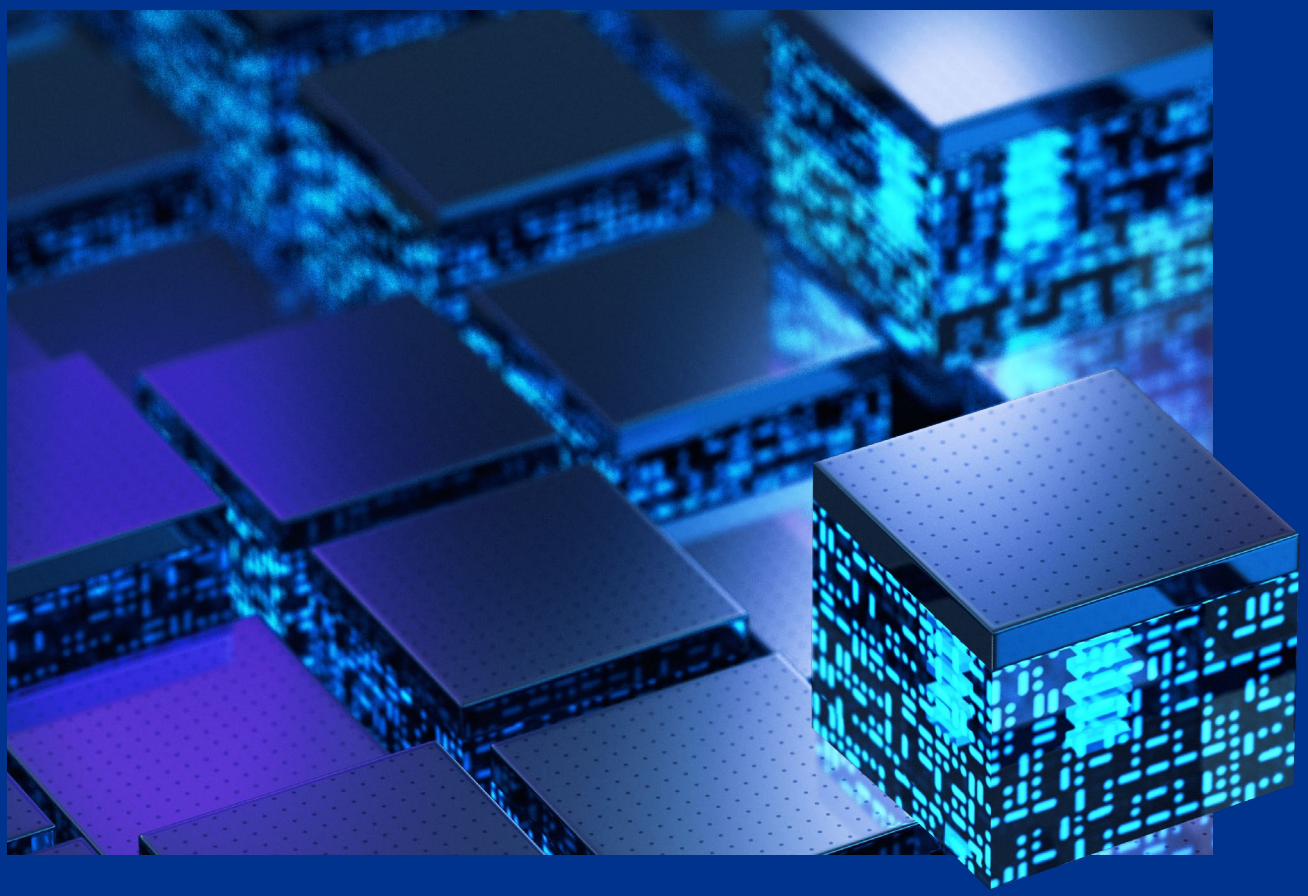
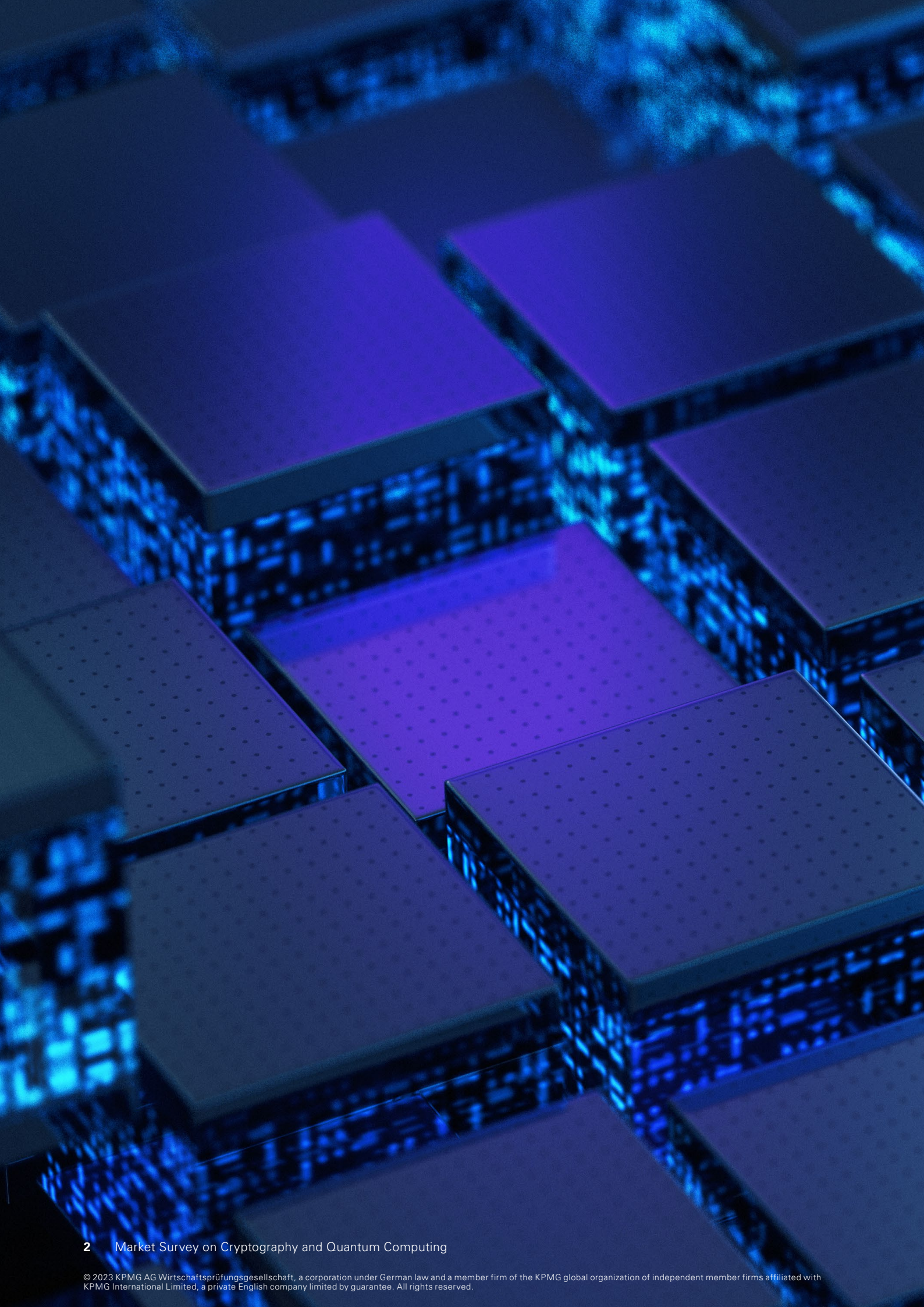
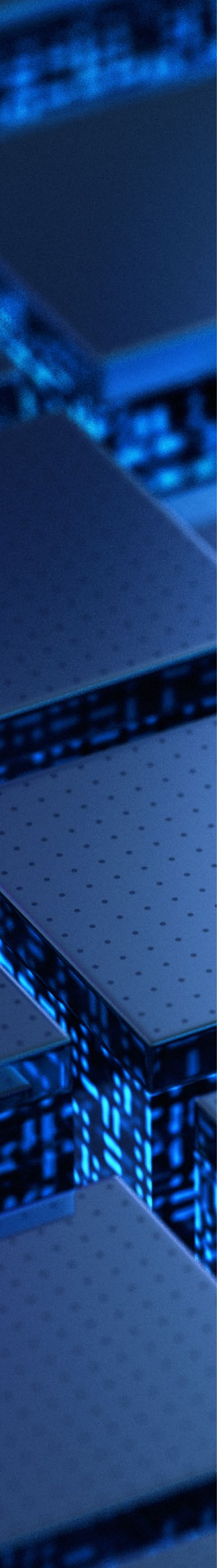
KPMG

Federal Office
for Information Security

Market Survey on Cryptography and Quantum Computing







Contents

1.
Introduction **04**

2.
The most important in a nutshell **07**

3.
Scenarios **08**

4.
Results **10**

4.1
How familiar are the participants with the topic? 11

4.2
To what extent are the participating organisations affected? 14

4.3
Can the organisations migrate to quantum-safe cryptography in good time? 17

4.4
What measures are the organisations taking? 20

4.5
What support do the companies require for the next steps? 24

5.
Summary, recommended actions and outlook **27**

1. Introduction

As the digital transformation continues, a growing proportion of our data is stored, processed and transferred in electronic form. This trend is opening up extensive new possibilities, but it also makes us increasingly dependent on technology. Cryptography is essential in order to guarantee the authenticity, integrity and reliability of information. Although it frequently goes unnoticed, cryptography is more or less omnipresent in the digital age.

Quantum computing is a technology that is being developed to harness the specific laws of physics governing the smallest particles (quantum mechanics) to perform efficient calculations. It is unclear as to when this technology will reach maturity in terms of practical applications – but it already exists and is becoming more powerful with each passing month. From biotechnology to urban planning, quantum computing offers the potential for huge progress. At the same time, however, it involves new risks with regard to information and communication security.

