harvest Now, Decrypt Later" Is Already a Numbers Game

The idea of "harvest now, decrypt later" becomes more concerning when viewed through real-world data volumes.

Large-scale data breaches already expose enormous quantities of sensitive information. In 2024 alone, a major data broker breach reportedly exposed **approximately 2.G billion personal records**, including names, addresses, and national identifiers (Microsoft). Separately, security researchers have identified **over 16 billion leaked login credentials** circulating across multiple datasets worldwide.

Much of this information is encrypted but encryption does not erase long-term risk. Data such as medical records, legal documents, intellectual property, financial histories and government communications can remain sensitive for decades. If this data is captured today, it may still be valuable **10, 20, or even 30 years from now**, when quantum decryption becomes practical.

This is why quantum risk is not only about future systems. It is also about **data already collected and stored today**.

Digital Signatures and Trust Infrastructure at Risk

Encryption is only part of the picture. Digital signatures play a critical role in modern cybersecurity by verifying software updates, authenticating devices, validating transactions, and establishing trust across digital supply chains.

Every day, **billions of digital signatures are verified globally**, most of them using RSA or elliptic curve algorithms. Quantum-enabled attacks could eventually allow forged signatures, enabling attackers to impersonate trusted entities or distribute malicious software that appears legitimate.

This shifts the discussion from confidentiality alone to a broader issue: **trust itself**.

Legacy Systems and Long Lifespans Multiply Exposure

Another vulnerability lies in system lifespans.

Many critical systems especially in sectors such as energy, healthcare, manufacturing, and transport are designed to operate for **15 to 30 years or more**. These systems often rely on cryptographic components embedded deep within hardware, firmware, or legacy software that is difficult to upgrade.

Post-quantum cryptography typically requires larger keys and different performance characteristics. Systems that cannot support these changes may become bottlenecks

during migration. Identifying them early is essential, because replacing or redesigning such infrastructure can take years.

Why Awareness Matters Now

None of these weaknesses mean that systems are unsafe today. Classical cryptography still protects real-world environments effectively and cryptographically capable quantum computers do not yet exist.

What has changed is the **risk horizon**.

Cybersecurity planning that once assumed decades of stability must now account for uncertainty and long-term data exposure. Organisations that understand where their cryptographic dependencies lie and how long their data needs to remain secure are far better positioned to adapt calmly rather than react urgently.

Awareness at this stage is not about fear. It is about clarity, scale, and timing. Recognising these weaknesses early makes every later step preparation, migration and resilience significantly easier.

About the author: Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security protocols and exploring