STATE OF PQC READINESS

ARE BUSINESSES PREPARED FOR Q-DAY?

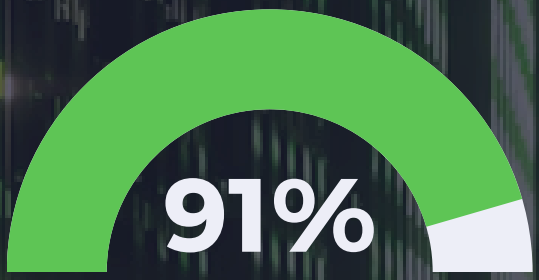
TRUSTED® COMPUTING GROUP

TRUSTED® COMPUTING GROUP

STATE OF PQC READINESS

The State of PQC Readiness report surveyed 1500 leading cybersecurity professionals across the USA and Europe earlier this year, providing a comprehensive perspective on their understanding of, preparations for, and concerns regarding post quantum cryptography.

KEY INSIGHTS



91%

of survey respondents currently do **not** have a formal PQC roadmap in place



Over 8 out of 10

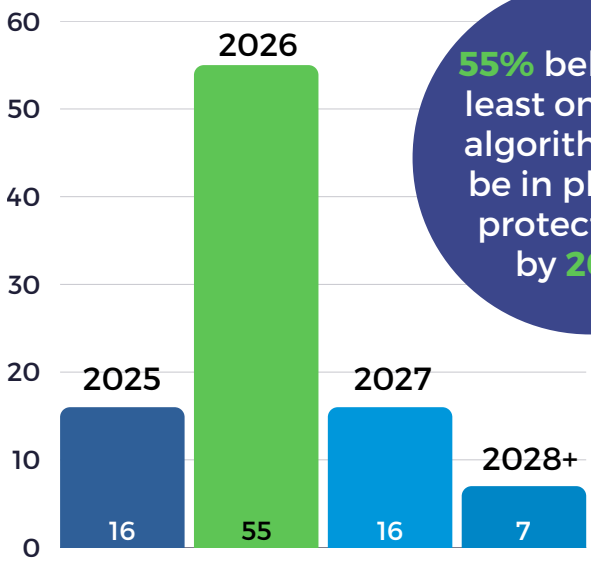
believe their current crypto-libraries and HSMs are **not ready** for PQC integration



Key adoption drivers include contractual requirements, industry consortium standards and new regulations



Key concerns include integration and compatibility, cost and budget restraints, and migration complexity



55% believe at least one PQC algorithm will be in place to protect data by **2026**

76%

are **confident** in their understanding of quantum computing's threat to existing cryptographic systems

39%

have already began undertaking **compliance readiness assessments** for PQC migration



CTOs, CIOs and CISOs are the main champions of PQC initiatives



58 percent of businesses plan to utilize **6-10%** of their available IT and security budgets to PQC migration efforts



FOREWORD

The time for PQC readiness is upon us. We're fast approaching the day when a quantum device capable of breaking most of today's widely-used forms of encryption methods becomes a reality, and this will have significant implications on any sector storing sensitive data.

Many experts now predict this day to arrive between 2030 to 2035, meaning the race is on to remain protected. So just how confident are security professionals in their migration efforts? What are the factors driving PQC readiness? And what is keeping the industry awake at night when it comes to this emerging quantum threat?

As organisations like NIST and the NCSC continue to approve PQC standards and set-out their roadmaps for full migration, the Trusted Computing Group offers this report to assess the current state of readiness across key sectors. Reflecting the insight from 1500 security professionals surveyed by Censuswide on behalf of TCG, our findings provide a clearer picture on the long-term security of businesses and the data pivotal to their operations.

Despite publicly declared worries from both within the sector and at Government level that quantum attacks will cause untold damage to businesses and critical infrastructure, 55% of professionals believe at least one PQC algorithm will be in place to protect them within the next year. At best, this is optimistic, and the fact that 90% of businesses do not have a clear roadmap for migration should be seen as a major cause for concern. 81% of professionals also feel their crypto-libraries and HSMs are not ready for PQC integration, indicating the work still required to become truly prepared.

However, the view that industry consortium standards will be crucial to these efforts is both noteworthy and promising. The Trusted Computing Group is working hard to update our specifications in preparation for the post-quantum era, aligning with the algorithms and parameter sets published by NIST and other institutions. Our foresight in this area was demonstrated through the algorithmic agility implemented during the transition to TPM 2.0 with its initial publication in 2013.

Industry migration to PQC will take some time, and the concerns raised over budgetary constraints are well-founded, but standards will play a key role in overcoming challenges surrounding integration complexities.

Overall, security professionals certainly seem to be confident in their understanding of quantum threats: references to 'harvest now, decrypt later' attacks indicate a knowledge of what's to come. However, it's difficult to look beyond the lack of roadmaps in place to mitigate these issues, compounded by fears over the available budget and expertise to implement them once they're developed. The sector's common prediction of having at least one PQC algorithm in place by the end of 2026 provides an interesting benchmark to measure – let's hope this confidence is proven correct within the next 12 months.

Joe Pennisi

Joe Pennisi
President
Trusted Computing Group

CONTENTS

05 **UNDERSTANDING THE QUANTUM THREAT**
Are businesses aware of the threat landscape?

06 **A QUANTUM OF SOLACE**
Are businesses jumping the gun on PQC readiness?

07 **QUANTUM THREAT, QUIET RESPONSE**
Only 1 in 10 businesses have a PQC plan in place

08 **VULNERABLE ASSETS**
Crypto-libraries and HSMs aren't ready for migration

09 **THE PQC DRIVERS WITHIN BUSINESSES**
The champions of crucial initiatives

10 **TAKING ACTION**
How proactive are businesses being?

11 **PRIORITIZING SYSTEMS**
The data businesses are securing first

12 **INVESTING IN PQC RESEARCH AND DEVELOPMENT**
How businesses will utilize already stretched budgets

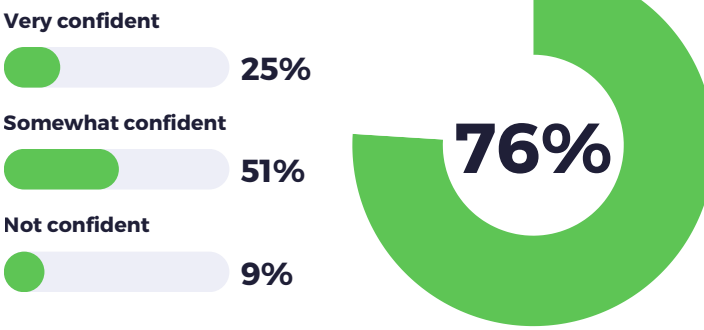
13 **ACCELERATING ADOPTION**
Computing standards in the top three drivers

14 **CAUSES FOR CONCERN**
What is keeping businesses awake at night?