As well as looking at the opportunities presented by this emerging and revolutionary technology, we must therefore also be prepared to deal with the accompanying risks, which are significant and far-reaching. Late last year, the German Federal Office for Information Security (BSI) published guidelines entitled "Quantum-safe cryptography – fundamentals, current developments and recommendations".

Cryptographic techniques that are currently considered to be safe and that are firmly integrated into our digital infrastructures could be broken by quantum computers in the future. Accordingly, they will soon need to be replaced and supplemented by new, quantum-safe techniques such as post-quantum cryptography.

To provide the authorities, businesses and society with the best possible support in this field, the BSI and KPMG have conducted a joint survey covering a wide range of different organisations. The aim of the survey and this analysis of the results is to present the current situation across various industries so that it can be better understood, as well as drawing the necessary attention to the topic and delivering recommendations for action.

Approach:
This market study is the result of a cooperation between the BSI and KPMG Germany. Experts from the two organisations worked together to develop a questionnaire to survey the awareness and knowledge of the potential impact of quantum computing on cryptography and the status of companies' migration to more quantum-safe alternatives. This also included questions about the respective company (e. g. industry, size) and the position of the respondent within their organisation. 28 companies and organisations participated in the market study. The response rate was lower than for other studies of this type.

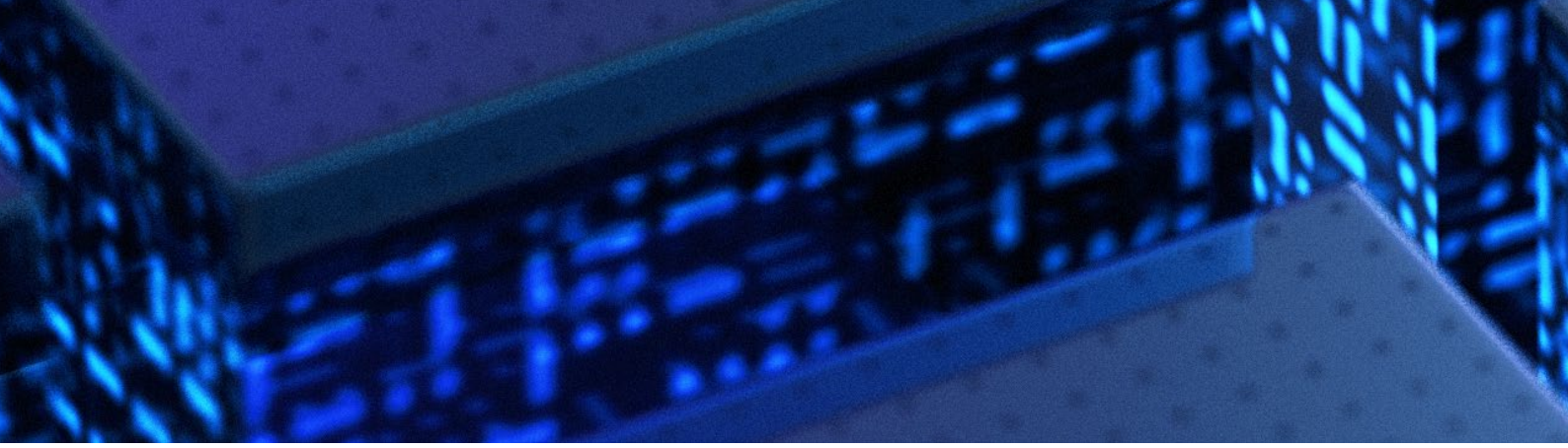
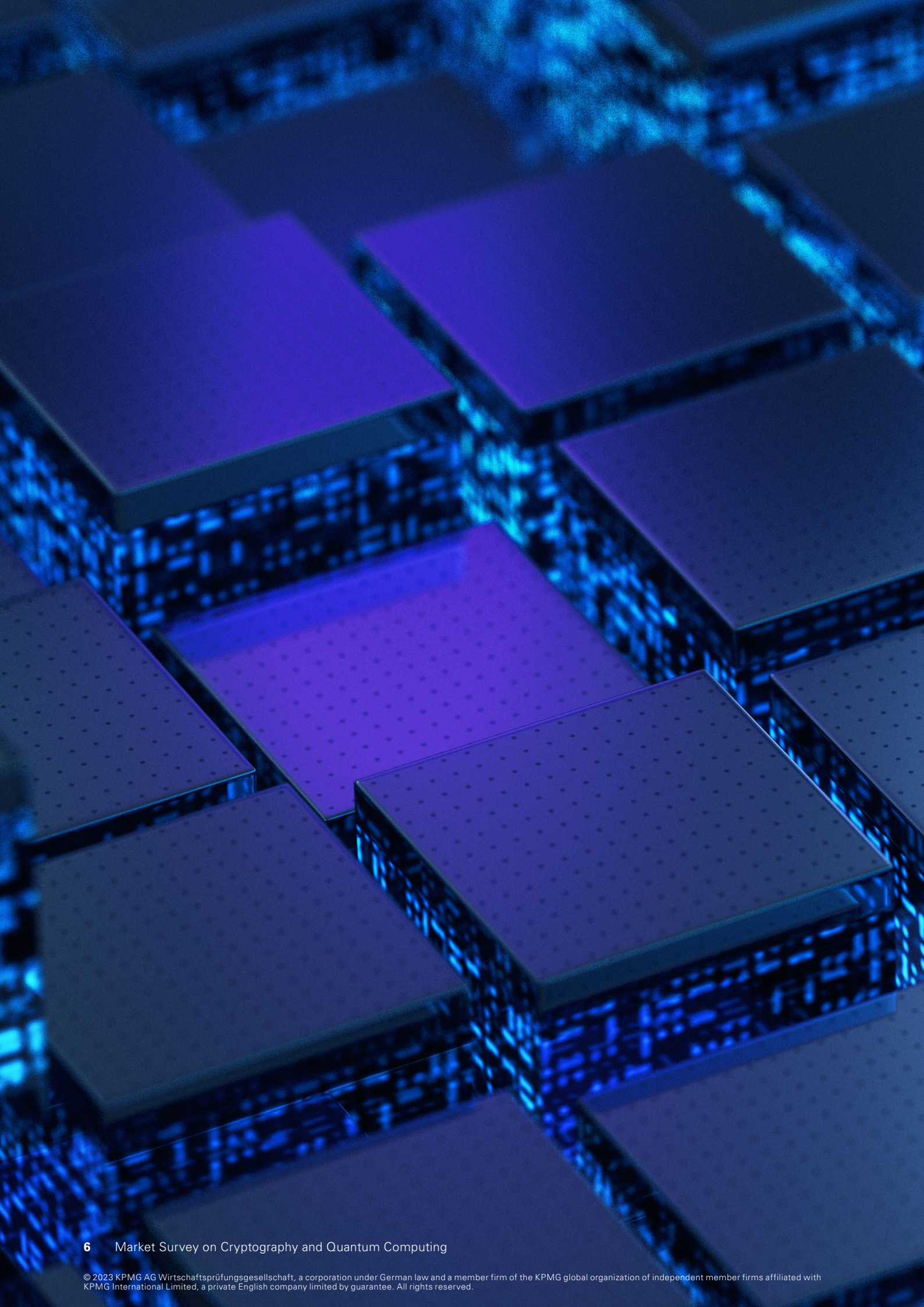


Fig. 1: Companies and organizations surveyed

Source: KPMG in Germany, 2022



2. The most important in a nutshell

Relevance

Over 95 percent of respondents rated the general relevance of quantum computing for the security of cryptographic techniques as “very high” or “high”.

Over 65 percent of respondents rated the average risk to data security within their own organisation as “very high” or “high”.

Timeframes

On average, the participants expect the cryptographic techniques currently in use to be broken in ten years’ time.

However, almost all participants expect the transition to more quantum-safe cryptography to take longer than is required to meet the confidentiality requirements for their organisation’s data.

Treatment

Only 25 percent of respondents said that the threat posed to cryptography by quantum computing is addressed in their organisation’s risk management system.

96 percent of participants stated that regulatory requirements would encourage investment decisions in favour of more quantum-safe cryptography, while 89 percent consider the existence of standards to be beneficial.

Responses

18.3 percent of the companies contacted participated in the survey.

71 percent of respondents agree with the prevailing expert opinion when it comes to the impact of quantum computing on cryptography.

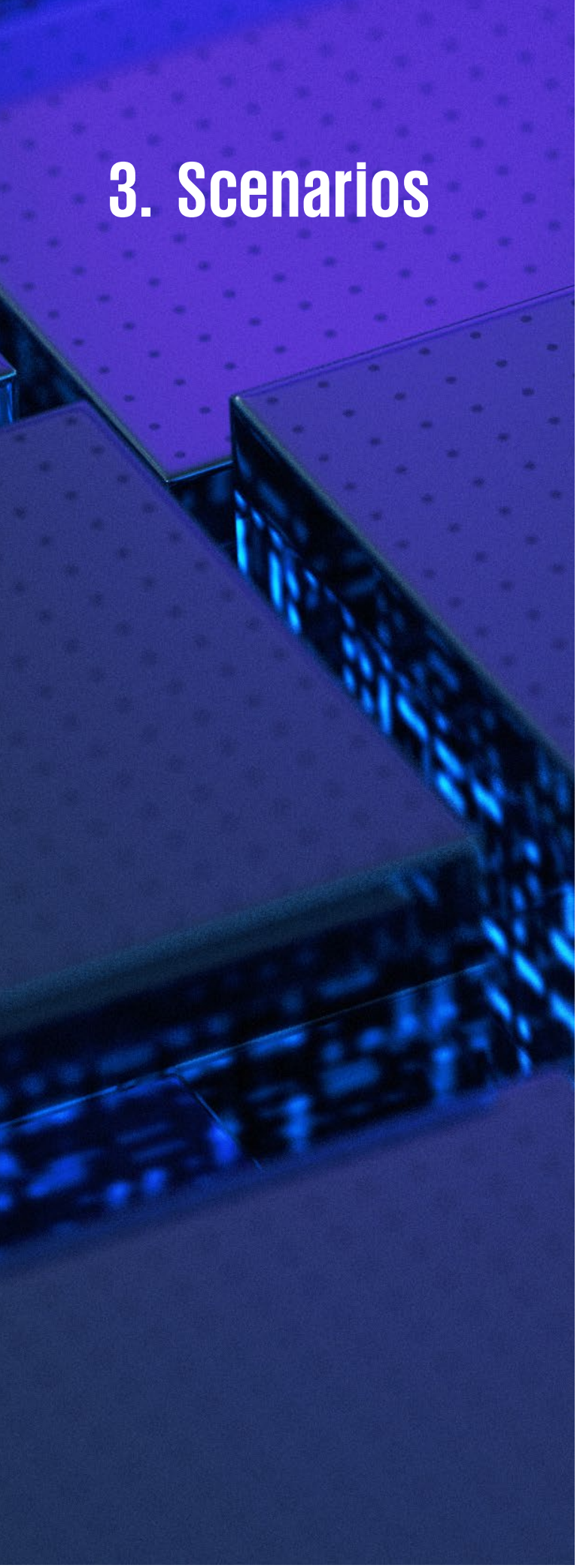
On average, the participants stated that they were “moderately familiar” with the topics listed.

