



PRESS RELEASE

October 1, 2026

Survey on Post-Quantum Cryptography

Companies May Be Running Out of Time to Transition to Post-Quantum Cryptography

- 55.2% of U.S. companies expect Q-Day to arrive within the next five years
- More than one in five organizations estimate their full PQC migration will take five to ten years
- 44.6% of companies must protect more than half of their sensitive data for at least ten years, making them vulnerable to "store now, decrypt later" attacks today

Ludwigsburg/Atlanta – Most U.S. companies expect a quantum threat within the next decade. At the same time, many organizations may not have enough time to transition their systems to Post-Quantum Cryptography (PQC). These are among the key findings of a recent study conducted by management and IT consultancy MHP. According to the research, 87.3% of the surveyed organizations are already addressing quantum-safe cryptography. Nevertheless, many companies are at risk of losing the race against Q-Day.

More than half of U.S. companies (55.2%) believe that quantum computers will be capable of breaking today's cryptographic standards, such as RSA and ECC, within the next five years. Another 33.5% expect this capability to emerge within the following five years. As a result, an overwhelming majority expect a cryptographically relevant quantum computer to arrive by the mid-2030s at the latest.

"Quantum risk, alongside the rapid advancement of AI, is no longer just a technology issue. It is a C-suite priority. With more than half of U.S. companies expecting Q-Day within the next five years, the time to prepare is now. Leaders need to understand their cryptographic exposure, modernize legacy environments, and invest in a structured transition. Those who act early will not only protect critical data and operations, but strengthen their long-term resilience and competitiveness," says Tobias Hoffmeister, President & CEO of MHP Americas.

Migration Timelines May Exceed the Remaining Window

One of the study's most important findings is the expected length of PQC migration projects. More than half of the surveyed organizations estimate that a complete transition to Post-



A PORSCHE COMPANY

Contact

MHP Management-
und IT-Beratung GmbH

Benjamin Brodbeck

Head of Public Relations
+49 (0) 152 33 14 58 09

Benjamin.Brodbeck@mhp.com



Mirko Geyer

Spokesperson AI, Cyber Security, Aerospace, Defense
+49 152 5580 7914

Mirko.Geyer@mhp.com



MHP Media / Newsroom
www.mhp.com/newsroom

Quantum Cryptography will take between two and five years. Another 21.8% believe the process will require between five and ten years.

As a result, many companies are working with project timelines that closely mirror the timeframe in which they expect the quantum threat to materialize. Organizations that have not yet begun their migration efforts will likely struggle to secure their systems before the arrival of Q-Day.

"The challenge today is no longer recognizing the risk," says Dr Jan Wehinger, Partner at MHP. "The key question is whether organizations can complete their transformation in time. The window for action is narrowing rapidly."

Legacy Systems Are the Biggest Obstacle

Built over years or even decades, these IT landscapes often include cryptographic functions across hundreds or thousands of systems, applications, and processes. Before migration can begin, these dependencies must be identified, assessed, and modernized.

The transition is further complicated by talent shortages, budget constraints, and the technical complexity of the topic itself. As a result, PQC migration is evolving from a traditional cybersecurity initiative into a company-wide transformation effort.

The Threat Has Already Begun

The study also highlights that the risk begins before the arrival of Q-Day itself. In so-called "store now, decrypt later" attacks, adversaries intercept and store encrypted data today so they can decrypt it once sufficiently powerful quantum computers become available. This threat is particularly relevant for organizations that must protect sensitive information over extended periods. According to the study, 44.6% of U.S. companies need to safeguard more than half of their sensitive data for at least ten years. For these organizations, the quantum risk is already a present-day concern.

Every delay increases the risk that sensitive information could be collected today and exposed in the future. The findings reveal a striking paradox: while the United States is widely seen as one of the most advanced markets for PQC readiness, many organizations may discover that technological progress is moving faster than their own transformation efforts.

[The full survey results are available here.](#)

About the Study

The survey was conducted online between February 5 and February 16, 2026. A total of 1,060 IT professionals from companies with 500 or more employees in Germany and the United States participated. The results are representative, based on quota sampling, and reflect a statistical margin of error of ± 4.3 percentage points.

About MHP

MHP is a management and IT consultancy headquartered in Ludwigsburg, Germany. For more than 30 years, MHP has combined deep industry expertise with technological know-how, supporting leading companies in complex strategy and IT transformations across the entire value chain. Its industry focus spans automotive and manufacturing, aerospace, defense, and energy, as well as the public sector. MHP provides strategic and operational consulting in key future-focused areas such as business transformation, artificial intelligence, SAP and cloud transformation, manufacturing and supply chain digitalization, software-defined products and operations, data-driven business models, and platform & ecosystem development. At the core is the ambition to translate technological excellence into industrial-scale solutions – fast, sovereign, and resilient. In doing so, MHP strengthens the global competitiveness of its clients. Around 4,500 employees worldwide work together to deliver on this ambition. For more information, visit www.mhp.com.