UNDERSTANDING THE QUANTUM THREAT

Are businesses aware of the threat landscape?

When it comes to the threats we face from quantum computing, 76 percent of security professionals surveyed advised they were confident in their understanding of them.

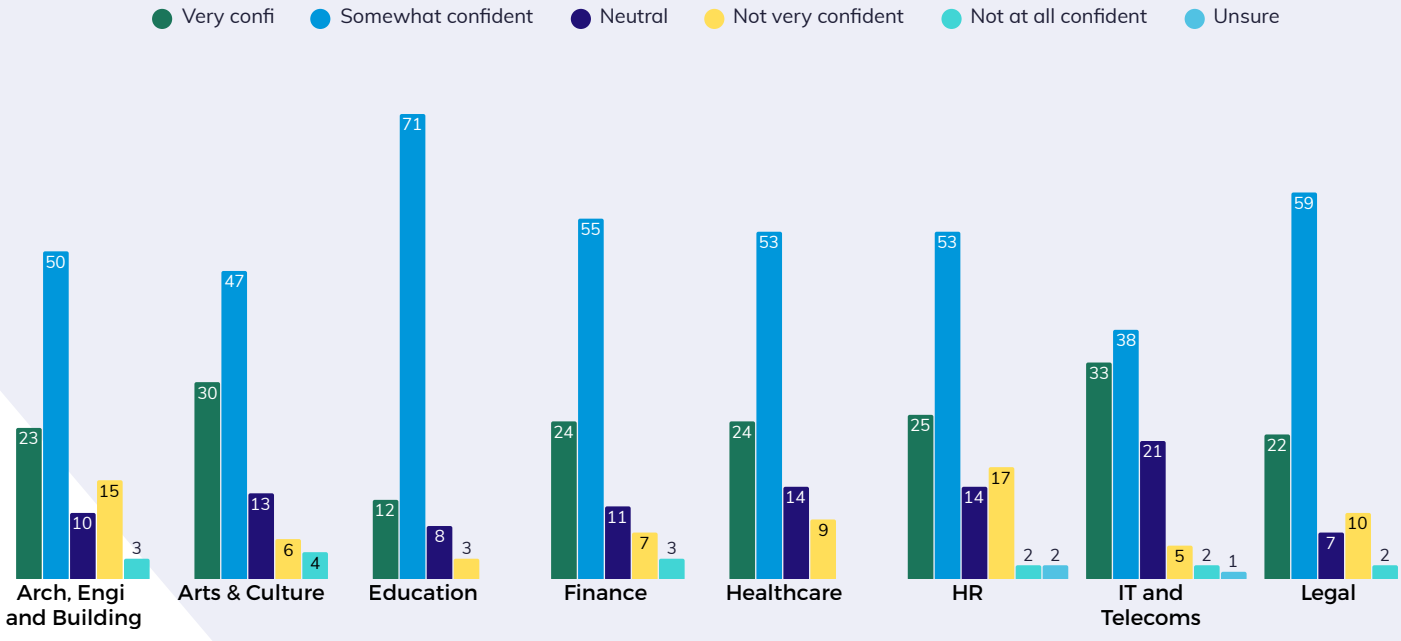


This confidence is more prominent in both the USA and the UK (83 and 82 percent, respectively). In Germany, this drops to 63 percent. Potential reasons for this include cybersecurity skills shortages within the country, and a slower regulatory response to quantum computing when compared to the governmental security agencies that are leading efforts in the USA and UK respectively.

The results also show a split in the attitudes between the different sectors we surveyed. As you would expect, those working in critical sectors which often come under threat from attacks demonstrate the highest understanding of quantum threats. This includes Education (82 percent), Legal (81 percent), and Healthcare (77 percent). Interestingly, professionals in IT and Telecoms only expressed a confidence level of 71 percent - however, this may be due to them having the greatest understanding of the complexities surrounding quantum attacks, and therefore the limitations of their knowledge in this field too.

UNDERSTANDING THE THREAT LANDSCAPE

How confident, if at all, are you in your understanding of quantum computing's threat to existing cryptographic systems?



In terms of the professionals feeling the least confident, these were mainly found in sectors that form part of the wider supply chain, and see less attacks. 18 percent of responses from both the Agriculture, Engineering and Building and HR sectors advised they were not confident in their understanding of quantum threats.

STATE OF PQC READINESS

A QUANTUM OF SOLACE

Are businesses jumping the gun on PQC readiness?

In response to being asked about their expectations regarding when PQC algorithms will be implemented within their operations, over half of respondents (55 percent) advised they believe at least one algorithm will be in place in 2026. This was true for all countries surveyed: 51 percent of professionals in the UK, 45 percent in the USA, and a staggering 70 percent in Germany.

This belief may be premature, and calls into question just how knowledgeable businesses are when it comes to quantum matters. In 2024, NIST published the first set of finalized PQC standards - for a key encapsulation mechanism (KEM) and digital signatures - but full use of PQC signatures is more challenging due to large signature sizes, compatibility and ecosystem readiness.