Based on the information provided by the participating organisations, the study found that their confidential data will be vulnerable to quantum computing for many years.

Although there are countermeasures that can already be performed or initiated right now, this is not yet taking place to a sufficient extent.
An important first step appears to be establishing the necessary risk awareness and imparting techniques for handling the corresponding risks.

It is extremely worrying that only 11% of the participants believe there is a possibility that they will be quantum-safe in good time!

Hans-Peter Fischer
KPMG, Germany
Partner



3. Scenarios

Two specific scenarios illustrate simply but clearly the potential consequences of cryptographic techniques being broken and why organisations need to address the topic of quantum resistance:

Scenario 1 (Confidentiality):

A company that manufactures complex machinery has locations in several countries and on several continents. The product development team at the European development centre sends its strictly confidential production plans to the production facilities in various other countries via confidential telecommunication lines. Public key cryptography is used for these confidential communications. A future attacker is able to use quantum computing to break the public key encryption and read the confidential messages – without the manufacturing company being aware it is happening. The production documents allow the attacker to copy the complex machinery. Shortly afterwards, a competitor product with copied technology appears on the market at a lower price. The manufacturing company loses considerable market share to the new competitor. The practice of "store now, decrypt later" (see box on page 12 – reference to store-now decrypt later) means this can also affect production plans that are sent prior to quantum computing becoming available.

Scenario 2 (Authentication):

A company that provides communication components for consumer products, such as a supplier of door locking systems, uses public-key cryptography in its products for authentication purposes. The public keys used are linked to the corresponding components (e. g. an access card) via digital certificates; the certificates themselves are verified via a public key infrastructure (PKI). A future attacker is able to use quantum computing to break the public-key encryption and breach the security of the locking systems by obtaining access to the private key of a root certification authority. The attacker can then use this key to create signed certificates at its convenience. For example, they can make counterfeit access cards that the verification systems recognise as valid.
A similar attack scenario is conceivable in a wide range of other applications, such as critical infrastructure. The main problem is that root certificates can have a long lifespan. In future, this means that even cost-intensive attacks on a root certification authority using quantum computing may be worth pursuing under certain circumstances.

In every scenario, quantum-safe cryptography must be installed to prevent a specific threat before quantum computing has the opportunity to break the cryptography that is currently in use. The time needed for this is the development time for a product with quantum-resistant cryptography plus the time taken to implement the new development in existing products and components. It may also be necessary to take into account the length of time for which the information is required to remain confidential (as described in Mosca's theorem).

4. Results

The main findings of the survey are described below. The responses are grouped under the following key questions:

1. How familiar are the participants with the topic?

2. To what extent are the participating organisations affected?

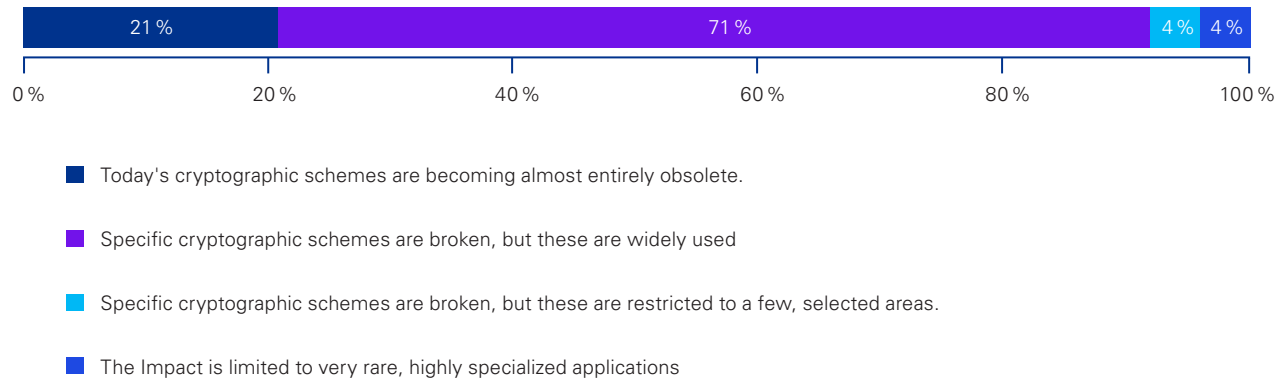
3. Can the organisations migrate to quantum-safe cryptography in good time?

4. What measures are the organisations taking?

5. What support do the organisations need for the next steps?

4.1 How familiar are the participants with the topic?

Fig. 2: In your view, what is the impact of quantum computing on cryptography?



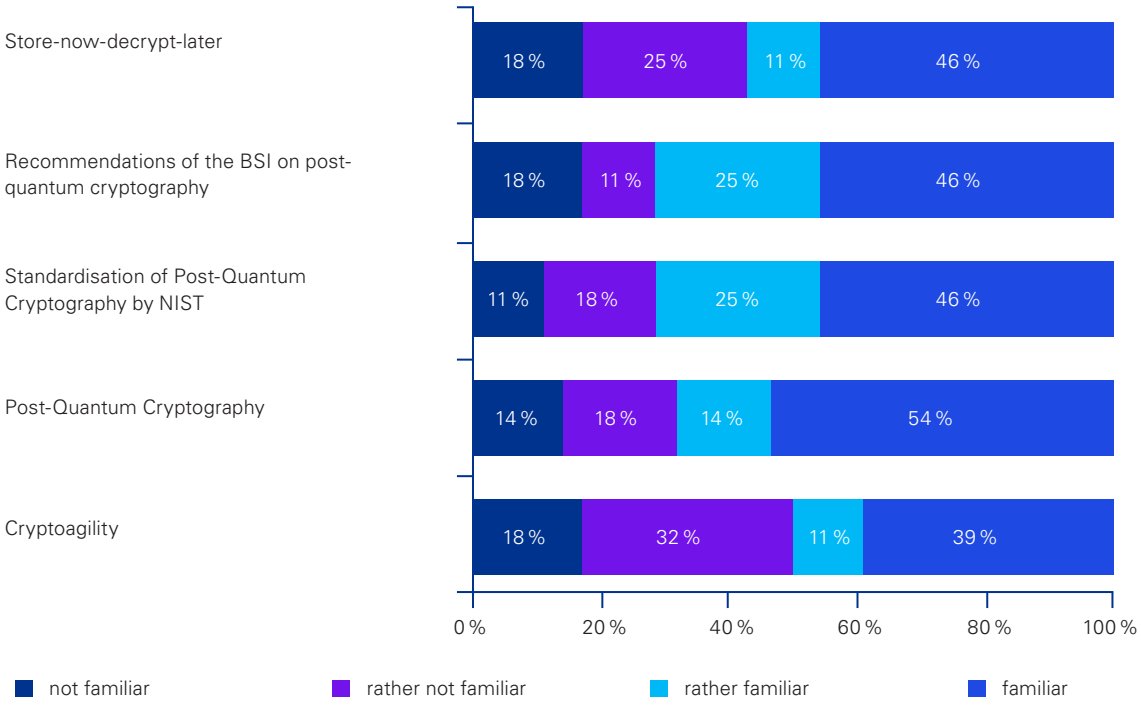
Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

To enable a better assessment of the other findings, the participants were firstly asked about their views concerning the impact of quantum computing on cryptography. 71 % said that they expected specific cryptographic techniques that are in widespread use to be broken. This corresponds to the prevailing expert opinion that public key cryptography in particular is under threat.

Assessment

This high level of agreement serves as an initial indicator that most of the participants were interested in issues relating to quantum computing and cryptography before they participated in the survey.

Fig. 3: How familiar are you with the following topics?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

The participants were also asked to rate their familiarity with various terms from the subject field. They were most familiar (responses of "very familiar" or "moderately familiar") with the current NIST standardisation process and the BSI recommendations on post-quantum cryptography (each 71 %), followed by post-quantum cryptography itself (68 %) and the "store now, decrypt later" concept (57 %). Cryptoagility took last place with a familiarity rate of 50 %.

Taken as an average for all of the topics and the feedback provided, the participants consider themselves to be "quite familiar" with the subject field.

As a general observation, the number of participants considering themselves to be "not familiar" with the five terms surveyed was low.

Store-now-decrypt-later

"Store now, decrypt later" describes the practice whereby encrypted information that is required to remain confidential for a considerable length of time is stored now, along with the public keys and the information exchanged on key negotiation, so that it can be decrypted as soon as quantum computing reaches the necessary maturity. This can also take the form of data harvesting, i.e. the large-scale, untargeted collection, storage and evaluation of data sent via public networks.
This possibility should be taken into account when sending long-term confidential data via accessible channels.

