MHP
A PORSCHE COMPANY

The Race Against Q-Day: Are Companies Too Late for the Quantum Era?

Status, Risks, and Implementation Challenges of Post-Quantum Cryptography in Germany and the United States

KEY FACTS

9 out of 10 companies are dealing with PQC

Post-Quantum Cryptography (PQC) is **no longer a future topic**: in Germany, around 86.6 percent of companies are addressing the issue; in the United States, the figure is 87.3 percent.

Q-Day is expected very soon

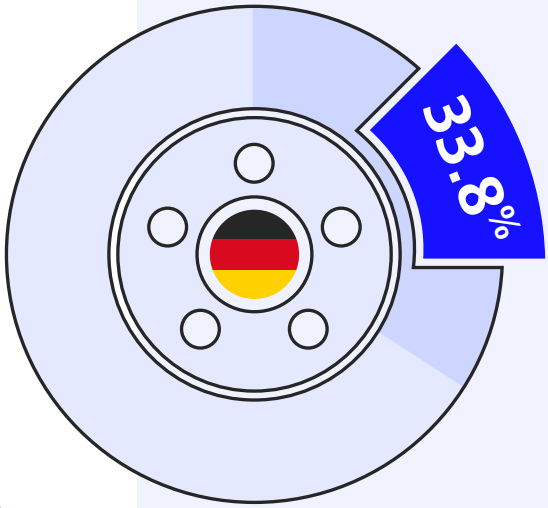
In Germany, 45.3 percent expect Q-Day within the next five years, by 2031; in the United States, as many as 55.2 percent do. A further 39 percent in Germany and 33.5 percent in the U.S. expect it within the next ten years, by 2036.

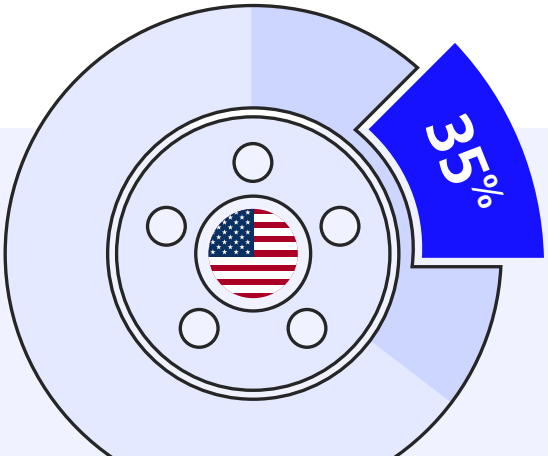
45.3%

55.2%

Legacy Systems Are Slowing Progress

Complex legacy systems are the main factor behind the slow transition to PQC. In Germany this affects 33.8 percent of companies surveyed; in the U.S., 35 percent.





Introduction

Quantum computers are increasingly evolving from a theoretical concept into a technology of practical relevance. Their progress opens up new fields of application, but at the same time creates substantial risks for IT security. In particular, there is a risk that established cryptographic methods will no longer provide adequate protection in the future. The point in time at which quantum computers will be capable of compromising today's commonly used encryption methods is referred to as "Q-Day."

This threat is not limited to a future scenario. Even today, encrypted data can be intercepted and stored in order to be decrypted later using powerful quantum computers. This approach is known as "store now, decrypt later." Against this backdrop, early engagement with Post-Quantum Cryptography (PQC) is becoming increasingly important. The goal is to establish cryptographic methods that are resistant to attacks by quantum computers and to gradually align existing products and systems accordingly.

To provide an overview of the status of post-quantum cryptography in Germany, and the U.S. the management and IT consultancy MHP surveyed 1,060 IT experts from companies with at least 500 employees in both Germany and the United States. The results offer a valid snapshot of progress in two of the world's leading economies.

The results provide a reliable snapshot of sentiment regarding progress in Germany and the United States – two of the world's leading economies.[1]

[1] Largest Economies (GDP) Worldwide in 2024 | Statista

„We're talking about a window of opportunity that's about to close: Most companies expect Q-Day to arrive within the next five to ten years, but migrating to new encryption often takes just as long. This is a structural problem, not a technical detail. Anyone still stuck in legacy systems today risks having their sensitive data compromised before their own transformation is even complete."

Markus Wambach
Group COO – MHP Management- und IT-Beratung GmbH

Attention Instead of Niche

Post-quantum cryptography no longer plays a marginal role – neither in Germany nor in the United States.

