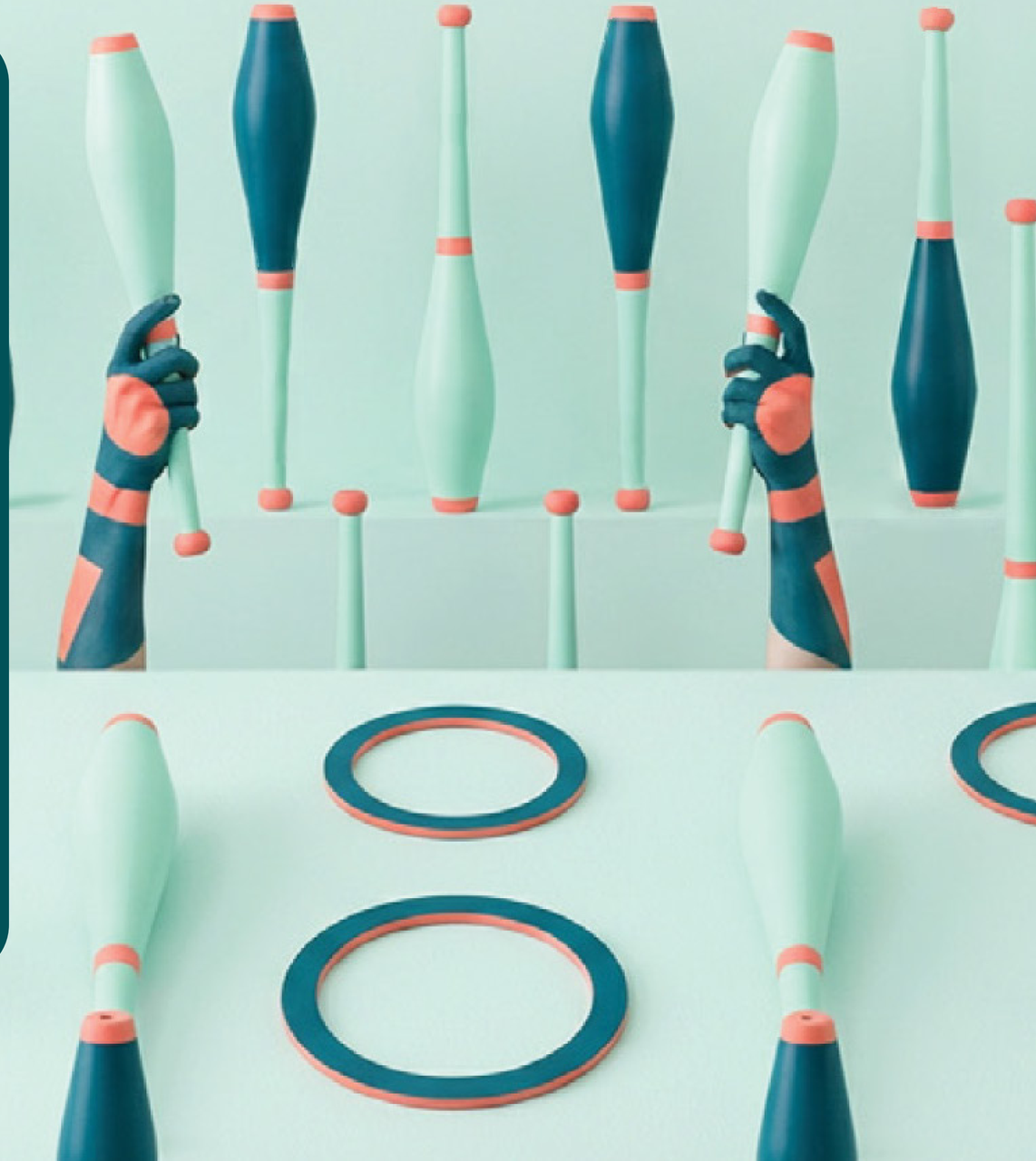
sectigo

The State of Crypto Agility

Data and insights reviewed by Omdia



Foreword from Tim Callan

Tim Callan
Chief Compliance Officer at Sectigo
Vice-Chair of the CA/Browser Forum
August, 2025

SSL/TLS public certificates and their underlying cryptography have been remarkably stable for 30 years. But that is changing.

Two mega trends are shaking up the world of PKI today. The radical shortening of certificate lifespans and the looming transition to post-quantum cryptography (PQC). These separate trends, though distinct, are intertwined in both their motivations and the transformations they demand from the digital ecosystem.

On April 11, 2025, the CA/Browser Forum approved a landmark decision to incrementally reduce the maximum allowed validity period for SSL/TLS public certificates from today's 398 days to just 47 days by 2029. This signals a new era of heightened security and operational agility. But with that comes a significant operational challenge: Enterprise IT teams will now need to update and manage certificates far more frequently or risk downtime and disruption.

For a long time, certificates have flown under the radar in most enterprise IT organizations. But overnight they have stepped into the spotlight.