Cryptoagility

In cryptosystem design, cryptoagility describes the principle of keeping cryptographic mechanisms "as flexible as possible in order to respond to developments, implement future recommendations and standards, and replace algorithms that potentially no longer meet the desired security level in future[1]." This is extremely relevant with regard to quantum computing because the standardisation of quantum-safe algorithms and protocols is not yet complete. Once standards are available, however, cryptographically agile systems can quickly be made quantum-safe with minimal effort. Organisations can and should start making their own cryptography agile today, beginning with the creation of a comprehensive inventory of the cryptography used. It is worth mentioning that cryptoagility should also be an important design criterion irrespective of quantum computing, as even in traditional computing occasionally there is the need to replace cryptography at short notice (e. g. because of the OpenSSL vulnerability that was discovered in 2022).

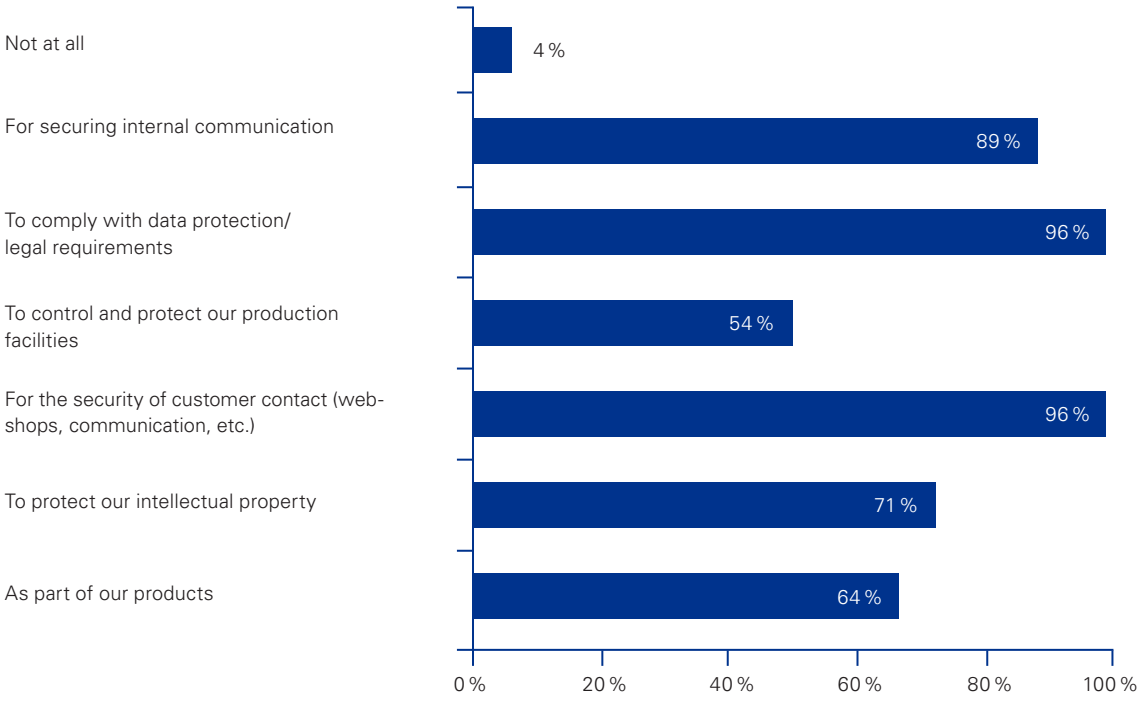
The 'store now, decrypt later' scenario clearly shows that the impact of quantum computing on cryptography is not merely a problem for the future. The threat is acute and needs to be addressed now.

Thomas Caspers
Head of Technology Competence Centres, BSI

[1] "Designing quantum-safe cryptography – basics, developments, recommendations", German Federal Office for Information Security (BSI), October 2021.

4.2 To what extent are the participating organisations affected?

Fig. 4: To which end are cryptographic techniques used in your organization?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

Answering this question firstly requires an assessment of the prevalence of cryptography within the respective organisation. Almost all participants said that cryptography was used at various places within their organisation. The most common uses were securing customer contact (96 %), complying with statutory requirements and data protection (96 %) and internal communication (89 %). The other responses were selected by considerably fewer participants (between 54 % and 71 %). The least common uses were "as part of our products" (64 %) and "to control and protect our production facilities" (54 %). Unlike the more frequently selected responses, the latter two aspects are more sector-specific because there can be considerable differences in terms of products and production facilities. "To secure customer contact" was selected by between 87.5 % and 100 % of respondents depending on the sector, whereas "as part of our products" was selected by between 33 % and 100 % of respondents. As such, it appears likely that the less frequent responses in this category are at least partially attributable to sector-specific aspects.

Cryptography is everywhere, and it is hard to imagine today's world without it. It is good that the participants are aware of this.

Wilhelm Dolle
KPMG Germany,
Partner, Head of Cyber Security

The participants were also asked about the general relevance of quantum computing for the security of cryptographic techniques. Across all sectors, 96 % of participants rated the relevance of quantum computing as "very high" (54 %) or "high" (43 %). It is notable that none of the participants rated the relevance of quantum computing as "very low" or "low". One respondent said that they had no opinion.

Assessment

Taken together, these two results suggest that the participants anticipate serious consequences if quantum computers become capable of breaking today's cryptographic techniques without adequate new technologies being deployed to combat them. On the other hand, the unanimity among the participants could also indicate that they come from a homogeneous group with a particular interest in quantum computing and cryptography in the first place.

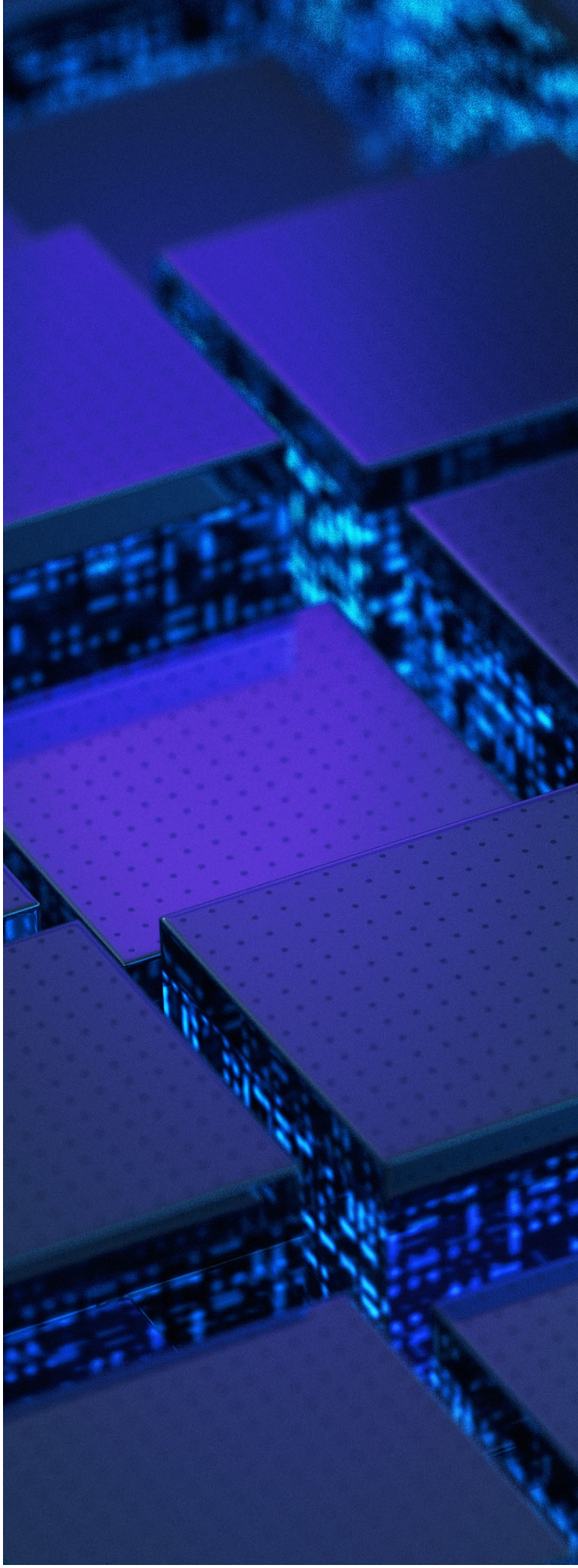
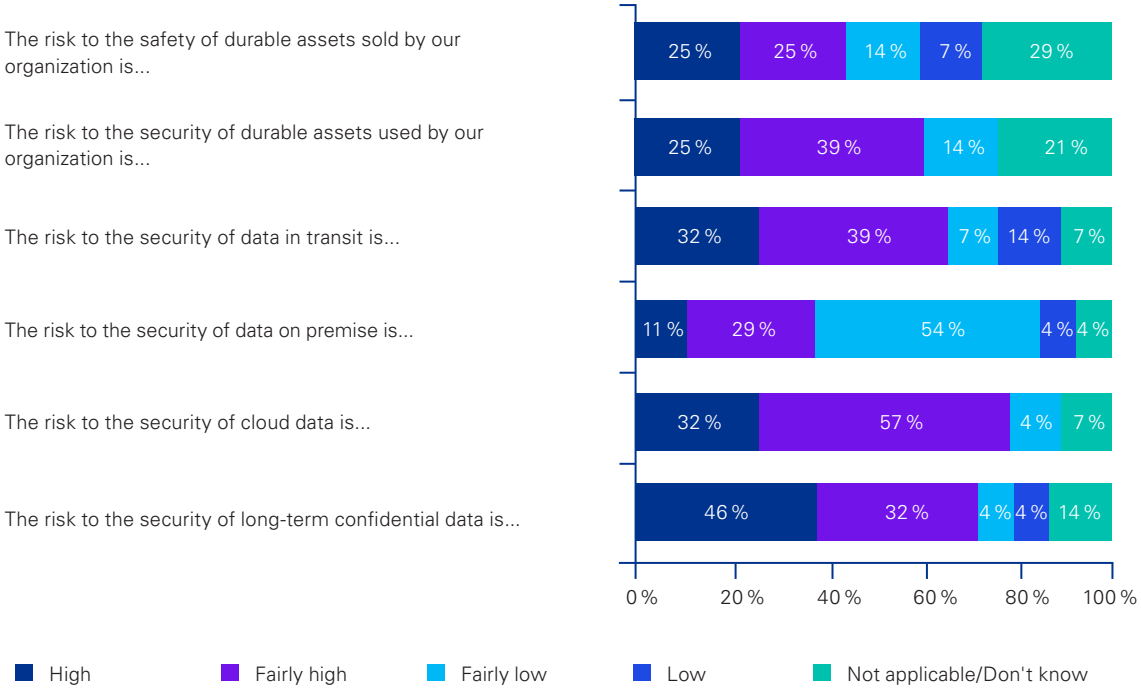


Fig. 5: How do you estimate the risks in your organization due to quantum computing?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

In terms of the risks to their organisation, 89 % of the participants rated the risk to cloud data as "high" or "quite high". The risk to long-term confidential data (78 %) and data in transit (71 %) is rated slightly lower. The security of durable goods is considered to be less of a risk factor, coming in at 64 % for the durable goods used by the organisation and 50 % for the durable goods sold by the organisation. Participants consider data on premise to be least under threat, with just 40 % anticipating heightened risk.