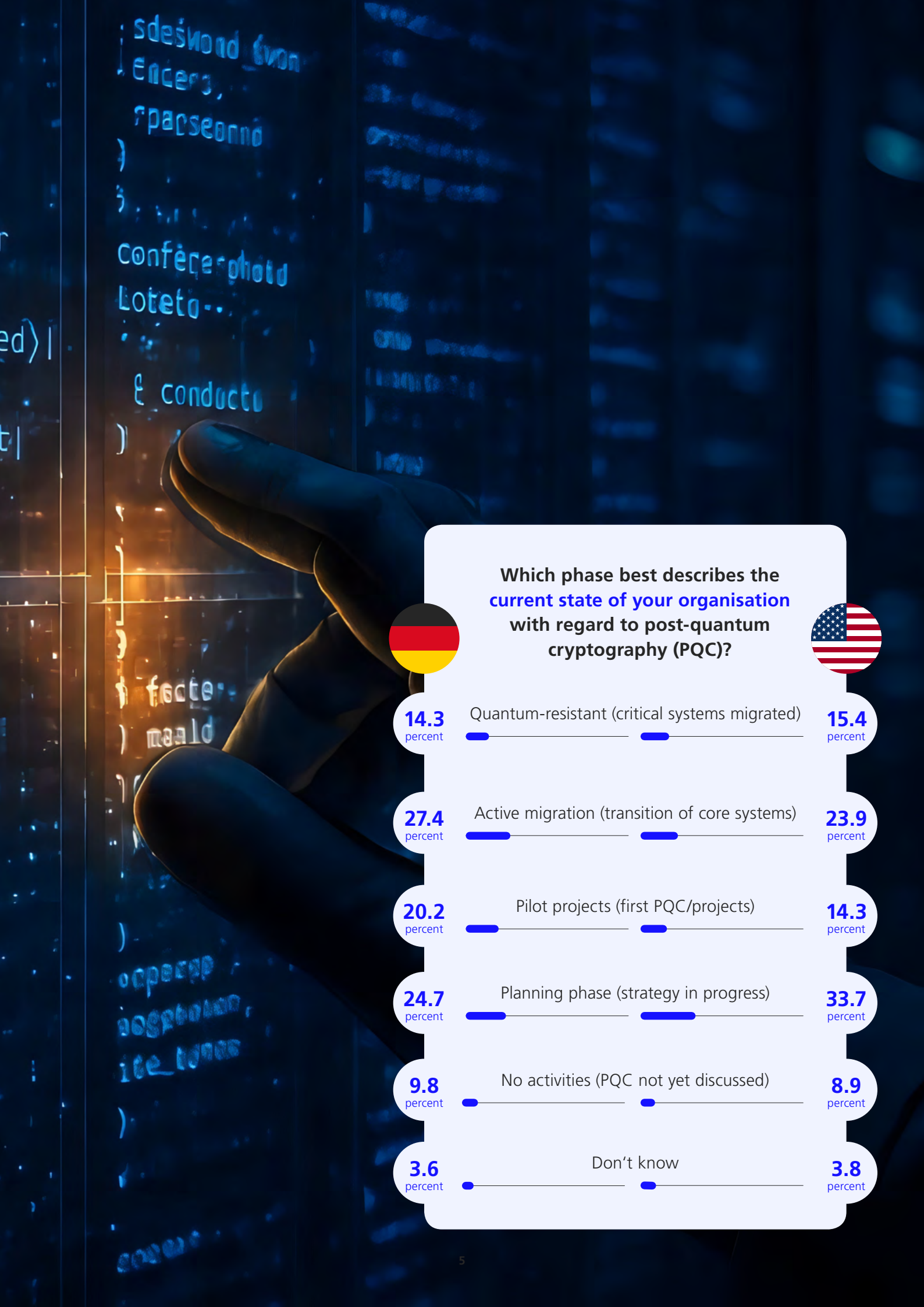
In Germany 86.6%

are dealing with the topic;

in the U.S. 87.3%

Particularly noteworthy: In Germany, 27.4 percent of organizations are already in active migration, and another 14.3 percent have even migrated critical systems to PQC and are therefore considered "quantum-resistant." The United States is almost on par, with 23.9 percent in active migration and 15.4 percent operating quantum-resistant systems.

At the same time, a concerning remainder persists: 9.8 percent of German companies and 8.9 percent of U.S. companies state that they have not yet begun any activities at all. Against the backdrop of the expected Q-Day timeframes and the "store now, decrypt later" problem, this represents a strategic risk – because those who do not act today are effectively planning to start migration only once the threat has already become real.



Which phase best describes the current state of your organisation with regard to post-quantum cryptography (PQC)?

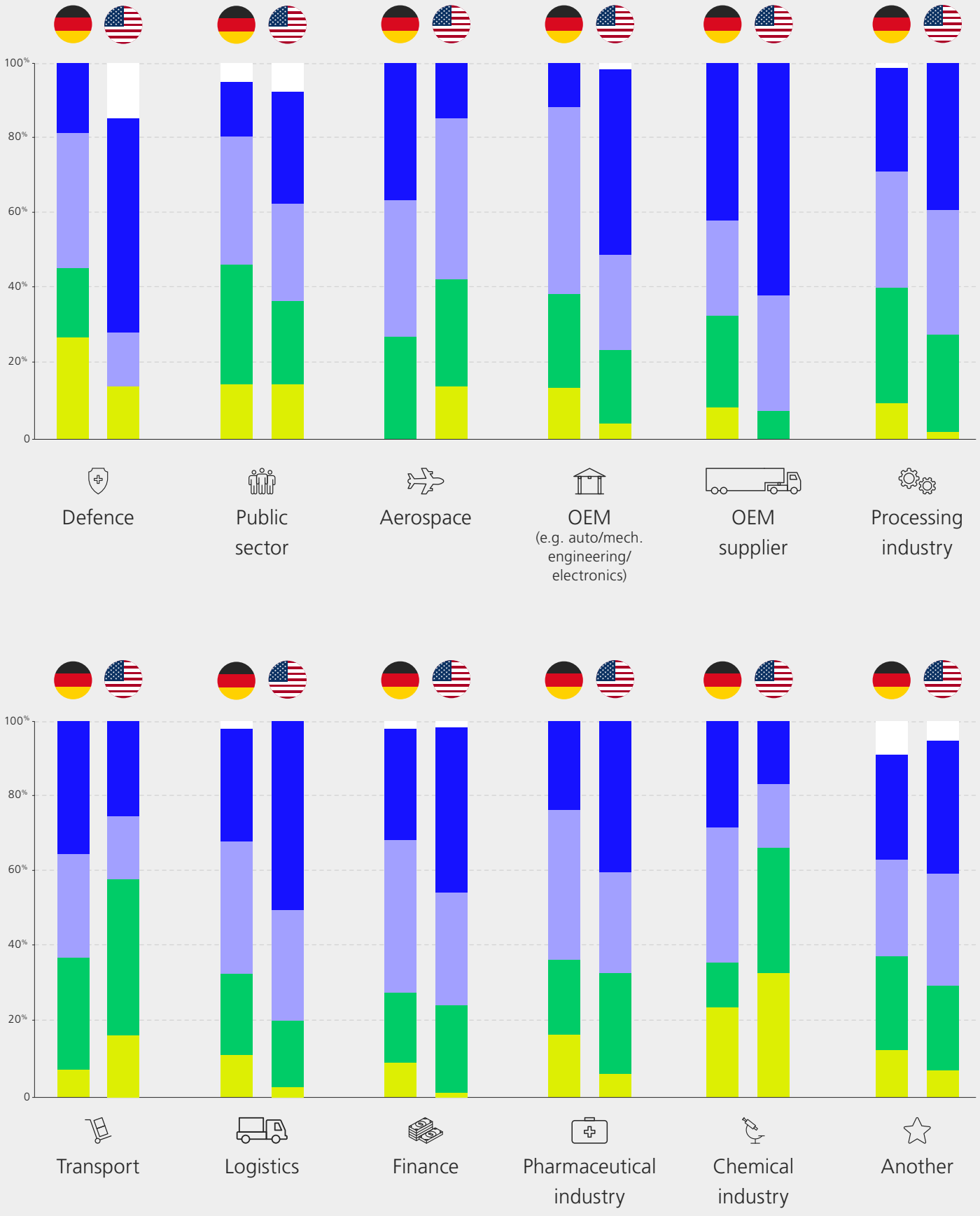
14.3 percent	Quantum-resistant (critical systems migrated)	15.4 percent
27.4 percent	Active migration (transition of core systems)	23.9 percent
20.2 percent	Pilot projects (first PQC/projects)	14.3 percent
24.7 percent	Planning phase (strategy in progress)	33.7 percent
9.8 percent	No activities (PQC not yet discussed)	8.9 percent
3.6 percent	Don't know	3.8 percent