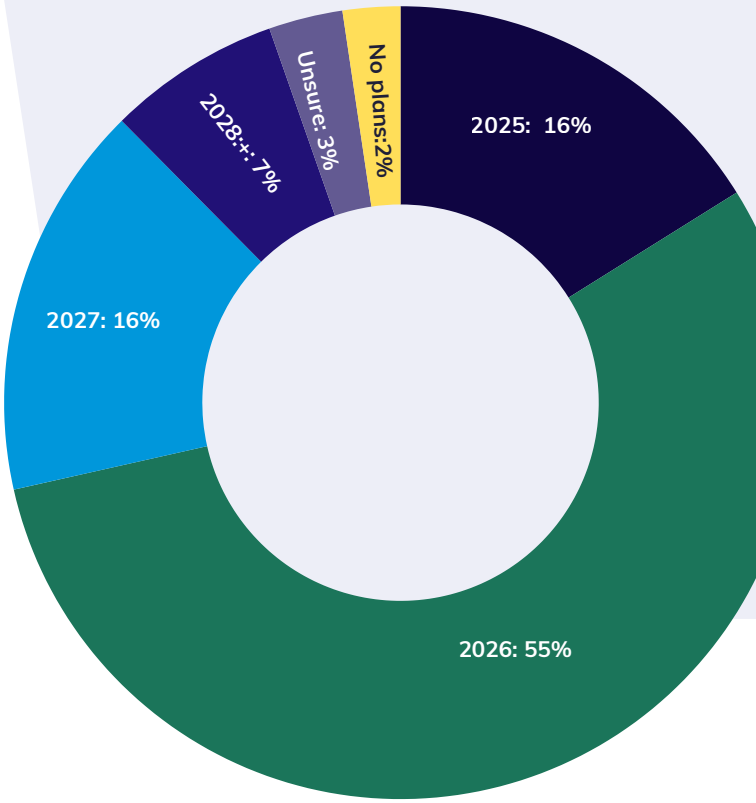
NIST even acknowledged in their *Transition to Post-Quantum Cryptography* roadmap that 'historically, the journey from algorithm standardization to full integration can take 10 to 20 years.'

We are already seeing businesses offer PQC-ready solutions, and while these are available, the issue is that the algorithms can not be fully integrated to cover *everything*. It's one thing implementing algorithms for smaller tasks like signing firmware, but a full migration process that protects all aspects of a organization's computing infrastructure is another matter entirely.

The vast majority of businesses will need to complete a full replacement of their PKI as part of the transition, so 2026 appears too soon a timeframe for implementation.

PQC ALGORITHM IMPLEMENTATION

By what year do you expect to have at least one PQC algorithm protecting production data, if at all?



When analyzing the survey results, it's clear the UK and USA are more cautious with their expectations: 27 percent of UK respondents believe the first algorithm will be implemented after 2026, with the USA respondents advising 28 percent. For those in Germany, this number plummets to just 16 percent.



The European Commission has advised the transition to PQC algorithms should be completed for medium and low risk systems by 31 December 2035 (*PQC Implementation Roadmap*, published June 2025). Within the USA, the government outlined the goal of 'mitigating as much of the quantum risk as is feasible by 2035' in the *National Security Memorandum 10 (NSM-10)*. This date was also specified in the recent *Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead* whitepaper published by Cornell University. The USA government was cited as estimating a 2035 deadline for non-National Security Systems.

STATE OF PQC READINESS

QUANTUM THREATS, QUIET RESPONSE

Only 1 in 10 businesses have a PQC plan in place

*How many businesses do **not** have a formal PQC roadmap in place?*



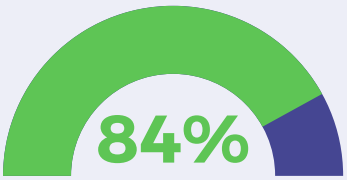
UK responses



USA responses



Germany responses



IT and Telecoms responses



Finance responses



Healthcare responses

With many organizations such as NIST outlining their own roadmaps for PQC migration, we asked security professions whether they have their own roadmaps in place. The answers were surprising, and slightly concerning.

Despite 73 percent of respondents feeling confident in their knowledge of quantum threats, and 55 percent expressing the belief that one PQC algorithm will be in place by 2026, 91 percent of those surveyed advised there is no formal roadmap in place presently. Of the ones who do have some form of plan in place, 5 percent of these are only draft roadmaps.

However, many of the draft and formal roadmaps indicate businesses have been aware of the quantum threat for some time. Responses from the USA revealed the earliest draft proposal was established as early as January 2013. However, there was a surge of these draft roadmaps around the same time NIST were proposing and finalizing their PQC roadmaps (2023-2025), indicating widespread engagement with external PQC planning. We see the same trend in formal roadmaps, albeit these were put in place at a later date - December 2020 was the earliest established roadmap advised by our respondents.

The UK also saw a few early movers, with the earliest draft roadmap established in January 2020. The majority of activity in terms of draft roadmaps were delivered between 2024-2025, as PQC algorithms were finalized, and government and industry guidance from organizations like the NCSC were publicly announced.

Respondents in Germany were by far the latest to establish roadmaps. The first draft roadmap put forward by a respondent was in February 2023, with a heavy concentration around April 2024. Interestingly, this aligns with the European Commission's *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*, which was published on April 11, 2024. Designed to synchronize efforts across all EU Member States for effective quantum threat preparation. Germany, though its Federal Office for Information Security (BSI), was a key contributor to the roadmap, and this development appeared to have stirred greater movement when it comes to roadmaps across the German market.

In some cases, formalization of roadmaps began before many draft dates in Germany, which suggests businesses may have skipped a formal draft phase, or retroactively documented it. Regulatory pressure may be a key reason for this.

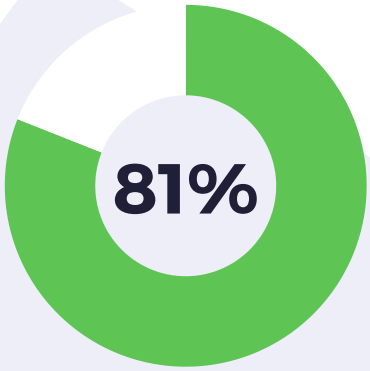
Unfortunately, the businesses with draft and formal roadmaps are the exception, not the norm. While the fact there have been early adopters suggests there is awareness of quantum threats, yet most businesses remain unprepared for them. Momentum may be building - a lot of plans were established between 2024 and 2025 - but this is only a small, proactive subset. Policy-driven spikes seen in Germany are promising, but while a few businesses are racing ahead, most are standing still. This gap could lead to significant vulnerabilities, especially if quantum-capable adversaries emerge before widespread PQC adoption.