Assessment

When evaluating these figures, it should be noted that, for the most part, the data types surveyed are not mutually exclusive. For example, long-term confidential data might also be in transit to a cloud. It should also be noted that the specific risks to the respective organisation were surveyed, and not all organisations necessarily sell durable goods. It appears likely that the relatively low figures for this response are at least partially attributable to this factor.

With organisations still increasingly migrating their IT infrastructure away from in-house data centres in favour of cloud or edge solutions, these results also indicate a high risk potential.

There is a correlation between the participants' degree of familiarity with the topics surveyed and their assessment of the risk level. In other words, the more familiar the participants are with the various aspects of quantum security in the context of cryptography, the greater they consider the risk potential to be. This finding could serve as an additional motivator for broad-based information and awareness campaigns.

4.3 Can the organisations migrate to quantum-safe cryptography in good time?

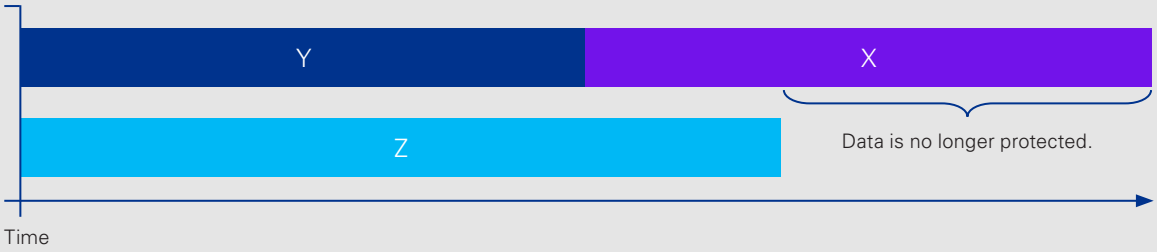
Mosca's theorem

The following formula developed by the theoretical physicist Michele Mosca vividly illustrates the time available for the migration to quantum computing-resistant cryptography.

Supposing that

- x is the number of years for which the data needs to be secured,
- y is the number of years required to migrate the corresponding system to quantum computing-resistant cryptography, and
- z is the number of years until there will be quantum computers that can break the cryptography that is currently in use.

If y+x > z, then you have a problem!

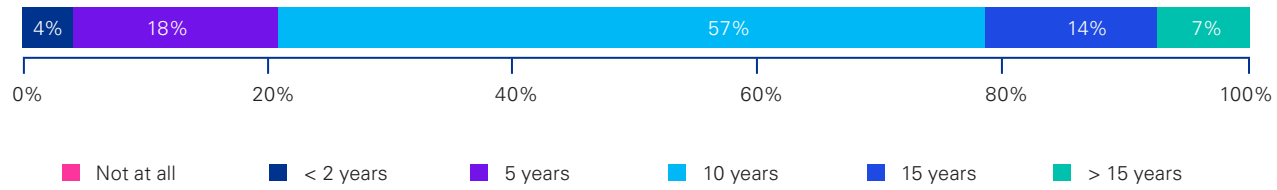


Source: BSI paper (co-author): "Kryptografie quantensicher gestalten - Grundlagen, Entwicklungen, Empfehlungen"BSI,October2021; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?

The purpose of the following questions was to estimate the x, y and z values according to Mosca's theorem (see box). The estimate for z is based on the responses to the question "When do you expect quantum computers to be capable of breaking relevant cryptographic techniques that are in use today?". For x, the assessment is based on the responses to the question "What is the maximum length of time for which your organisation keeps information confidential?".

The migration time (y) is based on a combination of the expected start date ("When is your organisation planning to begin the transition to post-quantum cryptography?") and the duration of the migration ("How long do you expect your organisation to need for the above transition?").

Fig. 6: When do you estimate quantum computers will be able to break certain cryptographic mechanisms in use today?



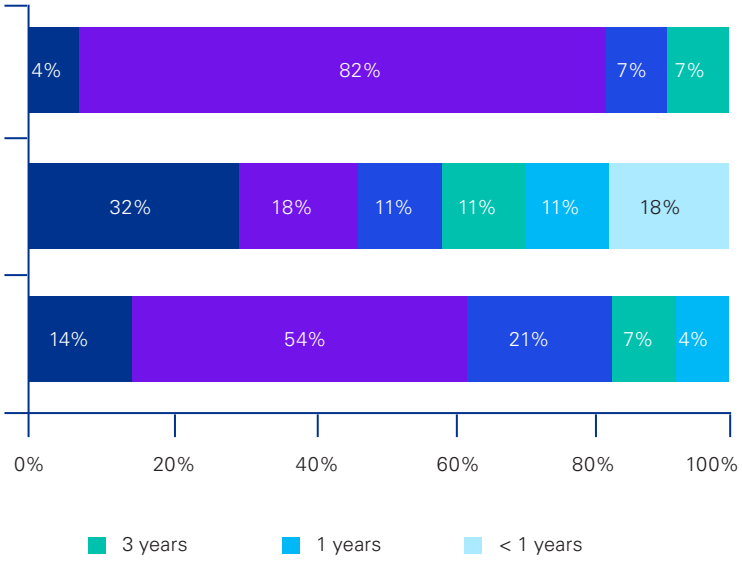
Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

Fig. 7: Please evaluate the following timescales

What is the maximum duration for which information must be kept confidential by your organizations?

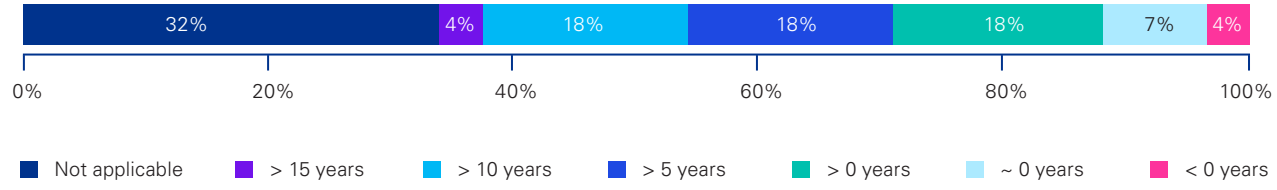
When does your organization plan to begin transitioning to quantum-resilient cryptography?

How long do you think it will take your organization to realize quantum resilience?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

Fig. 8: Estimated time by which the threshold for secure conversion to Post Qauntum cryptography is missed



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

The responses show that 79 % of the participating organisations expect it to take no more than ten years for quantum computers to be capable of breaking cryptographic techniques that are in use today – and all the organisations surveyed believe this will definitely happen at some point.

A large majority of the participants (89 %) are required to keep information confidential for a period of at least five years.

On average, this means the participating organisations expect to complete the migration to quantum-safe cryptography 6.5 years too late[2]. If confidential information can be read for many years, possibly while going unnoticed, this could have serious consequences.

Assessment

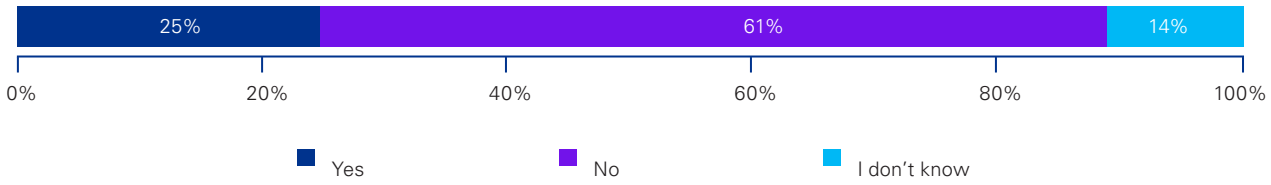
The question of when quantum computing will represent a real threat to public key cryptography is a matter of subjective judgement for the participants. When it comes to high-security areas, the German Federal Government and the BSI believe it is highly probable that cryptographically relevant quantum computers will be available by the early 2030s. This is not intended as a forecast, but as a working hypothesis for risk management purposes. This assessment of a period of approximately ten years is shared by the majority of the survey participants (57 %). Applying this figure as z for all of the participating organisations, the time by which they are expected to miss the deadline for secure migration to quantum-safe cryptography increases only slightly, to 7.16 years. However, applying this assumption means that quantum safety will not be achieved in time by **any** of the survey participants.

