Press contact:
Florence Lievre
Tel.: +33 1 47 54 50 71
Email: florence.lievre@capgemini.com

Nearly two-thirds of organizations consider quantum computing as the most critical cybersecurity threat in 3–5 years

Six in ten 'early adopters[1]' of quantum-safe technologies predict that 'Q-day[2]', the point at which quantum computers can break current cryptographic algorithms, will arrive within 5-10 years

Paris, July 10, 2025 – A Capgemini Research Institute report published today, *'Future encrypted: Why post-quantum cryptography tops the new cybersecurity agenda,'* highlights that rapid progress of quantum computing threatens to render current encryption algorithms obsolete. 'Harvest-now, decrypt-later[3]' attacks, together with tightening regulations and the evolving technology landscape, have elevated the importance of quantum safety. However, despite increasing awareness within the industry, many organizations still underestimate the risks surrounding quantum computing, which could lead to future data breaches and regulatory penalties.

According to the report, around two-thirds (65%) of organizations are concerned about the rise of 'harvest-now, decrypt-later' attacks. One in six early adopters believe that 'Q-day' will be within five years, while around six in ten believe it will arrive within a decade.

"Quantum readiness isn't about predicting a date–it's about managing irreversible risk. Every encrypted asset today could become tomorrow's breach if organizations delay adopting post-quantum protections. Transitioning early ensures business continuity, regulatory alignment, and long-term trust," said Marco Pereira, Global Head of Cybersecurity, Cloud Infrastructure Services at Capgemini. *"Quantum safety is not a discretionary spend but a strategic investment, which can turn a looming risk into a competitive advantage. The organizations that recognize this fact early will best insulate themselves against future cyber-attacks."*

While current quantum computers cannot break widely used encryption yet, high-risk industries such as defense and banking are leading the adoption of quantum-safe solutions. In contrast, consumer-focused sectors like consumer products and retail sectors are showing less urgency.

Post-quantum cryptography migration preferred over other quantum-security solutions

Most organizations surveyed (70%) are protecting their systems against emerging quantum threats by adopting the appropriate mix of post-quantum cryptographic (PQC) algorithms.

They view PQC as the best option to address near-term quantum security risks because it provides a comprehensive approach to securing data. Nearly half of early adopters are already exploring, assessing

[1] "Early adopters," who make up 70% of our survey respondents, are organizations that are either currently working on or planning to implement quantum-safe solutions within the next five years.

[2] 'Q-Day' is the hypothetical future date when quantum computers will become powerful enough to break the crypto-graphic algorithms that currently secure most of the world's digital data and communications.

[3] 'Harvest-now, decrypt-later' attacks rely on the acquisition of currently unreadable data with the possibility of decrypting it after 'Q-Day'.

feasibility, or piloting PQC solutions. For 70% of organizations, regulatory mandates are a key driver behind the shift to PQC.

While the early adopters are working towards quantum safety, a few organizations (30%) are still ignoring the quantum threat. They are struggling to allocate sufficient budget and personnel to cryptographic transition.

Report Methodology

The Capgemini Research Institute conducted a survey of 1,000 organizations with annual revenue of at least $1 billion across 13 sectors and 13 countries in Asia–Pacific, Europe, and North America. The global survey was carried out in April–May 2025. Around 70% of the sample in this report are referred to as 'early adopters'. This segment is either working on or planning to work on quantum-safe solutions in the next five years. The survey findings were supplemented through in-depth interviews with sixteen industry executives.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Get The Future You Want | www.capgemini.com

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think-tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the United Kingdom and the United States. It was ranked #1 in the world for the quality of its research by independent analysts for six consecutive times - an industry first.

Visit us at https://www.capgemini.com/researchinstitute/