VULNERABLE ASSETS

Crypto-libraries and HSMs aren't ready for migration

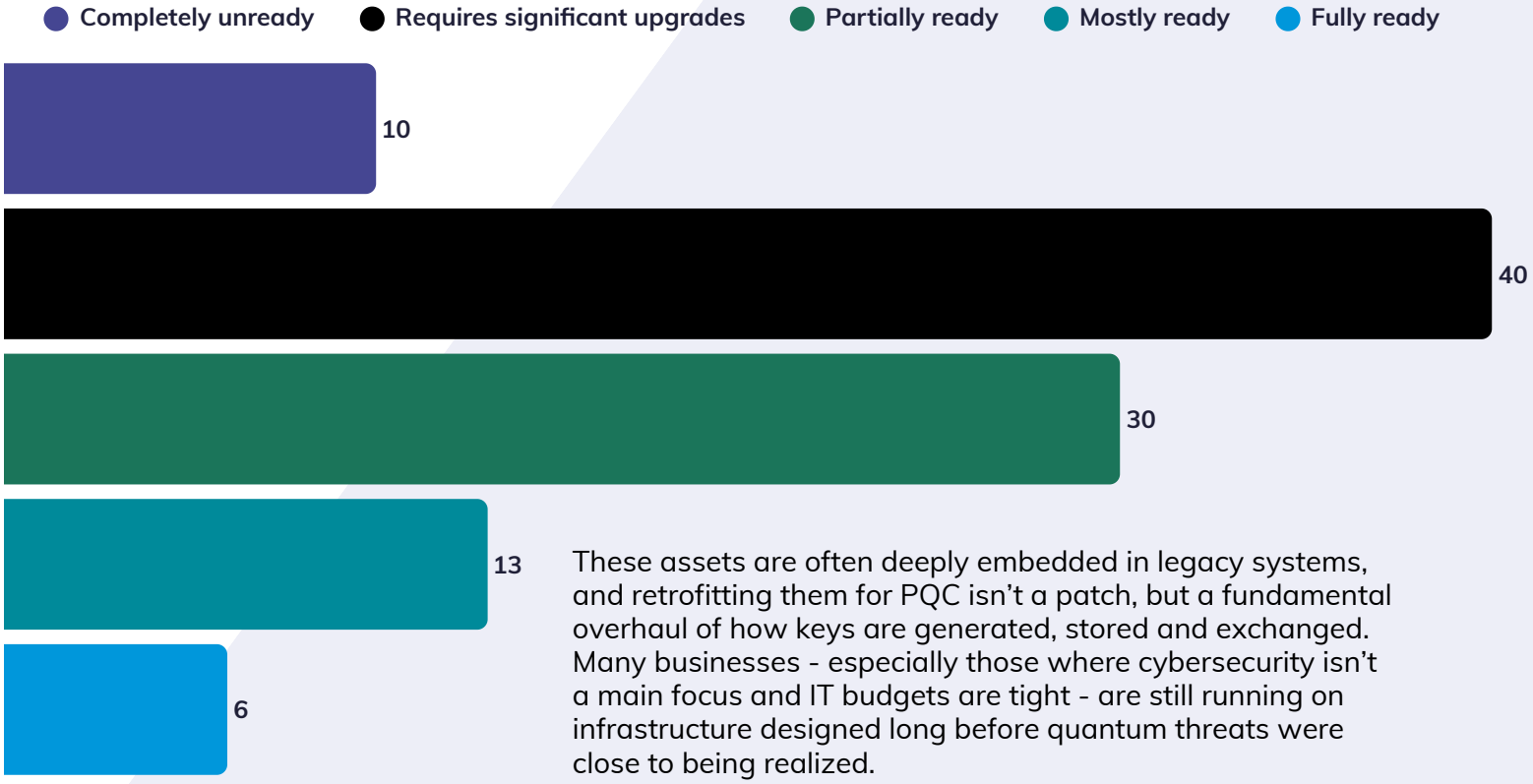
Compounding these issues is the fact the majority (81 percent of respondents) of businesses believe their assets are not ready for PQC migration.

Crypto-libraries and hardware security models are the backbone of secure communications and data protection. If these do not become PQC ready soon, organizations will quickly find themselves vulnerable to quantum attacks once Q-Day arrives. These results reflect the disconnect between awareness and action - our survey shows that businesses know PQC is coming, but have been slow to action changes.



ASSET READINESS

How ready, if at all, are your current crypto-libraries and HSMs for PQC integration?



These assets are often deeply embedded in legacy systems, and retrofitting them for PQC isn't a patch, but a fundamental overhaul of how keys are generated, stored and exchanged. Many businesses - especially those where cybersecurity isn't a main focus and IT budgets are tight - are still running on infrastructure designed long before quantum threats were close to being realized.

There's other dependencies that need to be considered too. There is an ongoing skills shortage within the cybersecurity sector - reports created by *IBM* and *(ISC)²* indicate a critical skills and talent shortfall of 4.8 million in 2025, and this gap is worsening. The truth is many IT and security teams lack the specialist knowledge required to assess readiness or plan migrations. Even among those aware of quantum risks, translating that knowledge into technical action is a challenge.

Most businesses are also heavily reliant on third-party vendors and standards bodies for their cryptographic tools. If these vendors haven't yet rolled out PQC-compatible updates, then internal teams are stuck waiting, creating a significant bottleneck for businesses looking to protect their assets.

STATE OF PQC READINESS

THE PQC DRIVERS WITHIN BUSINESSES

The champions of crucial initiatives

The roles of those championing PQC strategies are varied. However, Chief Technical Officers (CTOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and those holding relevant security leadership positions stand out as the main drivers for implementation, according to our respondents.

For the security professionals in Germany, 53 percent of all respondents emphatically named the CTO and CIO as the leading figure driving PQC initiatives within their businesses, followed by CISOs and those with security leadership positions (28 percent and 26 percent respectively).



The results from the UK and the USA were more evenly spread: in the UK, professionals see CISOs leading the charge at 39 percent, closely followed by risk and compliance teams at 38 percent. The respondents in the USA also named CISOs as the main driver within their businesses (40 percent), with the CTO coming in second (37 percent).

CTOs and CIOs are also the leading champions of PQC initiatives within the IT and Telecoms (53 percent), Healthcare (42 percent), and HR (35 percent) sectors, As these are the most likely targets for PQC attacks, it stands to reason that their CTOs and CIOs are 'in the know' regarding the threat landscape.

On the other hand, businesses within the Architecture, Engineering and Building, and Educations sectors are the most reliant on outside support, naming external consultants and advisors as their main drivers of PQC initiatives, with 50 percent and 38 percent respectively. Professionals within the legal space placed equal responsibility on their CIO and external advisers (36 percent).

The Architecture, Engineering and Building, Education and Legal sectors all see external consultants and advisers as the lead or co-lead driver of PQC initiatives.

TAKING ACTION

How proactive are businesses being?

