FORGING BUSINESS RESILIENCE IN A POST-QUANTUM WORLD

By Christophe Barel

In a not-too-distant future, the maturing of quantum computing technology could prove devastating to institutions unprepared for its impact on cybersecurity and business risk.

For many business leaders, quantum computing is a far-in-the-future consideration, as the technology is still in its early development stages. Significantly more powerful than classical computers, quantum computers use qubits instead of bits, which makes them capable of performing difficult calculations, navigating complex algorithms, and breaking current encryption methods.

With such capabilities, quantum computing presents many opportunities for optimising operations, performing complex risk analysis, and other boons to business. However, the same technology could arm cybercriminals with the most potent tool yet in their ever-evolving arsenal. Financial institutions must prepare their information security systems to move to post-quantum cryptography (PQC) today to be resilient in the face of tomorrow's threats.

WHY NOW?

When quantum computing will actually be a reality is a matter of great debate, with estimates ranging from five to 30 years to break current encryption. Building a commercially viable quantum computer has proven challenging due to the need for extreme conditions to maintain stability; qubits need to be kept at absolute zero temperatures. Current working quantum computers are limited in the problems they can solve. However, the world's most powerful countries and tech companies are pouring investments into quantum technologies and small breakthroughs could significantly speed up the timeline, especially for systems that could render today's encryption methods obsolete.

Current cryptographic algorithms used to protect financial transactions, such as public key encryption and digital signatures, rely on the difficulty of specific mathematical problems. The problem is that quantum computers can solve these problems exponentially faster than classical computers. In 2019, Google claimed "quantum supremacy" – a milestone marking a quantum computer's superiority over classical computers by performing calculations previously deemed impossible – by demonstrating that its quantum computer could solve a problem that would take a classical computer 10,000 years in just 200 seconds. Four years on, these capabilities have advanced substantially. Just as we are currently seeing artificial intelligence breakthroughs compounding extremely quickly, with new developments occurring almost daily, we should anticipate the same with quantum technologies once a certain tipping point is reached.

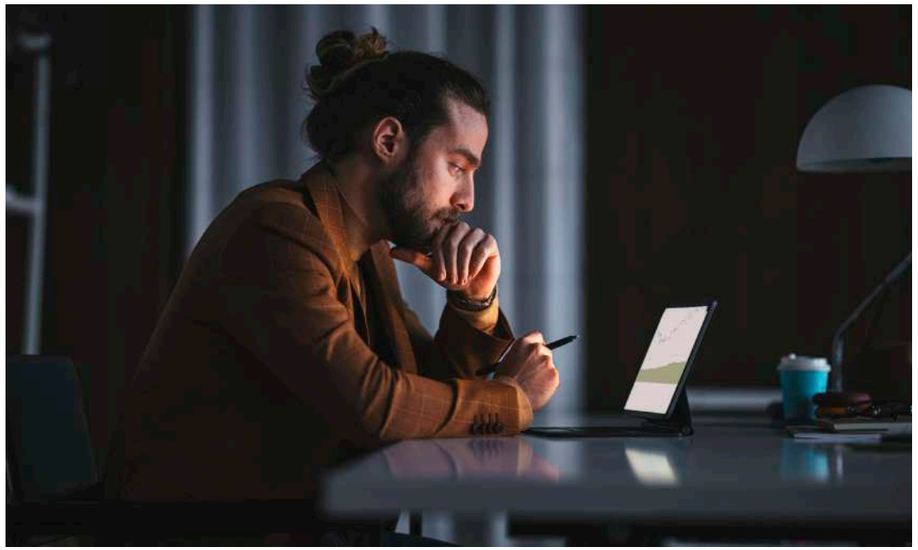
Threat actors are certainly acting as if this is the case, already stockpiling encrypted data for 'harvest now, decrypt later' attacks. Using this attack strategy, threat actors exfiltrate large quantities of encrypted data and store it until they can break the cryptography using quantum computers. Such quantum-powered attacks could significantly compromise the privacy and security of the global financial system and that of its customers.

COUNTERING THE THREAT – WHERE DO WE STAND?

In anticipation of a post-quantum world, significant efforts are underway to develop more resilient tools, technologies, and algorithms to protect the data and consumers

of financial institutions. These include post-quantum encryption algorithms, which use advanced mathematical problems that are considered difficult for quantum computers to solve; quantum-safe blockchain technology, which is more resistant to cyberattacks than centralised systems; and quantum key distribution, a method of communication using quantum mechanics principles to ensure immunity from tampering. Many financial institutions are investing in hiring or developing quantum experts and collaborating with quantum computing startups on pilot projects.

