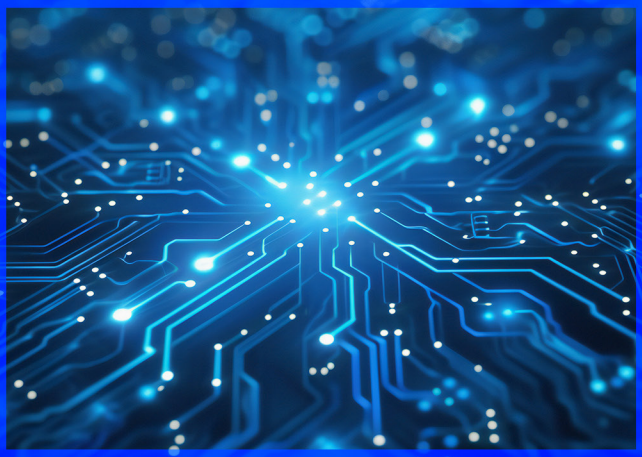
Q-Day

The quantum threat is no longer theoretical.



Quantum computing is surging forward with breakthroughs in qubit stability and error correction, paving the way for powerful, scalable systems. Paired with cutting-edge algorithmic advances, these leaps are fast-tracking us toward Q-Day, when quantum computers could shatter today's encryption standards.

> **Whether quantum tech disrupts everything or not, organizations need to start their postquantum cryptography migrations now. Waiting could cost you significantly more than acting.**
>
> — Dr. Aaron Kemp
> US Quantum Lead, KPMG LLP

For real this time?

For decades, quantum computing has been the tantalizing "five years away" dream—a disruptive technology brimming with potential yet always just out of reach. But recent breakthroughs in qubit stability, error correction, and algorithmic efficiency are changing the game, rapidly accelerating the path to Q-Day, when quantum computers could upend current encryption standards. As these advancements reshape the technological landscape, the urgency for postquantum cryptography (PQC) has never been greater, demanding robust solutions to secure our digital future against this looming quantum revolution.

Big players...major breakthroughs

The race for quantum supremacy is heating up, with major breakthroughs from leading tech giants driving unprecedented progress in quantum computing innovation.

Google

In December 2024, Google introduced the Willow chip, a quantum computing breakthrough that achieved exponential error suppression, enabling computations beyond the capabilities of classical supercomputers. Google executives project that this advancement will bring practical quantum applications, such as drug discovery and optimization, within reach in the next five years.

1,000x fewer qubits

Advancements in quantum computing have slashed the number of physical qubits needed to crack a 2,048-bit Rivest-Shamir-Adleman (RSA) key by 1,000-fold, from roughly 1 billion in 2012 to just 1 million by 2025. Breakthroughs in error correction, circuit optimization, and algorithms like Shor's have lowered quantum hardware demands, making the threat to current encryption more imminent. This rapid progress underscores the urgent need for PQC to safeguard sensitive data.

2012

1,000,000,000 qubits needed to crack **RSA 2,048**

2019

20,000,000 qubits needed to crack **RSA 2,048**

2025

Less than **1,000,000** qubits needed to crack **RSA 2,048**

Quantum leaps

Microsoft

In February 2025, Microsoft unveiled the Majorana 1 chip, marking a significant milestone as the world's first quantum chip powered by topological qubits and a novel state of matter. This breakthrough promises enhanced qubit stability, potentially revolutionizing applications in fields like medicine, cryptography, and materials science. Although some experts have expressed skepticism about the claims' full validity, the implications would be significant if Microsoft has indeed realized a new state of matter.

IBM

IBM made significant strides towards commercially viable quantum computing with its June 2025 roadmap outlining plans for a large-scale, fault-tolerant quantum computer by 2029, leveraging a new error-correcting code. Additionally, in October 2024, IBM opened its first European quantum data center, expanding global access to quantum resources and advancing its mission to integrate quantum and classical computing for practical applications.

The next 10 years

The next decade will transform quantum computing from a distant dream into a game-changing reality. By 2028–2033, fault-tolerant quantum systems will emerge, driven by breakthroughs in logical qubit stability and error correction, enabling reliable, large-scale computations.[1] [2] Industry revenues are projected to soar from over $1 billion in 2025 to beyond $622 billion by 2040, propelled by a 30 percent annual growth rate as sectors like finance and pharmaceuticals adopt quantum solutions.[2] [3] [4] Innovations in quantum chips will unlock unprecedented computational power, revolutionizing drug discovery and materials science with faster simulations and advanced designs. Major tech players are accelerating this progress with cutting-edge quantum processors, pushing algorithms for optimization and cryptography.[1] [5] The urgency for PQC is critical, as quantum computers could crack RSA by the early 2030s, demanding action to secure data now.[6] [7] [8]

Why is PQC preparation important?

Migrating to PQC is crucial for organizations to protect their sensitive data from future quantum computer threats, ensuring long-term security in an evolving technological landscape. Additionally, adopting PQC early can help organizations maintain compliance with emerging regulations and establish themselves as leaders in cybersecurity, safeguarding trust with clients and stakeholders.

How can KPMG help?

KPMG LLP can provide thorough support for your PQC migration by offering specialized guidance on implementing PQC solutions, working to keep your systems secure against emerging quantum threats. Additionally, our team can assist in creating a strategic roadmap tailored to your organization's specific needs, facilitating a smooth transition to quantum-resistant technologies.

Brace for the quantum leap with knowledgeable guidance from KPMG on PQC migration. Our leading approach and deep industry experience empower your organization to smoothly transition to quantum-resistant encryption, safeguarding your data against tomorrow's threats today.

Sources

[1] BCG (July 2024)—The Long-Term Forecast for Quantum Computing Still Looks Bright

[2] McKinsey & Company (2023)—Quantum Technology Monitor (via Statista)

[3] MarketsandMarkets—Quantum Computing Market Size, Share, Growth Report 2030

[4] Precedence Research (February 2026)—Quantum Computing Market Size to Reach USD 19.44 Billion by 2035

[5] Google Quantum AI/Craig Gidney (May 2025)—Breaking RSA Encryption Just Got 20x Easier for Quantum Computers (via CSO Online)

[6] The Quantum Insider (May 2025)—Google Researcher Lowers Quantum Bar to Crack RSA Encryption

[7] Global Risk Institute—Quantum Threat Timeline Report 2024 (referenced via Palo Alto Networks and TCG)

[8] TCG (September 2025)—Q-Day: When Will Quantum Computers Break Encryption?

Contact us

Richard Entrup
Emerging Solutions Leader, KPMG LLP
T: 201-307-7575
E: rentrup@kpmg.com

Dr. Aaron Kemp
US Quantum Lead, KPMG LLP
T: 404-358-3138
E: aaronkemp@kpmg.com

Dr. Lekshmy Sankar
US Quantum Security Lead, KPMG LLP
T: 303-296-2323
E: lekshmysankar@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**