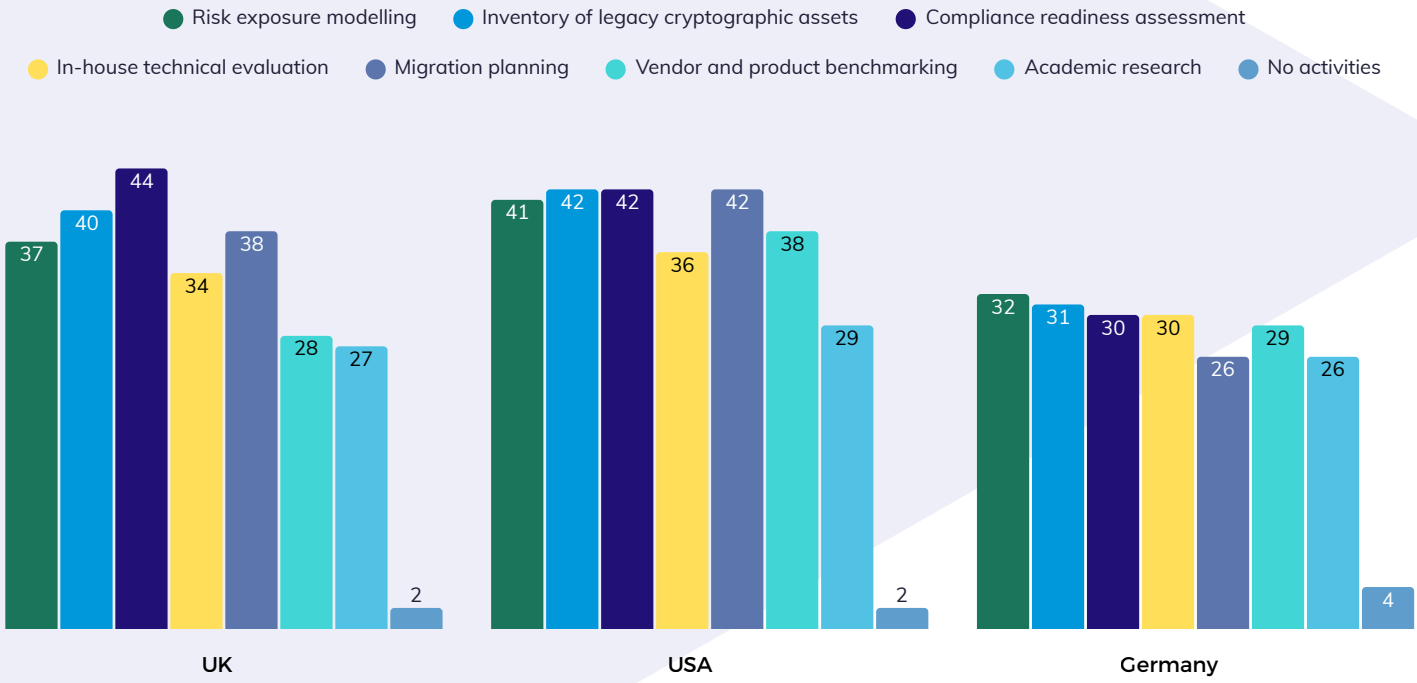
Because the majority of security professionals have some understanding of the quantum threat, companies across all sectors have started to action measures to stay ahead of attacks. Of all the steps a business or organization may take, compliance readiness assessments seems to be the priority for those surveyed (39 percent).

This action is closely followed by risk exposure modelling and the inventorying of legacy cryptographic assets (both at 37 percent). Despite concerns, this does appear to be one area businesses are being proactive in their approach to PQC activities, with only 2 percent of responses indicating no actions are underway at present.

Of the three countries surveyed, only Germany differed from the average, with the results highlighting risk exposure modelling (32 percent) as their main action. However said results also demonstrate a more even distribution across activities: unlike the UK and the US which are compliance-driven, German businesses appear to be exploring PQC activities through a more uniform approach. According to our findings, of the actions taken there is only a 8 percent gap between the top and bottom result - academic research at 26 percent. For the UK and USA, this gap sits at 17 percent and 13 percent respectively.

ONGOING ACTIVITIES

What activities related to PQC is your organization already undertaking, if any?



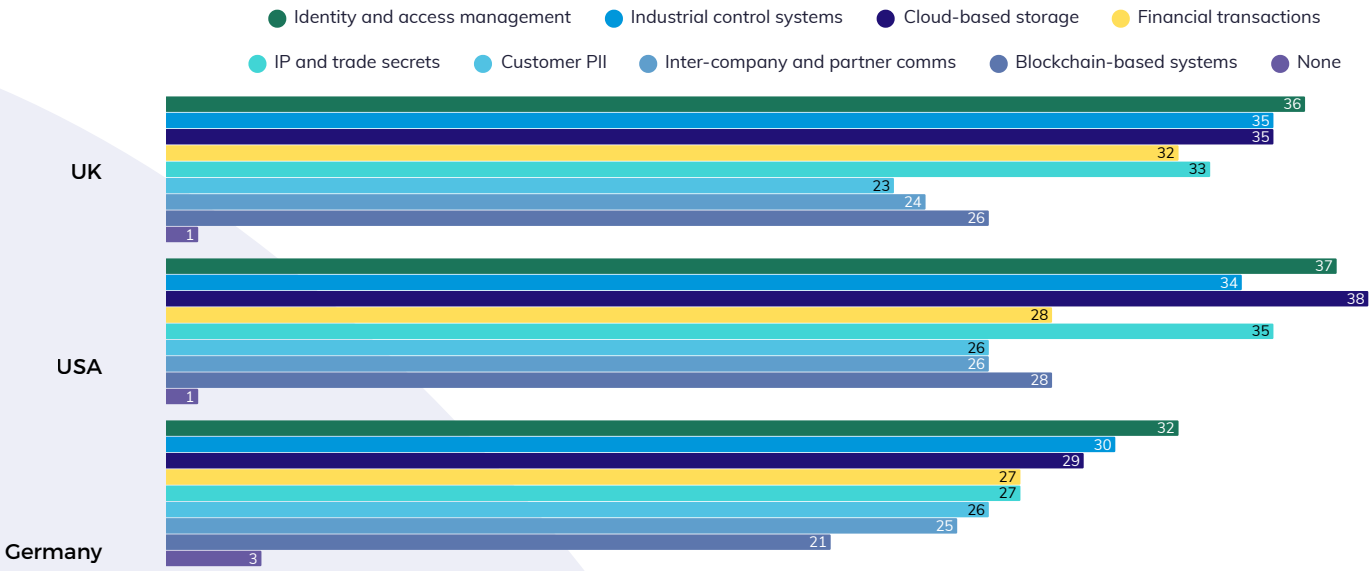
This may be because IT budgets in Germany often fall short of what's available to professionals in both the UK and USA, so a more measured approach to prioritization makes more sense fiscally.