Management Attention and Budget – PQC Becomes a Board-Level Issue

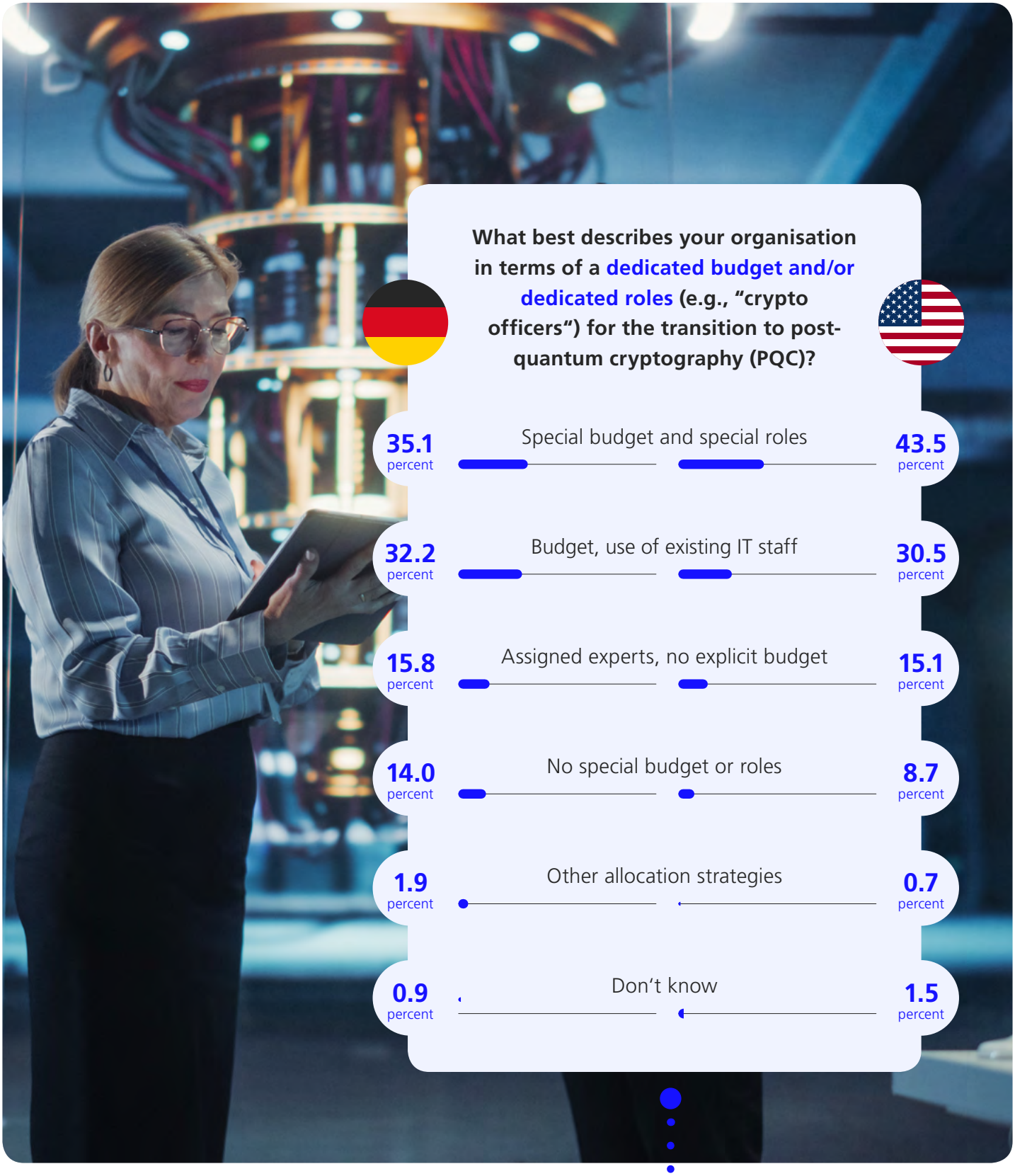
The broad engagement with PQC is evident not only in technical activities, but increasingly at the leadership level as well. In 25.8 percent of German companies, PQC is already a strategic board-level topic; in the United States, this applies to as many as 39.7 percent. As a result, PQC has long since moved beyond an expert niche in many organizations and has become an issue actively addressed by top management. Only 12.3 percent of German companies and 6.2 percent of U.S. companies state that PQC is not on the radar of senior management at all.

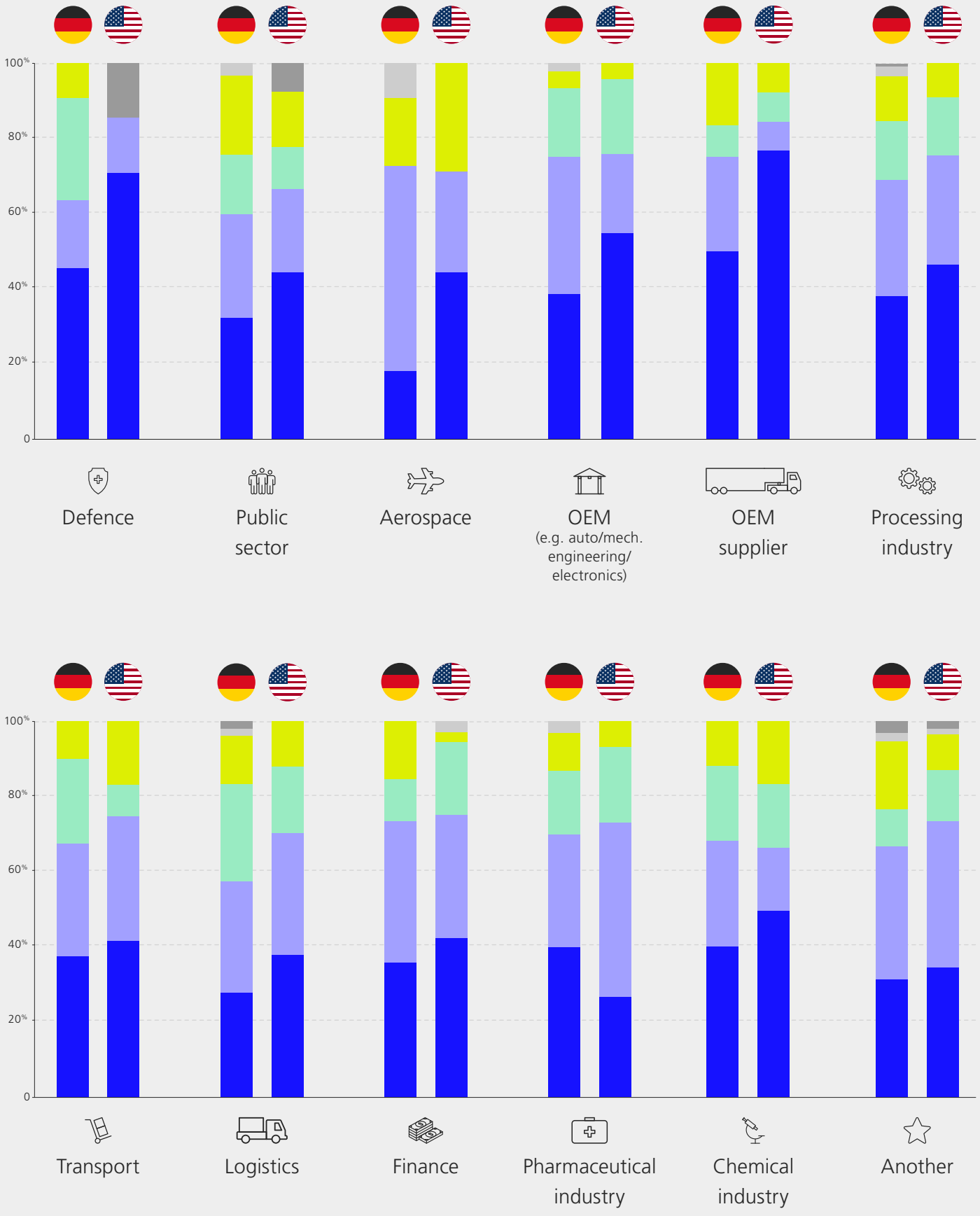
Which statement best describes the priority of the transition to post-quantum cryptography (PQC) on the strategic agenda of your company's management/board?