With regard to the responses concerning the probable start date, it is also notable that 32 % of the participants consider this question to be "not applicable/relevant" – even though only one organisation stated that it does not use any cryptographic techniques (see section 3.2). This is remarkable, since a response of "not applicable/relevant" suggests that the organisations in question do not consider there is any need for action in terms of migrating to post-quantum cryptography. As it is fairly improbable that they use only symmetric cryptography, however, these organisations are likely to be affected by the threat of quantum computing all the same

[2] This estimate is based on the assumption that the relational operators indicate a deviation of 50%, i.e. "< 1 year" is interpreted as 0.5 years and "> 5 years" as 7.5 years for the purposes of the calculation.

4.4 What measures are the organisations taking?

Fig. 9: Is the issue "threats of quantum computing to cryptography" considered in your organisation's risk management?



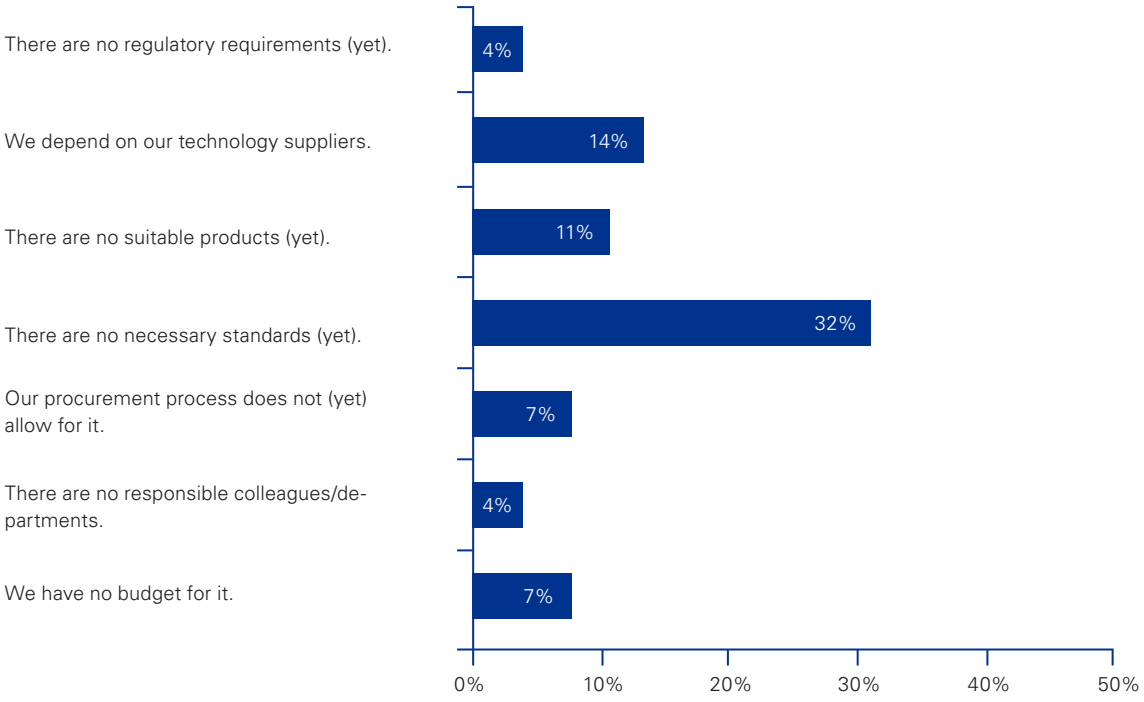
Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

Although the time-based forecasts are mostly negative (as described in section 3.3), the majority of organisations (61 %) say that the threat posed to cryptography by quantum computing is not ad-dressed in their risk management system. The continued absence of standards (32 %), dependence on technology suppliers (14 %) and the absence of products (11 %) are most commonly cited as the main reason for this. Interestingly, the responses that might seem the most obvious ("We do not have the corresponding budget" and "We do not have any employees/ departments with responsibility for this topic") are rarely given as the main reason for the lack of inclusion in the risk management system: the former was named by only two of the participating organisations, while the latter was cited by just one. This could serve as a further indication that the respondents come from a relatively homogeneous group of organisations that are already engaging with the risks of quantum computing for cryptography.

Relevance of risk management

For companies, risk management is a key tool that allows economic and technical risks to be identified at an early stage, measured, evaluated, documented and mitigated. This helps them to act pre-emptively to avoid losing revenue and incurring substantial costs. The necessary processes are established as part of strategic controlling so that the necessary facts and data can be collected and the required information delivered to the responsible decision-makers.

Fig. 10: If there are no initiatives/projects regarding this topic in your organization — why not?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

In order to establish the participants' current progress and potential plans in terms of migrating to post-quantum cryptography, they were asked about individual recommended actions from the BSI guidelines issued in late 2021, "Designing quantum-safe cryptography".

This found that crypto-agility is already well established, even though the participants said they were less familiar with the topic when asked about it in a different question (see section 4.1): More than one-third of the respondents stated that they are already taking care to ensure that cryptographic mechanisms are designed to be as flexible as possible, almost one-third are currently working on doing so, and half of the remaining companies at least intend to do so. The minimum length of 192 bits for symmetric keys also appears to be gaining acceptance. Furthermore, almost 50 % of the participants are already using or preparing to use hash-based signature schemes for software/firmware updates.

The situation is rather different when it comes to the recommendations on public key cryptography: Just 7 % of the participants are already using quantum-safe (hybrid) key agreement, although half of them are working on this or intend to do so. Only one respondent is migrating to quantum-safe digital certificates.

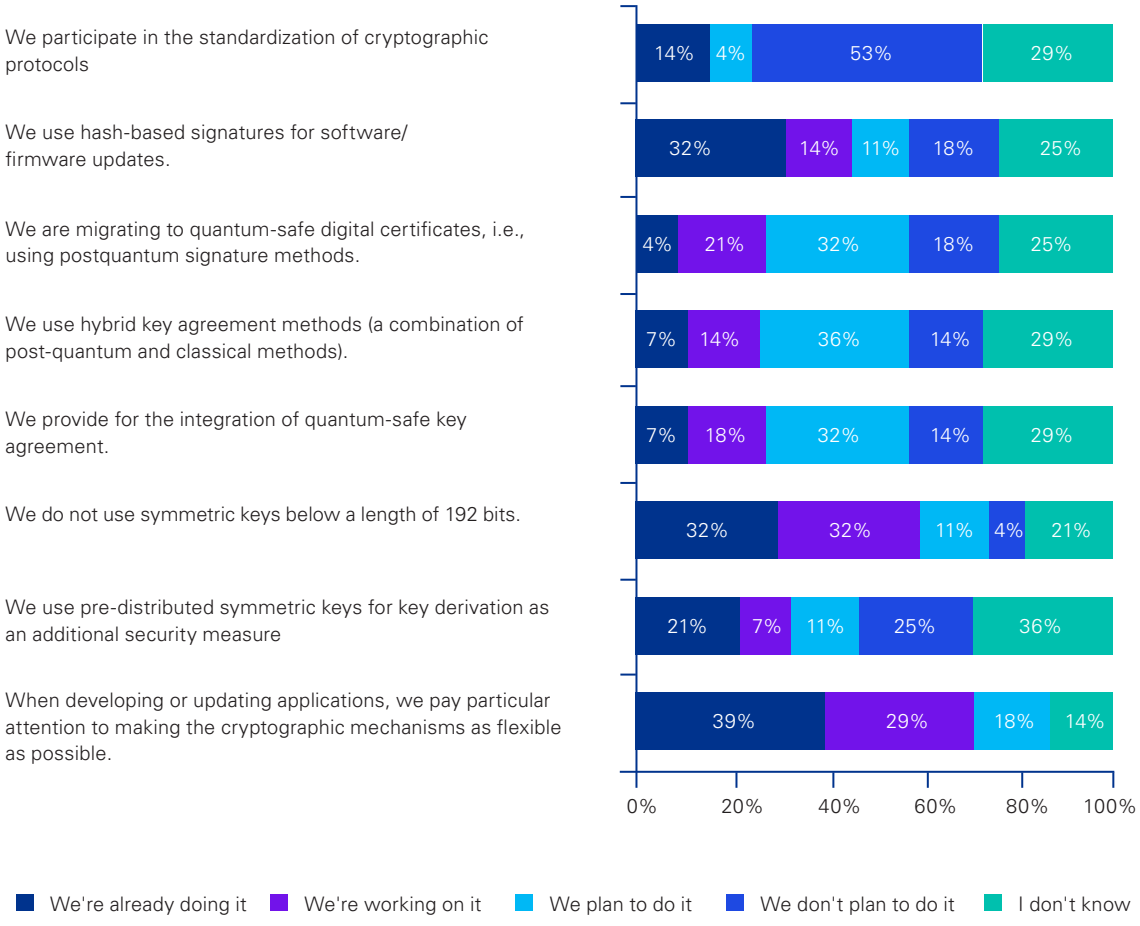
Additionally, most companies are not currently planning to participate in the standardisation of cryptographic techniques: More than half of the respondents said they were not involved in the corresponding processes.

Assessment

While it is true that there are currently almost no standards for post-quantum cryptography (with the exception of hash-based signature schemes), meaning that it has been implemented in very few products to date, it is already possible to prepare for and engage with the topic. Potential approaches for doing so are described in greater detail below.

Fig. 11: Recently, BSI published the guideline "Quantum-safe Cryptography – fundamentals current developments and recommendations". Among other things, it recommends the following actions for the migration to post-quantum cryptography.