The Legal sector was the only one to advise vendor and product benchmarking was the main activity being carried out regarding PQC

PRIORITIZING SYSTEMS

The data businesses are securing first

As quantum computing edges closer to practical viability, industries and government bodies are beginning to prioritize their sensitive data to reduce the risk of a breach, with Identity and Access Management (IAM) declared the main focus by respondents (35 percent).



This is because IAM systems are heavily reliant on public key cryptography, which are particularly vulnerable to quantum algorithms like Shor's, which may soon be able to break common encryption methods like RSA and EEC. Sectors including IT and Telecoms and Healthcare (36 percent) ranked this data element as the highest priority - unsurprising given their reliance on secure authentication and digital signatures to protect sensitive data. It should come as no surprise that NIST's PQC standardization attempts made IAM a focal point of early migration planning.

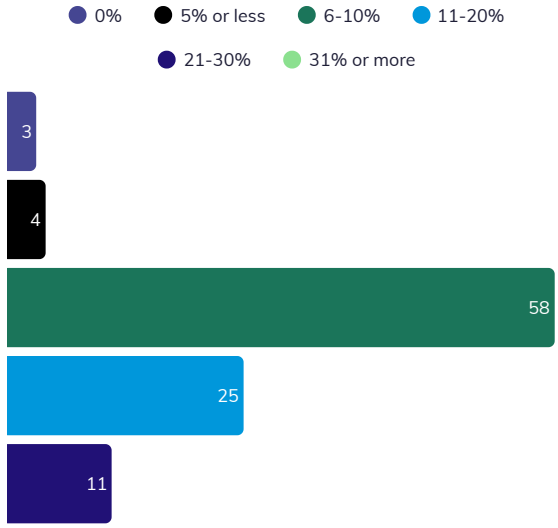
Industrial Control Systems (ICS) were the priority for professionals within Architecture, Engineering and Building (45 percent), alongside the Finance (41 percent), HR (37 percent) and Legal (43 percent) sectors. ICS often run on legacy infrastructure with lengthy lifecycles, making them difficult to patch. Ensuring there's enough time to prepare these for NIST's algorithms is crucial to the PQC migration process.

Protecting IP and trade secrets also scored particularly high in USA (35 percent) and UK (33 percent) responses. The main industry prioritizing this area was Arts and Culture at 36 percent, which revolves heavily around unique contracts, creative assets and proprietary methods. Long-term encrypted archived works such as creative works may be vulnerable to future decryption if not migrated.

Interestingly, the Education sector is the only to focus heavily on prioritizing Blockchain-based storage (40 percent). Academic records and credentials often need to preserved permanently, and Blockchain can offer tamper-evident, decentralized storage for this information. Blockchain-based diplomas and certificates are already been offered by universities such as MIT, but as these rely on public key cryptography, they too must be secured to avoid devastating quantum attacks.

INVESTING IN PQC RESEARCH AND DEVELOPMENT

How businesses will utilize already stretched budgets

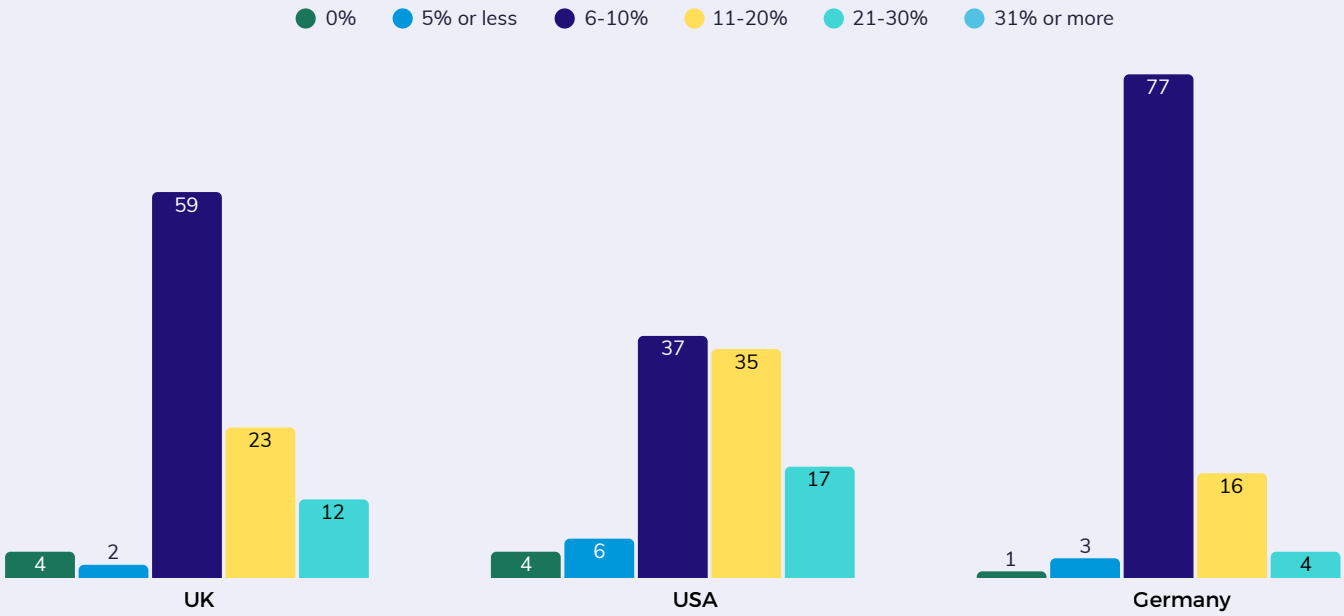


The majority of businesses surveyed (97 percent) plan to invest some of their available cybersecurity budget for PQC measures over the next 24 months, with 58 percent of respondents saying the value of this investment will fall between 6 to 10 percent.

While this figure may appear small, it is still a reasonable amount to put aside for PQC measures in an age where cybersecurity budgets continue to be squeezed. Despite a rise in cyber threats, economic uncertainties are leading organizations to prioritize other areas of their operations. In 2025, the average cybersecurity budget grew by only 4 percent, half the growth seen in 2024, according to *Digit News*.