25.8 percent	Important strategic initiative of the board	39.7 percent
34.2 percent	Part of the regular security roadmap	28.8 percent
25.1 percent	Being observed, but not an important driver	22.6 percent
12.3 percent	Not on the management's radar	6.2 percent
2.6 percent	Don't know	2.7 percent


100%
80%
60%
40%
20%
0
Defence
Public sector
Aerospace
OEM (e.g. auto/mech. engineering/ electronics)
OEM supplier
Processing industry
Transport
Logistics
Finance
Pharmaceutical industry
Chemical industry
Another
Not on the management's radar
Being observed, but not an important driver
Part of the regular security roadmap
Important strategic initiative of the board
Don't know

This leadership focus is also reflected in resource allocation: Around 67.3 percent of companies in Germany and 73.5 percent in the United States already provide a dedicated budget for their PQC migration, in some cases complemented by specifically introduced roles. The figures clearly show that PQC is no longer a peripheral aspect of cybersecurity, but a strategic transformation program anchored both organizationally and financially.




100%
80%
60%
40%
20%
0
Defence
Public sector
Aerospace
OEM (e.g. auto/mech. engineering/ electronics)
OEM supplier
Processing industry
Transport
Logistics
Finance
Pharmaceutical industry
Chemical industry
Another
Special budget and special roles
Budget, use of existing IT staff
Assigned experts, no explicit budget
No special budget or roles
Other allocation strategies
Don't knowt

“The progress of this development cannot be stopped. All the more reason to bring PQC even more strongly into focus. The impact of quantum computers on cybersecurity is real and not a distant future scenario.”

Dr. Jan Wehinger

Partner – MHP Management- und IT-Beratung GmbH

A Key Factor: Inventory Management

Clear differences in maturity also emerge in inventory management: while U.S. companies rely more heavily on automated approaches, manual methods still dominate in Germany.

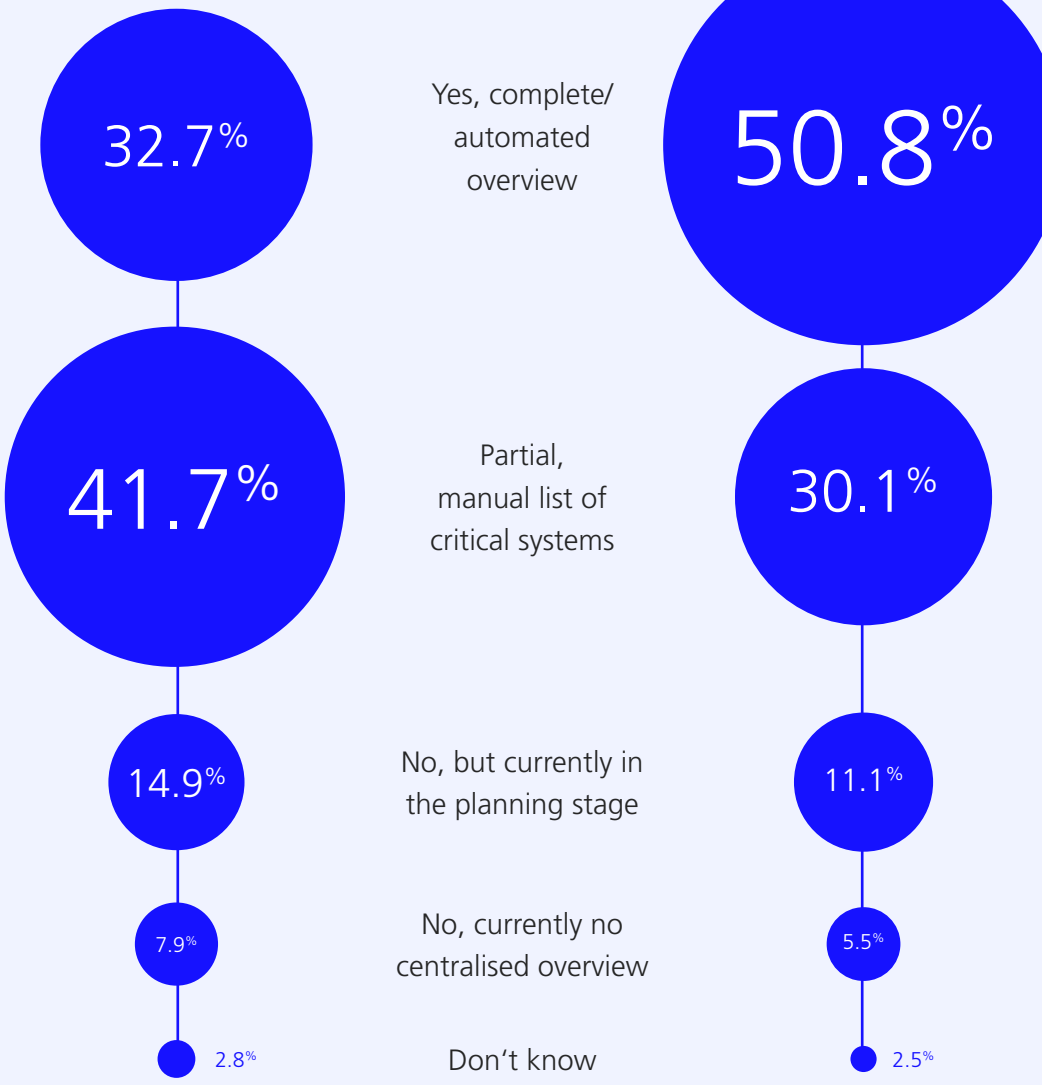
Another decisive difference between the United States and Germany can be seen in cryptographic inventorying, an important step in PQC migration. While 50.8 percent of U.S. companies already have a complete and largely automated overview of their cryptographic assets, Germany lags significantly behind at 32.7 percent. The majority still work with manual lists that are neither complete nor up to date enough to plan a migration efficiently or to respond quickly in an emergency.