In the US, the National Institute of Standards and Technology has been leading an effort to identify and standardise post-quantum cryptographic algorithms. We expect that this standardisation will help the adoption of PQC across the industry.



A ROADMAP FOR POST-QUANTUM PREPARATION

The full impact of quantum computing on cyber and business risk in the financial services sector is currently unknown, but organisations must prioritise preparations today as the drivers to advance quantum technologies accelerate. According to McKinsey, global funding for quantum computing startups increased by 13.5% last year to USD1.1 billion, with China planning to invest USD15.3 billion and the European Union USD7.2 billion in the industry.

It is important for organisations to understand their ability to react to changes in the PQC landscape and be ready for them. This entails developing security protocols that secure data against both quantum and classical computers and can interoperate with existing practices. To this end, the Financial Services Information Sharing and Analysis Center's (FS-ISAC) Post-Quantum Cryptography Working Group has developed a road map for post-quantum preparation.

+ Inventory existing encryption assets: Building a clear inventory of cryptographic assets and their uses helps an organisation proactively identify risks and challenges brought by advances in PQC, enabling the company to be crypto-agile.

According to McKinsey, **GLOBAL FUNDING FOR QUANTUM COMPUTING STARTUPS INCREASED BY 13.5% LAST YEAR TO USD1.1 BILLION,** with China planning to invest USD15.3 billion and the European Union USD7.2 billion in the industry.

+ Assess risk: Identify the assets, threats, vulnerabilities, and potential impacts of a security incident or data breach. The risk assessment outcome should include a comprehensive list of all the risks, controls implemented to mitigate identified risks, and mitigation action plans.

+ Create a risk assessment framework: A starting point for organisations to understand and assess the threats that quantum computing may pose to its information security and a tool to help key stakeholders communicate risks effectively and aid in aligning security goals with operational goals and objectives.

+ Apply a risk model: In the absence of absolute insight on risks posed by cryptographically relevant quantum computers (CRQC), the recommended immediate best practice is to create several risk scenarios for specific assets, with some of these scenarios being "more likely" than others. Once all likely risk scenarios are identified and prioritised, take proactive measures to protect against those risks with the most impact first.

+ Assess vendors: Plan for vendor PQC requirements and update current risk assessment procedures and legal/contract requirements to include PQC provisions. Furthermore, organisations should work to raise vendor knowledge of PQC.

FINANCIAL INSTITUTIONS CANNOT AFFORD TO WAIT

While there is no immediate call for alarm, the accelerating pace of quantum research and development means that it would be prudent to begin enacting quantum-resistant measures as soon as possible. Currently, quantum development is being driven by governments, academic institutions, and Big Tech, but, like with many major technological waves, it will not remain in their hands for long. As such, FS-ISAC's Post-Quantum Cryptography Working Group has developed a set of publicly available white papers for financial institutions to begin their post-quantum journey.

Organisations must prepare now — particularly in the financial services industry, where the stakes are so high. Financial institutions must keep pace with advancing technologies and strengthen their quantum resilience posture accordingly. A comprehensive approach incorporating intelligence and knowledge sharing, incident response exercises, and a mindset shift in prioritising quantum risk, among others, is needed to achieve resilience in anticipation of such emerging threats. Financial institutions must begin building quantum resilience today, in order to safely navigate the post-quantum threat landscape of tomorrow. ✱

A comprehensive approach incorporating intelligence and knowledge sharing, incident response exercises, and a **MINDSET SHIFT IN PRIORITISING QUANTUM RISK,** among others, is needed to achieve resilience in anticipation of such emerging threats.

■ *Christophe Barel is the Managing Director for Asia Pacific at FS-ISAC, the member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve. Founded in 1999, the organisation's real-time information sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defence. Member financial firms represent more than USD100 trillion in assets in more than 70 countries.*

Prior to joining FS-ISAC, Christophe was Managing Director at data and intelligence provider Acuris Group where he has set up their Risk & Compliance business for Asia Pacific, focusing on areas such as AML/KYC screening, cybersecurity and enhanced due diligence. Christophe has been based in Asia for about a decade, starting off in Hong Kong before moving to Singapore in 2015. Previously, he worked for a variety of consulting and tech companies.