INVESTMENT LEVELS

Over the next two years, how much of your cybersecurity budget will you allocate to PQC research, tooling or deployment?



Worryingly, 4 percent of those surveyed in the UK and USA will not look to utilize their available budgets for PQC measures, despite believing that at least one algorithm will be in place to protect systems by 2026. However, the USA is expected to lead the way in terms of the amount of budget being spent, with 52 percent of businesses confirming at least 11 percent of their budget will be used for research, tooling or deployment. As mentioned previously, companies and organizations within the USA typically have significantly larger security budgets than their UK and German counterparts, and the North American market continues to account for the highest share of global cybersecurity spending, so our results come as no surprise in this area.

STATE OF PQC READINESS

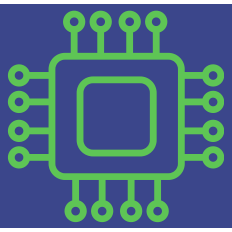
ACCELERATING ADOPTION

Computing standards in the top three drivers

When it comes to the factors capable of accelerating an organization's adoption of PQC measures, contractual requirements outlined by customers and partners are seen as the biggest (22 percent).

Security professionals in both the USA and Germany both saw this as the top driver for PQC adoption (24 percent and 21 percent respectively). In the UK, the main driver was identified as industry consortium standards, such as those developed by the Trusted Computing Group (TCG), followed by the threat of quantum-security incidents (21 percent) and new government regulations and mandates (20 percent). Interestingly, security incidents was the least popular answer given by those in the USA at only 15 percent.

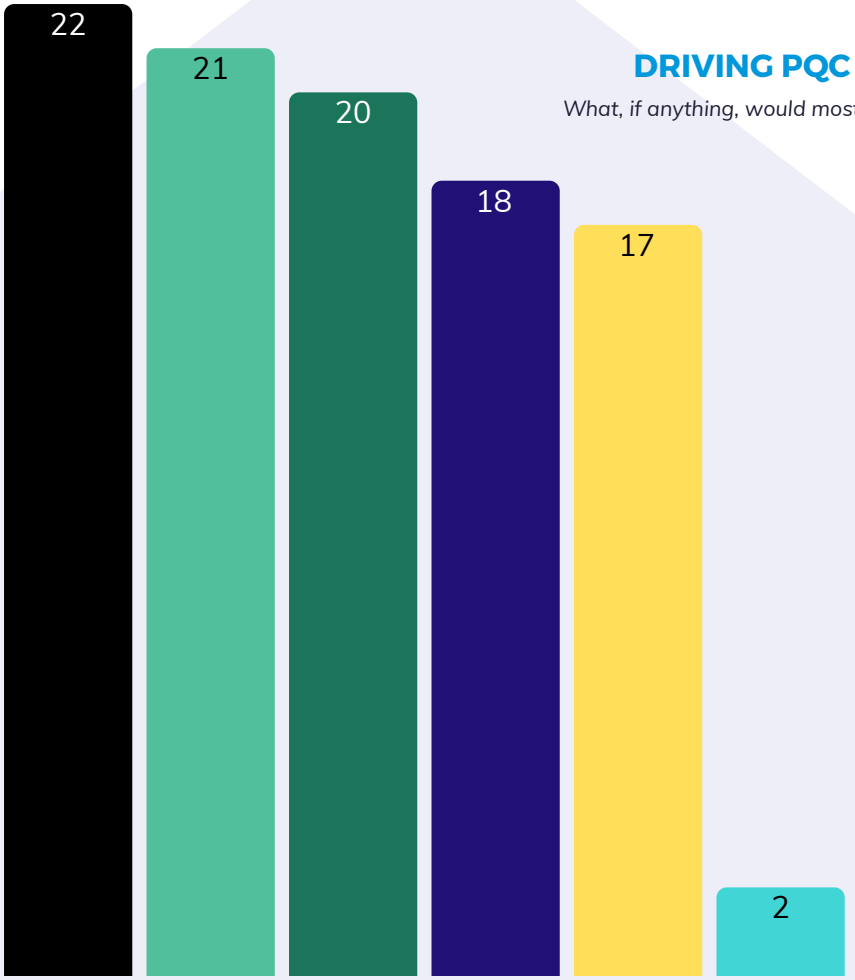
TCG's foresight in preparing for the post-quantum era of computing was evidenced through the algorithmic agility implemented during the transition to TPM 2.0, with its initial publication in 2013.



TPM 2.0

DRIVING PQC ADOPTION (BY PERCENTAGE)

What, if anything, would most accelerate your organization's adoption of PQC?



Contractual requirements were also the key drivers in the Arts and Culture (32 percent), Finance (24 percent), Healthcare (21 percent) and IT and Telecoms sectors (22 percent).

In terms of those led by government regulations and mandates, both the Architecture, Engineering and Building, and HR sectors were the only to advise this as the primary reason for adoption (40 percent and 23 percent respectively).

While only the Legal sector indicated standards as their main driver at 28 percent, this appeared in the top three of all but two sectors analyzed, indicating their importance in battling quantum threats.

CAUSES FOR CONCERN

What is keeping businesses awake at night?

153 of our respondents also provided insight into the main concerns over the current migration to PQC standards.

While the answers provided were varied, the three main concerns detailed by security professionals included integration and compatibility, security risks and exposure, and current cost and budgetary restraints. The complexity of migration processes and current training and talent shortages are also weighing heavily on the minds of our survey respondents.