Yet this very overview is a strategic key factor: without knowing where cryptographic methods are used, which protocols are affected, and what

dependencies exist, PQC migration is hardly possible. Relevant both for this migration and beyond is crypto agility within companies – the ability to flexibly and quickly replace cryptographic methods. This capability depends directly on such an inventory. Those who do not know their cryptographic landscape simply cannot respond in time to new threat scenarios.

The figures clearly show: the United States has not only started earlier, but has also created the prerequisites to actually implement migration. Germany, by contrast, risks losing valuable time due to manual processes – at a stage when time itself is becoming a critical resource.

Does your company maintain a centralised „Cryptography Bill of Materials“ (CBOM) or a complete inventory of all cryptographic assets and their locations?



Paradox: Awareness vs. Time

In Germany, 45.3 percent expect Q-Day within the next five years, by 2031; in the United States, as many as 55.2 percent do. A further 39 percent in Germany and 33.5 percent in the U.S. expect it within the next ten years, by 2036.

This assessment is also shared by established security institutions and analyst firms: The Federal Office for Information Security (BSI), for example, has for years described post-quantum cryptography as one of the key security policy priorities and regularly emphasizes that organizations must begin migration proactively, as even moderate estimates foresee a threat within the coming decade. International analysts arrive at similar projections.

Gartner analysts summarize it succinctly in their Tech Trends 2025:

“By 2029, advances in quantum computing will make most conventional asymmetric cryptography unsafe to use.”

Particularly alarming, however, is the technological trend of recent years. The theoretically required number of physical qubits to break RSA keys has steadily declined over the past decade – not only due to hardware breakthroughs, but above all because of advances in algorithms and error correction.

- In 2012, researchers (Fowler et al.) still estimated the requirement at around 1 billion physical qubits.
- In 2025, Google Quantum AI scientists (Gidney et al.) reduced this estimate to around 1 million qubits – a reduction by a factor of 1,000.
- In 2026, a preprint by Webster et al. (Iceberg Quantum) even suggested that fewer than 100,000 physical qubits might suffice to break RSA (Rivest-Shamir-Adleman) – one of the most widely used encryption methods today, employed among other things for secure internet connections.

This development shows a clear trend:
The threshold for cryptographic relevance is falling faster than originally assumed.

The situation becomes even more critical when these figures are compared with the roadmaps of leading hardware manufacturers:

- U.S. company IonQ plans systems with around 200,000 qubits by 2029 and up to 2 million by 2030.
- European quantum start-up IQM cites targets of 100,000 qubits by 2031 and 1 million by 2033.

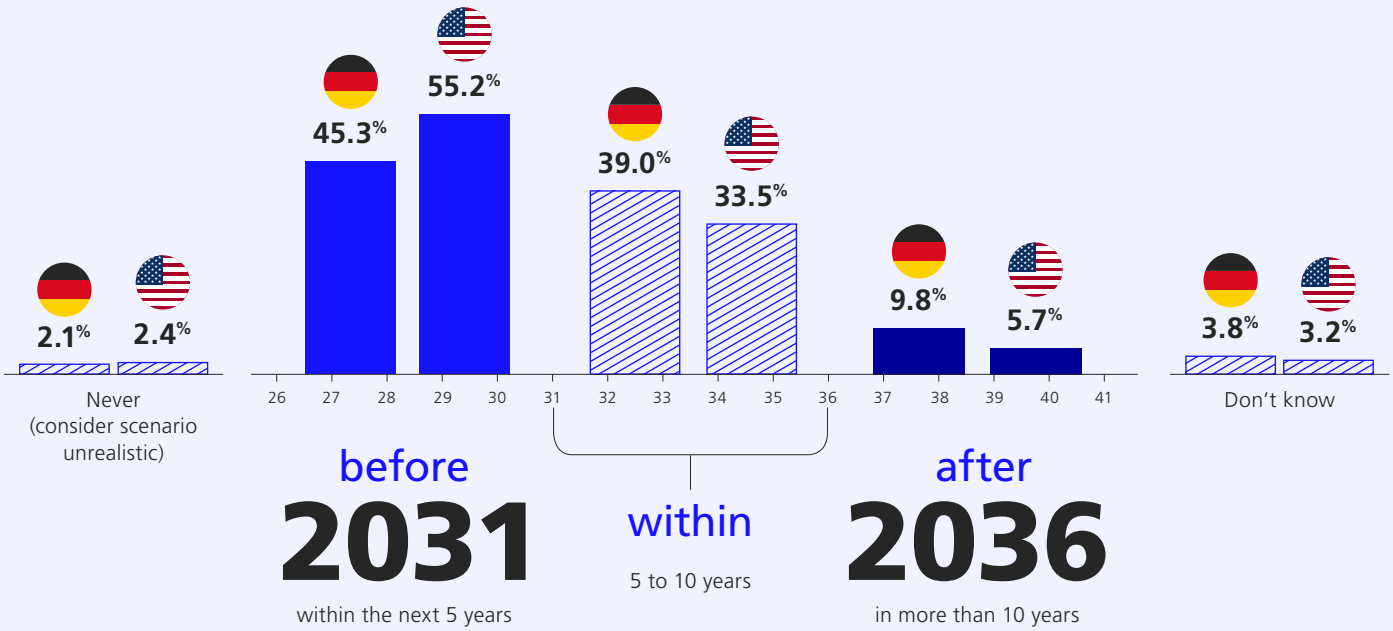
Even when technological realities are assessed conservatively, the combination of

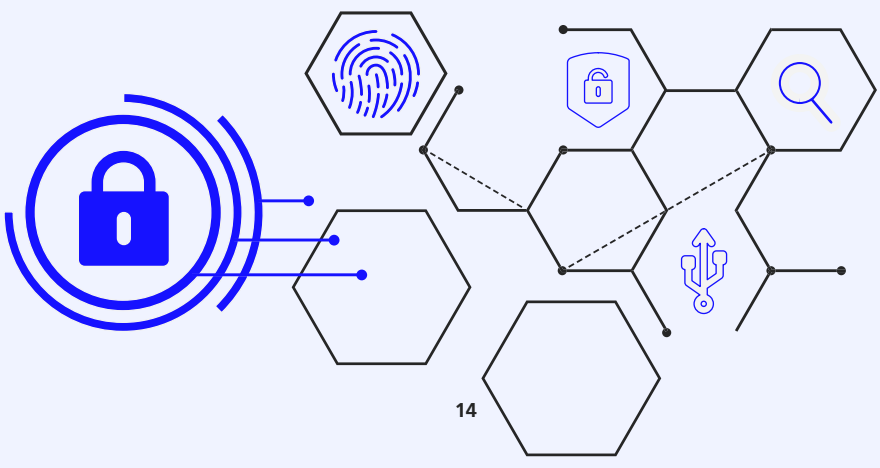
→ declining qubit requirements,
→ increasingly efficient algorithms, and
→ massively accelerated development roadmaps

produces a consistent global picture:
Q-Day is being pulled forward rather than pushed back.