Please rate the following statements:



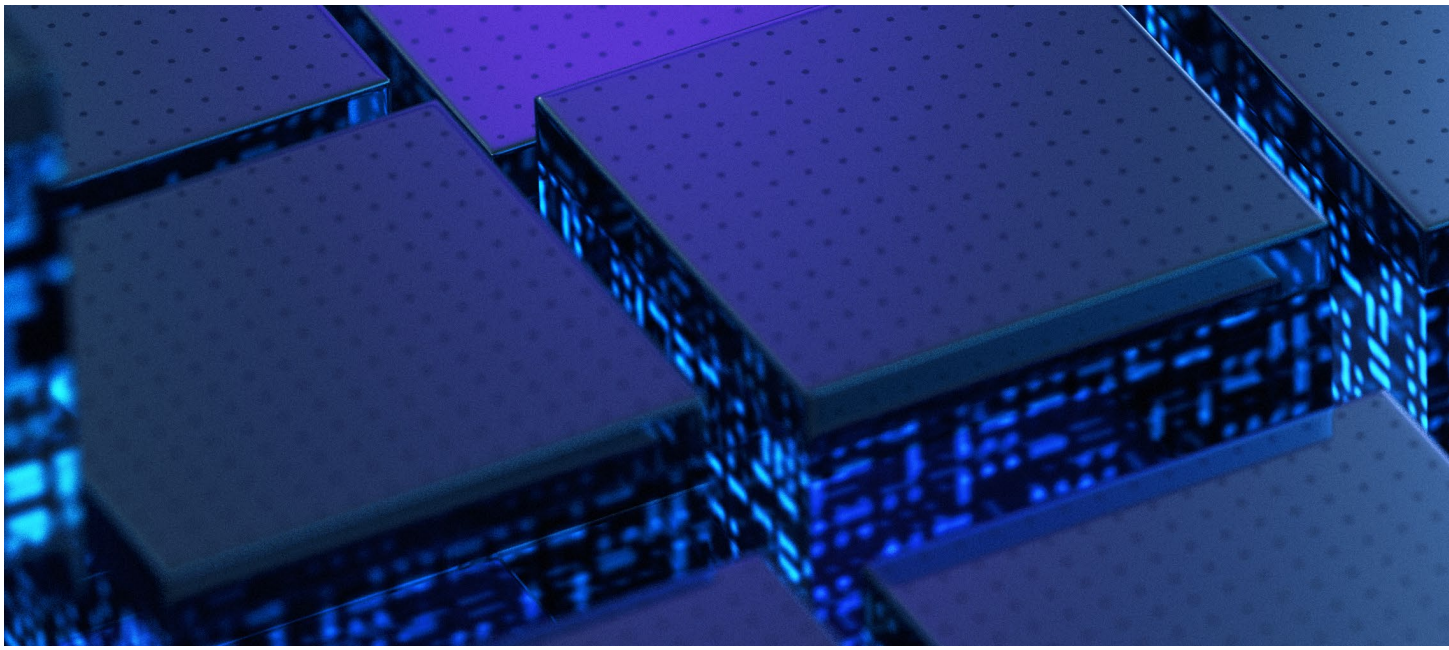
Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

Assessment

The results suggest that around half of the participating companies are aware of the steps required for migrating to post-quantum cryptography. With a few exceptions, however, they have yet to implement the actions recommended by the BSI.

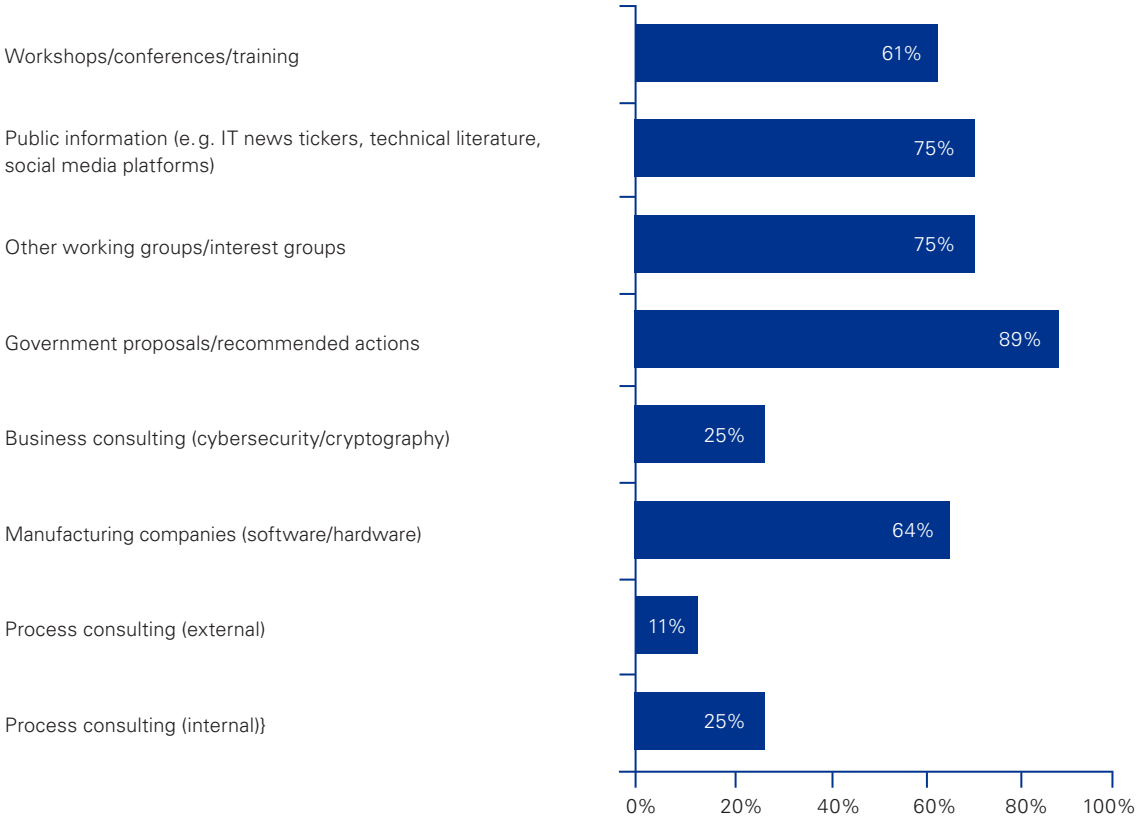
The BSI guidelines and the recommendations on quantum computing have met with considerable resonance. We have our finger on the pulse when it comes to this topic. Now we need to use the available time to advance the principles and applications and ensure that quantum-safe cryptography starts being used actively.

Dr. Günther Welsch
Head of Crypto Technology and IT Management, BSI



4.5 What support do the companies require for the next steps?

Fig. 12: What support do you use/plan to use?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

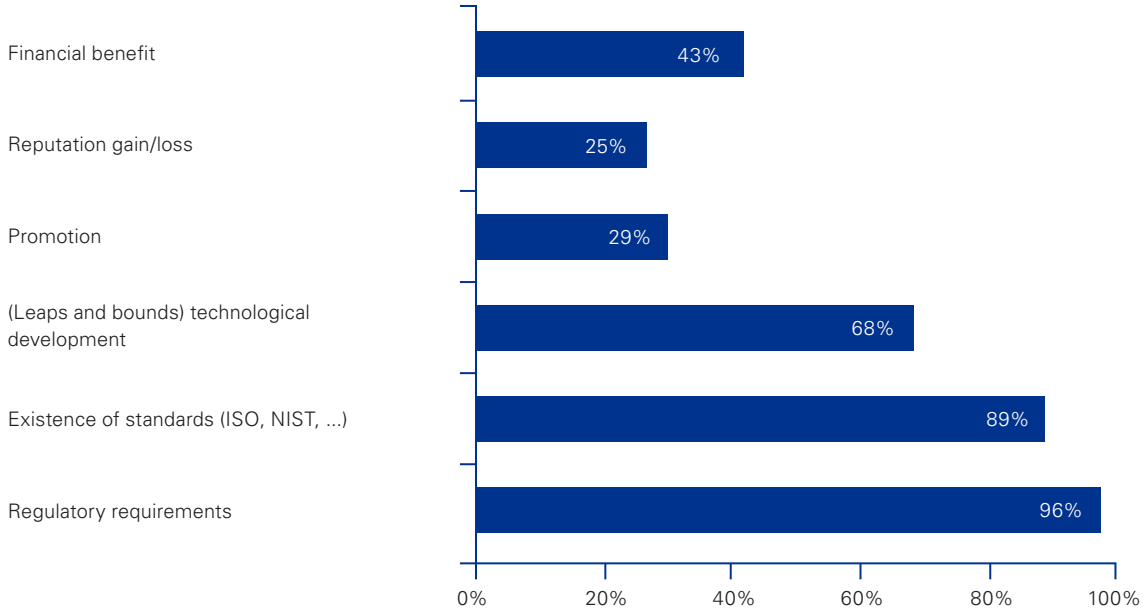
The results above suggest that there is still some work to be done before the transition to post-quantum cryptography can be completed successfully. When asked about the support they use or are planning to use, the majority of respondents (89 %) cited regulatory recommendations for action. At 75 %, other working groups and interest groups were mentioned by the same number of participants as public information (e.g. IT news tickers, specialist literature and social media).

Hardware/software manufacturers and visits to conferences, workshops and training were cited by 64 % and 61 % of respondents respectively.
At 79 % for their own products and 93 % for their own processes, most of the participants believe that responsibility for addressing the risk to cryptography resulting from quantum computing lies with them.

Assessment

The fact that the participants are mainly interested in support that they can implement themselves is consistent. This leads to the conclusion that the role of awareness campaigns and publicly available information should not be underestimated when it comes to the broad-based transition to quantum-safe cryptography. Public channels should seek to empower the responsible officers to achieve quantum safety within their organisations. Publicly available and comprehensible guidelines and best practice recommendations could be an effective tool for advancing this process. The relatively low degree of familiarity with "store now, decrypt later" and the concept of crypto-agility (see above) suggest that this is already relevant now.

Fig. 13: What would encourage your organisation to make investment decisions?



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

In order to narrow down what the organisations need in order to make their cryptographic systems quantum-safe, the participants were asked which aspects they believe would encourage investment decisions. Two responses were especially popular: Regulatory requirements were cited by 96 % of the participants, while 89 % named the existence of standards (ISO, NIST...). Meanwhile, rapid technological development was cited by 68 % of respondents. Traditional motivators like financial benefit, reputation and financial support were mentioned by fewer participants (43 %, 29 % and 25 % respectively).