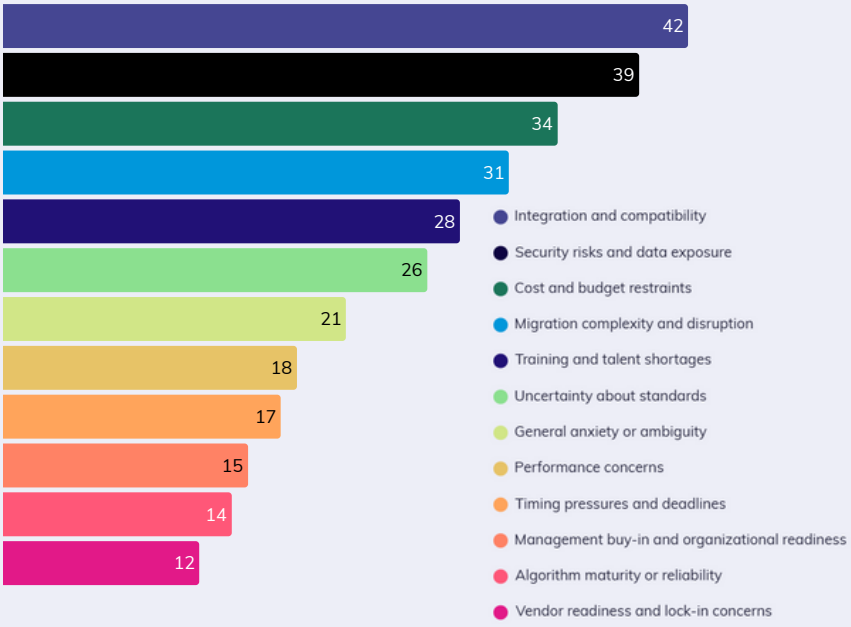
Integration and compatibility

Security risks and data exposure

Cost and budget restraints

THE CONCERNS OVER PQC MIGRATION

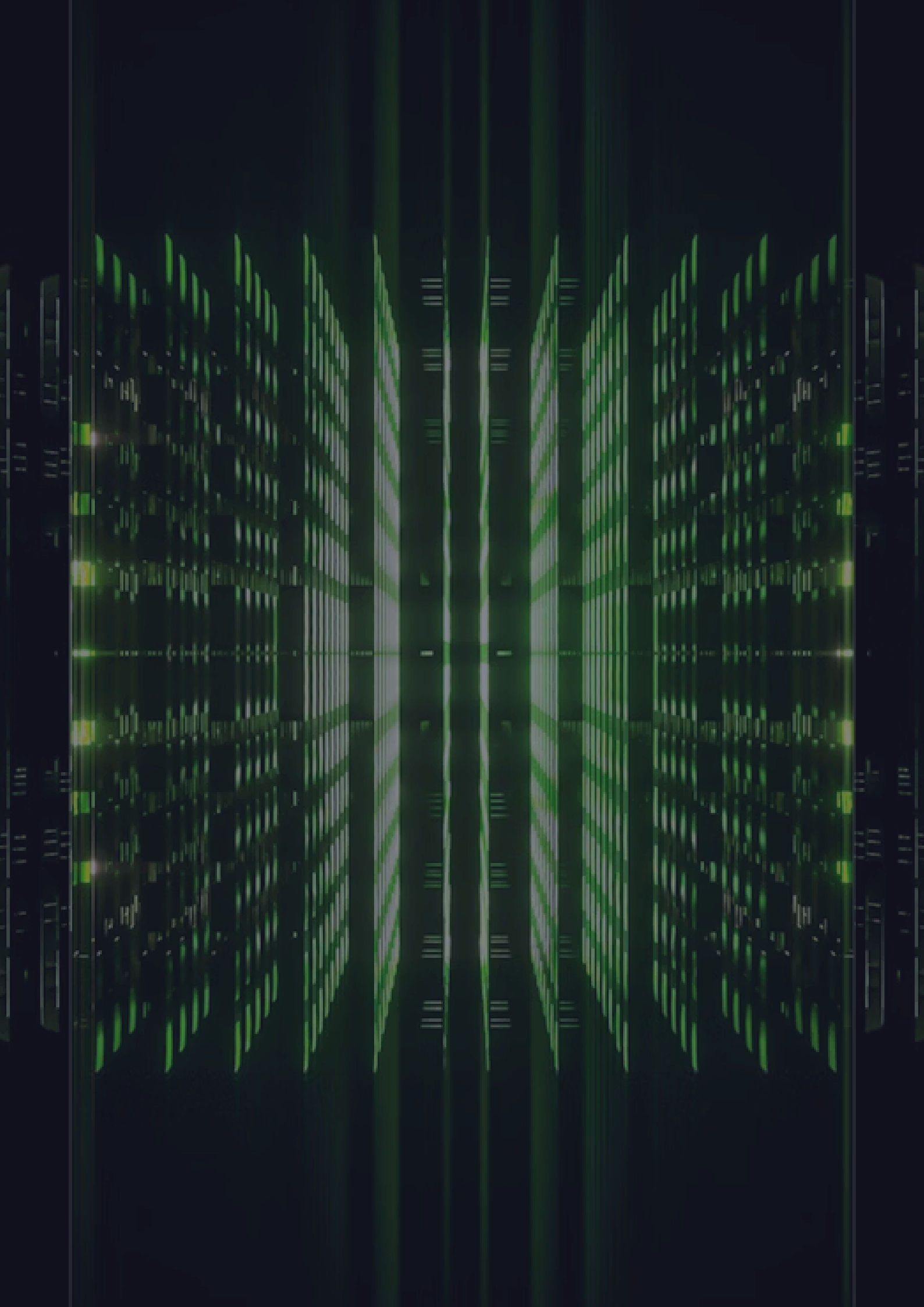
What, if anything, keeps you up at night when you think about moving to PQC?



The responses from the UK highlighted a heavy focus on cost, training and compatibility with legacy systems. Professionals also raised concerns over management buy-in and a lack of internal guidance, alongside a general anxiety over quantum threats.

In Germany, many voiced concerns over timeline pressures, migration complexity and a lack of talent available. Several responses allude to algorithm safety, while flagging issues surrounding multi-cloud co-ordination and critical asset identification.

Within the USA, we saw strong responses regarding integration complexity, alongside performance and standardization uncertainties. Many specifically referenced ‘harvest now, decrypt later’ attacks as a cause for concern, suggesting a higher level of understanding of quantum threats within the region. Broader concerns linked to job stability, family, and the impact PQC might have on their careers were also highlighted by security professionals within the country.



STATE OF PQC READINESS

TRUSTED® COMPUTING GROUP

ABOUT THE TRUSTED COMPUTING GROUP

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral and global industry specifications and standards which form the backbone of the theory of trusted computing.

Since creating the first Trusted Platform Module (TPM) specification, we have embedded the core concepts of trust into over a billion devices. The standards, specifications, guidance and software developed by the TCG are the building blocks enabling one component in a network to trust all the other pieces of hardware and software they are linked to.

Through the TCG, trusted computing has been established across key industries, including the finance, healthcare, industry and automotive sectors.

CONTACT US

Website
www.trustedcomputinggroup.org

LinkedIn
Trusted Computing Group

Email
admin@trustedcomputinggroup.org