As a result, the 5–10 year timeframe assumed by the majority of respondents appears realistic – possibly even too optimistic.

In which year do you think a cryptographically relevant quantum computer (CRQC) will be able to decrypt the current RSA/ECC encryption?

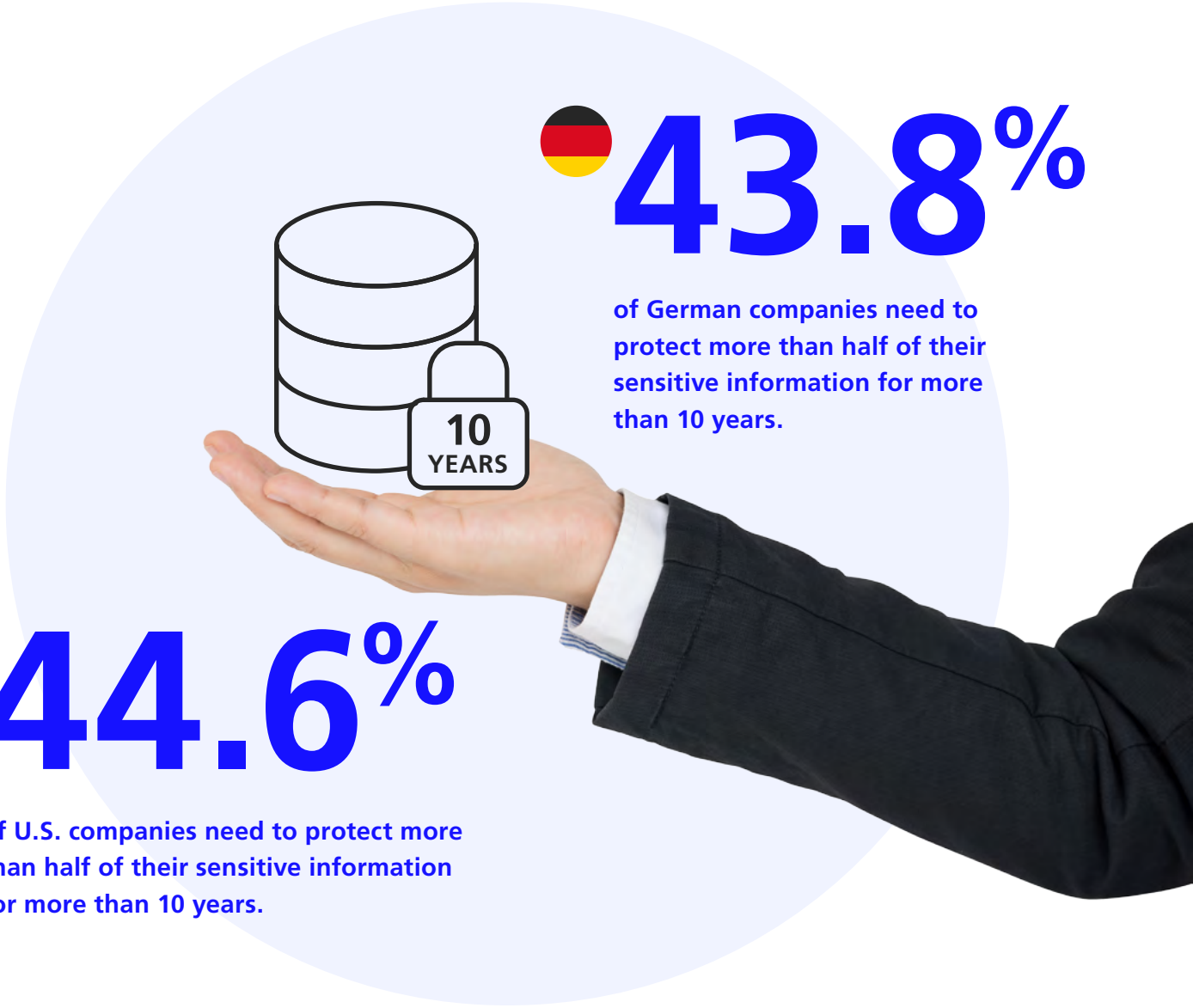




Companies Know How Much Sensitive Data They Hold – and How Long It Must Be Protected

One crucial and often underestimated factor is the share of data that must be protected for more than ten years. According to our survey, this applies to more than half of sensitive information for 43.8 percent of German companies and 44.6 percent of U.S. companies (categories "51–75%" and "76–100%").

For these organizations in particular, the "store-now, decrypt-later" threat represents a significant risk: data intercepted today remains exploitable even if Q-Day occurs only in five or ten years. For companies with long-term sensitive information, every delay increases the likelihood that attackers already possess data that can later be decrypted.



43.8%

of German companies need to protect more than half of their sensitive information for more than 10 years.

44.6%

of U.S. companies need to protect more than half of their sensitive information for more than 10 years.

What percentage of your company's sensitive data requires a confidentiality period of 10 years or more (e.g., due to long-term legal requirements or health data)?

	🇩🇪	🇺🇸
0–25%	7.9%	11.5%
26–50%	46.4%	41.6%
51–75%	32.8%	33.5%
76–100%	11.0%	11.1%
Don't know	1.9%	2.3%

The forecast migration timelines underscore that delayed or still absent activities can lead to structural backlogs.

While most companies expect Q-Day within the next five to ten years, they simultaneously estimate migration timelines that fall squarely within this critical window.

In Germany,

53.4 %

of respondents expect a PQC migration to take between two and under five years; a further

27.5 %

anticipate five to ten years.

In the United States, a very similar picture emerges:

51.8 %

calculate two to five years, and

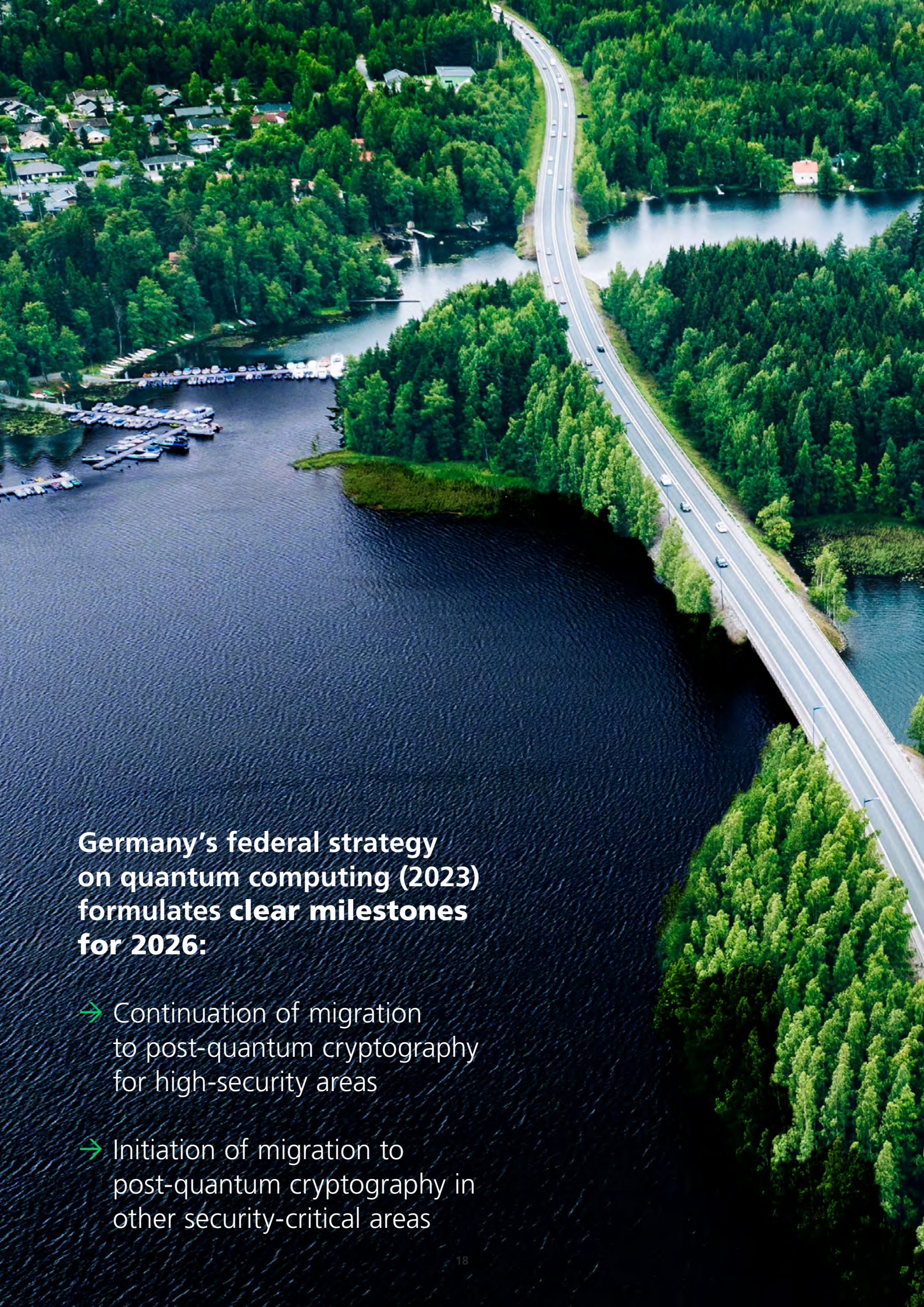
21.8 %

five to ten years.

This exposes a structural risk:

Those who have not yet started today will not be able to complete migration before the projected arrival of Q-Day.

The “store-now, decrypt-later” problem further exacerbates this situation, because data intercepted today can be decrypted in five to ten years if companies are still in the middle of their migration. This assessment is supported not only by analysts and research institutions, but also by political guidelines and warnings.



Germany’s federal strategy on quantum computing (2023) formulates clear milestones for 2026:

- Continuation of migration to post-quantum cryptography for high-security areas
- Initiation of migration to post-quantum cryptography in other security-critical areas

The implicit finding:

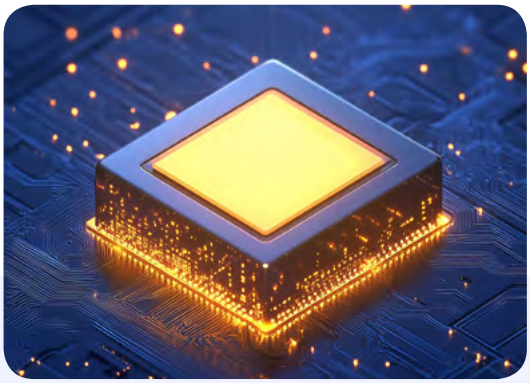
For high-security areas, migration should already be underway. And for all other critical sectors, the starting point has been reached at the latest now. This urgency is reinforced across Europe. In a joint statement, 18 EU member states and their national cybersecurity authorities summarize:

“We urge public administration, critical infrastructure providers, IT providers, as well as all of industry, to make the transition to post-quantum cryptography a top priority. For the reasons outlined above, organizations and governments should start the transition now.”

Taken together, a clear picture emerges:

- → Q-Day is approaching faster than expected, as both qubit requirements and hardware roadmaps point toward acceleration.
- → The expected migration timelines of many companies lie dangerously close to the projected Q-Day.
- → Governments explicitly call for migration to begin now in order to preserve security and operational resilience.

The strategic consequence is therefore clear: Those who do not begin this year are effectively planning a migration into an already compromised cryptographic system.



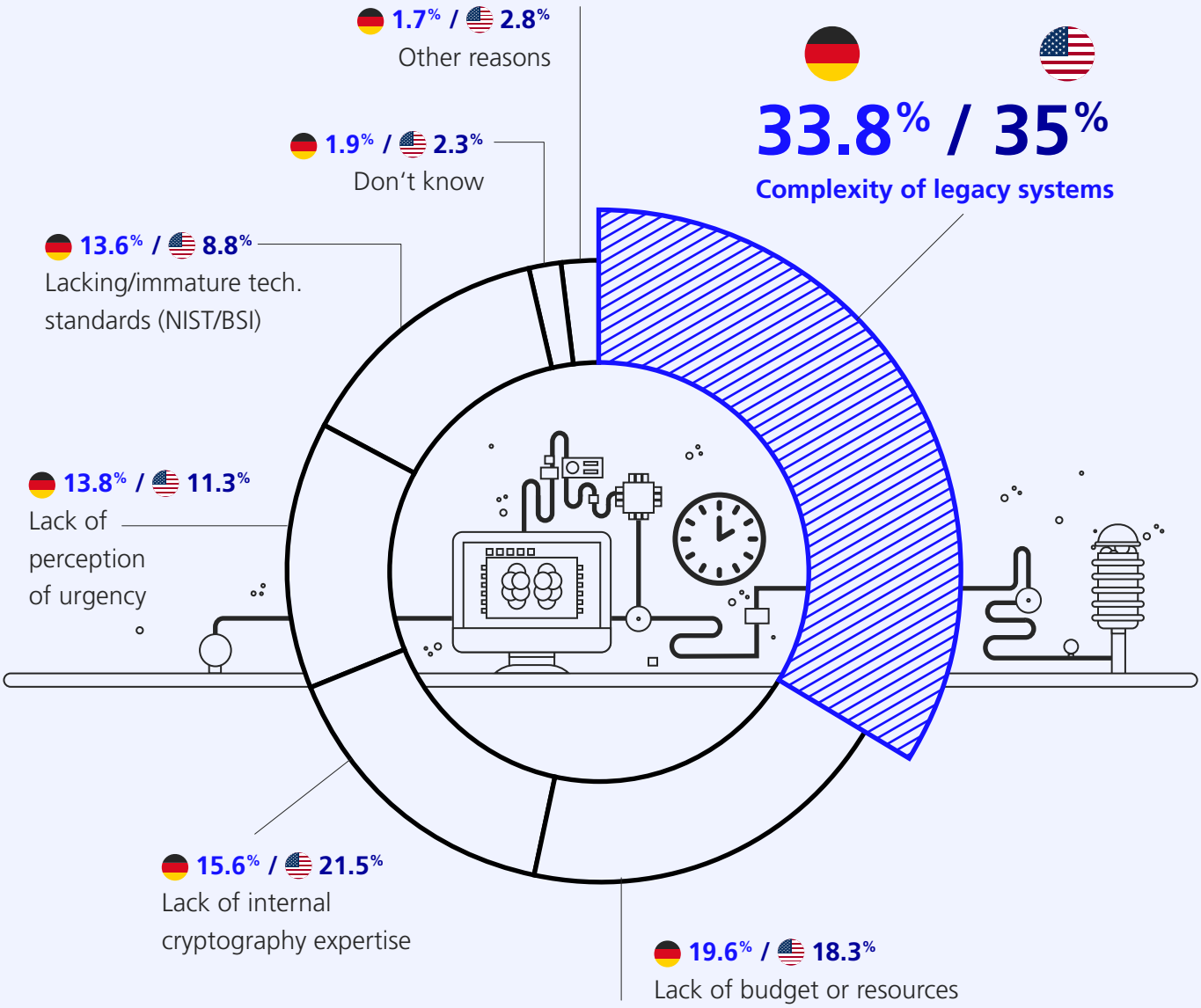
How many years do you estimate it will take to complete the technical migration to post-quantum cryptography (PQC) across your organisation?