This is consistent with the fact that fulfilling regulatory and data protection requirements was cited as one of the most frequent uses of cryptography, while 32 % of participants stated that the absence of standards was the main reason for the lack of initiatives within their organisation.

This would also appear to correlate with the fact that budget and staff were rarely named as reasons for the lack of initiatives (i. e. by just one and two of the participating organisations respectively) and the fact that financial support is of limited appeal in this context.

Assessment

The relatively rare mention of traditional economic factors can be seen as an indicator that there is no shortage of motivation to meet the challenges arising from quantum computing. This is reflected in the high degree of relevance attributed to the topic by the participants. However, this could also correlate with the conjecture that the respondents belong to a homogeneous group with a general prior interest in the subject matter.

The good news is that progress is being made with the standardisation of post-quantum cryptography. NIST made an initial decision on future standards in July 2022 and will publish its initial drafts in the near future. Other organisations are expected to apply these standards and follow suit. The BSI already recommended the first quantum-safe techniques for key agreement in spring 2020. At the BSI's instigation, the ISO/IEC SC27 WG2 recently launched a preliminary work item for the "Inclusion of key encapsulation mechanisms for PQC in ISO/IEC standards" project and called for expert contributions. This project could result in ISO standards for FrodoKEM and Classic McEliece. However, our participants would also like regulatory authorities to consider the quantum safety of cryptographic solutions.

The results of this survey show that very few people have engaged with our topic so far – but among those who have, the threat posed to cryptography by quantum computing is being taken extremely seriously. As such, I can only draw one conclusion: We need more well-informed people. And this urgently needs to include the responsible decision-makers.

Dr. Frank Damm
KPMG Germany,
Senior Manager

5. Summary, recommended actions and outlook

Timeframes

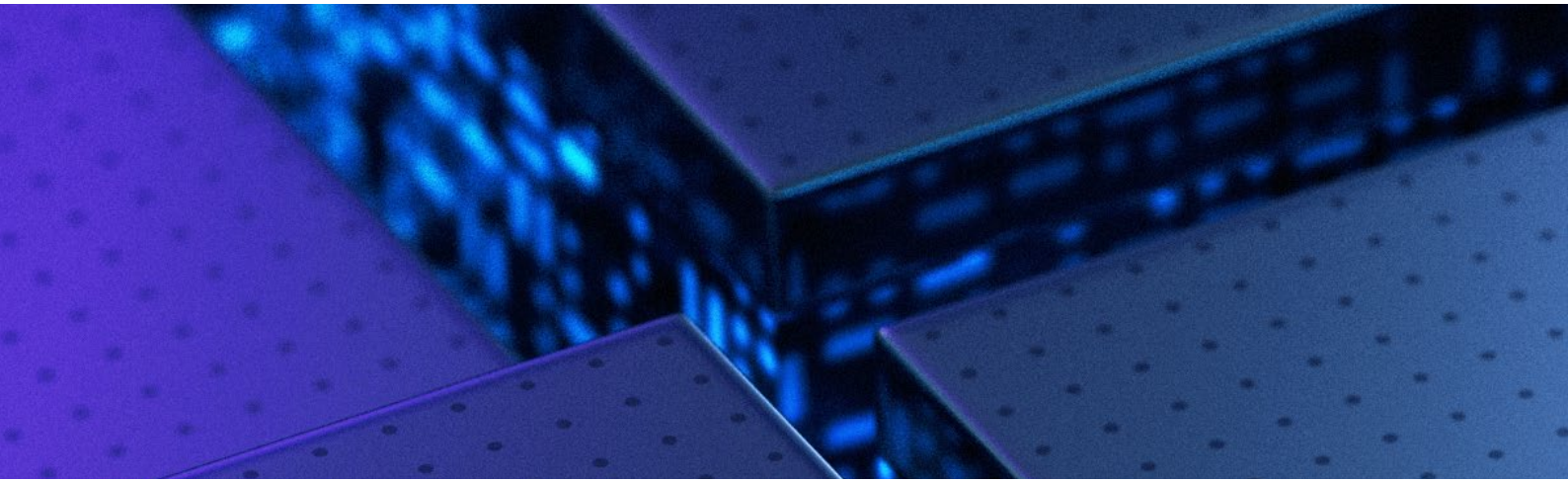
The BSI has been warning about the threat to public key cryptography from quantum computing for a number of years and has already initiated the migration to more quantum-safe solutions for high-security areas. The high-security government sector is applying the working hypothesis that crypto-graphically relevant quantum computers will be available by the early 2030s[3]. This is not intended as a forecast of the availability of quantum computers, but as a point of reference for risk assessment purposes.

This corresponds to the opinion of the participants. On average, they expect quantum computers to be capable of breaking the cryptographic techniques that are currently in use in 10.4 years. Based on their own assessment – as described in section 3.3 – their own migration to quantum-safe cryptography would therefore be completed 6.5 years too late. Applying Mosca's theorem[4], this means only 11 % of the participants believe there is a possibility that they will be quantum-safe before the confidentiality of their data is breached.

Almost 90 % of participants expect to be unable to counter the threat posed to cryptography by the emergence of quantum computing. In other words, there is a severe need for action in order to prevent data confidentiality from being significantly compromised.

97 % of respondents rated the general relevance of quantum computing for the security of today's cryptographic techniques as "high" or "quite high", while the figure for the average risk to data security within their own organisation was 65 %.

[3] https://dserver.bundestag.de/btd/19/252/1925208.pdf
[4] https://eprint.iacr.org/2015/1075.pdf, retrieved 20.03.2023



Treatment

Despite this, the threat of quantum computing is included in the risk management system of only 25 % of the participating organisations. Additionally, 32 % of participants considered the question of when their organisation is planning to begin the transition to be "not applicable/relevant". This implies that a transition is not even planned in these cases.

Asked about the factors that would encourage investment decisions in favour of more quantum-safe cryptography, 96 % of the respondents cited regulatory requirements and 89 % mentioned the existence of standards.

Although the necessary standards do not yet exist, organisations can already begin planning and implementing the transition of the cryptography they use. Leaving aside the time that is expected to be required until the transition begins, 32 % of participants would expect to achieve quantum resilience in good time.

In addition, measures to reduce the time required for the transition could already be taken now.

One example is the creation and maintenance of a crypto inventory, i. e. a detailed list of the cryptographic techniques used within an organisation and where. This would make it fairly straightforward for the threat to be taken into account in risk management. Additional measures to support such efforts can be found in the BSI guideline "Designing quantum-safe cryptography – basics, developments, recommendations". Some of the suggestions mentioned in the guideline, such as crypto-agility and the use of hash-based signature schemes, have already achieved a relatively high degree of penetration according to this survey. However, the participants' responses show that what they have achieved so far is not enough.

Furthermore, it is already possible to take precautions in order to circumvent the fact that quantum safety will not be achieved in good time. Here, too, corresponding risk management would be helpful when it comes to developing the necessary contingency plans.

Awareness

With 28 respondents, the response rate was considerably lower than for a comparable study on vulnerability management, for example. However, those who did participate in the survey already appear to have some knowledge of quantum computing and cryptography. 71 % of the participants share the prevailing expert opinion when it comes to the expected impact of sufficiently powerful quantum computers. On average, the respondents stated that they were "quite familiar" with the surveyed aspects of the subject field.

Taken together, these aspects suggest that the participants belong to a group of people with a prior interest in quantum computing and cryptography who view the security consequences of sufficiently powerful quantum computers as dramatic. This is consistent with the finding that the participants' risk assessment correlates to their familiarity with the material.

This indicates that the role of awareness should not be underestimated when it comes to ensuring the long-term confidentiality and integrity of sensitive data, from communicating an appropriate degree of risk awareness and the confidentiality requirements for certain data types through to techniques for dealing with risks. The management also needs to be trained and must have the necessary risk awareness. Ultimately, the call for regulation in this context can be satisfied only if political decisions are taken in the awareness of the emerging threat.

Political guidelines required?

Political guidelines on quantum security have already been adopted in the US. In January 2022, the White House published a memorandum requiring the ministries and security agencies to identify all non-quantum-safe cryptography techniques in National Security Systems (NSS) and draw up a migration timeline[5] within 180 days. The aim is for the migration to quantum-safe cryptography in the US to be substantially complete by 2035.

In Germany and Europe, current activities in the field of quantum technology are primarily focused on the development of quantum computers and keeping pace with the leading nations when it comes to quantum communication. However, the threat posed to cryptography by quantum computing is also being taken increasingly seriously by the German government. In its cybersecurity agenda, the German Federal Ministry of the Interior (BMI) defined investments in post-quantum cryptography as one of the measures to be taken in the 20th legislative period[6].

It remains to be seen what additional technical, scientific and political developments we will encounter in this field. However, one thing is clear: post-quantum cryptography will become the rule sooner or later. As such, it is advisable to begin the migration process in good time – or be prepared to address the consequences.

If I could give companies and organisations three pieces of advice as they prepare for quantum safety, they would be:

- **Include the threat in your risk management system**
- **Create a crypto inventory**
- **Implement and use crypto-agility**

Dr. Gerhard Schabhüser
Vice President, BSI

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[6] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4, retrieved 20.03.2023

Contact

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Federal Office for Information Security
Postfach 200363
53133 Bonn
T +49 228 99 9582-0
bsi@bsi.bund.de

Hans-Peter Fischer
Partner
T +49 69 9587-2404
hpfischer@kpmg.com

Dr. Heike Hagemeier
Referat TK 21 – Technology- and research strategy
T +49 228 99 9582-5968
heike.hagemeier@bsi.bund.de

Dr. Frank Damm
Senior Manager
T +49 221 2073-5728
fdamm@kpmg.com

Dr. Manfred Lochter
Referat KM 21 – Specifications for and development of crypto methods
T +49 228 99 9582-5643
manfred.lochter@bsi.bund.de

www.kpmg.de

www.kpmg.de/socialmedia

www.bsi.bund.de

https://bsi.bund.de/dok/520160