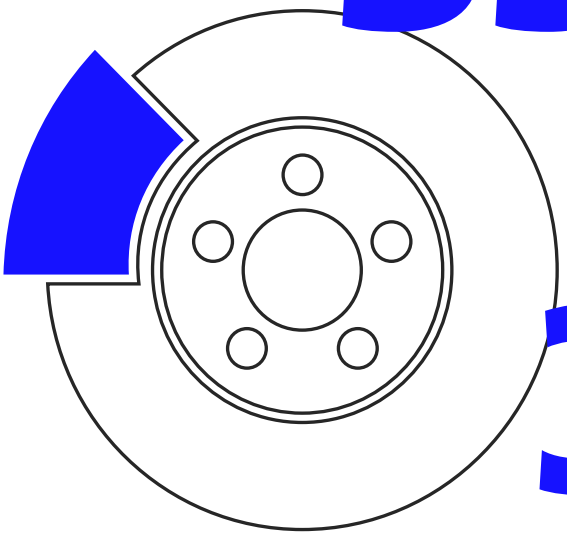
10.6 percent	Less than 2 years	17.9 percent
53.4 percent	2 to less than 5 years	51.8 percent
27.5 percent	5 to 10 years	21.8 percent
5.3 percent	More than 10 years	5.1 percent
3.2 percent	Don’t know	3.4 percent

Reasons for Slow Implementation

Across industries and regions, complex legacy systems prove to be the dominant braking factor in the introduction of PQC. Organizational and personnel-related factors – such as limited financial resources or a lack of in-house cryptography expertise – further complicate PQC migration.

What is currently the main factor slowing down or preventing your organisation's transition to post-quantum cryptography (PQC)?





33.8%

Complex legacy systems are the main factor behind the slow transition to PQC among the companies surveyed.

35%

“Those who get their legacy systems under control also enable a timely transition to PQC – but there is no time left to lose,” explains Christian Zgardea, Partner at MHP. “There is nothing to be gained by waiting. Even beyond PQC, it pays to keep one’s own systems under control and to limit uncontrolled growth.”

Christian Zgardea
Partner Cyber Security – MHP Management- und IT-Beratung GmbH

Conclusion

The results show two sides of the same development. On the one hand, Germany and the United States have begun, at remarkable speed, to make post-quantum cryptography a fixed component of their security strategies. With more than 40 percent of companies already in active migration or even in a quantum-resistant state, the transformation process in many cases is not only underway but well advanced. This demonstrates that PQC is no longer a theoretical concept –
it is being implemented in practice, embedded in critical systems, and increasingly managed strategically.

At the same time, the core message remains clear: Q-Day is approaching faster than many organizations realize, and the self-estimated migration timelines come dangerously close to that point. Added to this are the high proportion of data requiring long-term protection and the growing gap between rapid technological progress in quantum hardware and the persistence of legacy hurdles within companies.

The combination of rising awareness, increased management attention, and growing investment is a strong signal – but it is not enough as long as a significant minority continues to hesitate.

The real challenge now is to leverage the existing momentum and turn the transformation from an exceptional project into standard practice across the board.

Those who act today can future-proof their systems and mitigate one of the central security challenges of the coming decade.

Those who wait risk beginning migration only once the cryptography of today has already been compromised.

Publisher

MHP Management- und IT-Beratung GmbH

MHP is an international management and IT consultancy headquartered in Ludwigsburg, Germany. For nearly three decades, the company has been supporting the transformation of processes and products for around 300 clients worldwide across the Automotive, Manufacturing, Aerospace, Public, and Defense sectors. As part of the Porsche Group, MHP provides both strategic and operational consulting in key areas such as Customer Experience and Workforce Transformation, Factory Planning, Supply Chain Management, Cloud Solutions, Integration and Scaling, Cyber Security, Big Data and Artificial Intelligence, Platforms and Ecosystems, as well as Industry 4.0 and Intelligent Products. The goal is to sustainably enhance speed, sovereignty, and resilience. The consultancy operates internationally, with its headquarters in Germany and subsidiaries in the USA, Mexico, India, the United Kingdom, Romania, and China. Around 4,500 MHP employees share a commitment to excellence and sustainable success. This ambition continues to drive the company – today and in the future.

mhp.com/newsroom

Survey methodology

The survey was conducted online between February 5 and February 16, 2026. In each country, 530 IT experts from companies with at least 500 employees in Germany and the United States were surveyed. The results are representative, were analyzed using quota sampling, and account for a statistical margin of error of 4.3 percentage points.

Layout & Design: www.freiland-design.de

Contact

MHP
A PORSCHE COMPANY

SPONSOR
Dr. Jan Wehinger
Partner

E-Mail: jan.wehinger@mhp.com

AUTHOR
Julian Seyfarth
Associate

E-Mail: julian.seyfarth@mhp.com

EXPERT
Kevin Euler
Associated Partner Cyber Security

E-Mail: kevin.euler@mhp.com

AUTHOR
Mirko Geyer
Spokesperson AI, Cyber Security, Aerospace & Defense

E-Mail: mirko.geyer@mhp.com

EXPERT
Christian Zgardea
Partner Cyber Security

E-Mail: christian.zgardea@mhp.com

www.mhp.com