SSL/TLS certificates are the foundation of digital trust. They enable encrypted communication by securely distributing public keys and verifying digital identities. Because most cryptographic operations are governed by certificates, certificate agility—which is the ability to quickly find, manage, and replace them—is essential . Historically, organizations have been able to get by with poor certificate hygiene because cryptography was largely static. But now, with a quantum era looming, that margin for error is disappearing.

And certificates are just the beginning.

The second disruptive trend is the approaching reality of quantum computing. Experts have long warned that once quantum machines reach sufficient power, they could break RSA and ECC, which between them encrypt most of our digital data. Although this “Q-day” is still years away, the threat is already here: Attackers are harvesting encrypted data today in hopes of decrypting it in the future.

The U.S. National Institute of Standards and Technology (NIST) is not waiting for Q-day and has proactively published guidance for the deprecation of RSA and ECC cryptographic algorithms in 2030. Not waiting for Q-day also means that NIST has released standards for a new set of quantum-resistant algorithms. These new algorithms subvert the threat from quantum computers, and the NIST standards provide guidance for how to use them. Some tech providers are moving quickly, but most enterprises, especially those with legacy systems, will require time, planning, and new capabilities to make the switch.

This is why crypto agility (short for cryptographic agility) has become a strategic imperative. It’s not just about being able to adopt new algorithms but also about knowing what you have, where it's used, and how quickly you can change it. And that agility begins with certificates. Without full visibility and control over your certificate infrastructure, your cryptography is essentially out of your hands.

To better understand where enterprises stand on this journey, we partnered with Omdia, a global technology research firm, to survey 272 IT decision-makers from medium to large enterprises across the world. The findings reveal a clear pattern: While awareness is high, execution is lagging. Many organizations know they need to act but lack clear roadmaps or the internal alignment to do so.

The good news: Efforts to prepare for 47-day certificates overlap significantly with the steps needed for broader cryptographic agility. By building certificate agility today, organizations lay the groundwork for a future-proof cryptographic strategy.

As certificate lifespans shrink and PQC timelines become clearer, enterprise IT teams are entering a new era—one that demands faster responses, greater visibility, and the ability to pivot quickly. This report explores how organizations are planning to navigate that transformation.

Table of Contents

Introduction

Measuring the industry's preparedness for shorter certificate lifecycles, quantum migration, and the future of digital trust.

For the first time in our lifetimes, the basic cryptography that secures digital systems across the globe must be ripped out and replaced. The looming threat of quantum computing will soon render today's encryption obsolete, forcing the world to update its cryptographic foundations. This is unprecedented in the history of computing. Every industry, every system, every digital interaction depends on encryption standards we've long taken for granted, but those assumptions are now obsolete.

This change combined with evolving security needs requires a move toward operational models where certificate lifetimes are radically shortened, agility is built by design, and automation is everywhere. Technology leaders must confront a new reality where cryptography has become a dynamic and evolving discipline that they must continuously manage at scale, under pressure, and without breaking the systems we rely on every day.

96%

of organizations are concerned about the impact of shorter SSL/TLS certificate lifespans on their business [figure 5], but less than 1 in 5 feel prepared to handle monthly renewals [figure 4].

100%

of organizations expect to increase investment in PQC over the next 2-3 years [figure 13].

90%

of organizations recognize some degree of overlap between their organization's preparedness for shorter certificate lifespans and PQC readiness [figure 10].

Certificates: From the shadows to the spotlight.

In today's always-on environment, ensuring uninterrupted access to online services is essential for businesses. Yet one of the most frequent, and avoidable, causes of downtime stems from SSL/TLS certificate failures. Whether due to unexpected expiration, misconfiguration, or invalid setup, these certificate issues can render websites or applications completely inaccessible, ultimately eroding customer confidence and damaging a business's brand.

This is precisely why certificate agility is essential, especially as certificate lifespans shrink. Monthly renewals will soon become the norm, forcing IT and security teams to handle:

12x
more renewals

12x
the risk of triggering outages

12x
more work

Manual certificate management simply won't scale.

Are you ready?

The CA/Browser Forum will significantly reduce the maximum allowed validity term for public SSL/TLS certificates over time. The first deadline occurs early in 2026. The time to implement crypto agility practices and automated certificate lifecycle management is now.

Here are the dates you need to know:

Deadline	Maximum Public TLS Lifespan	Renewal Cadence	Maximum DCV Reuse Period
March 15, 2026	**199 days**	**6 months**	**199 days**
March 15, 2027	99 days	3 months	99 days
March 15, 2029	46 days	1 month	9 days

94% of IT decision makers understand 47-day SSL/TLS certificate requirements and deadlines [figure 3].

28% of organizations have a complete certificate inventory [figure 1].

13% feel extremely confident they are tracking all certificates [figure 2].

Without complete visibility into their certificate landscapes, organizations are effectively flying blind.

This shaky confidence with both certificate inventory and certificate discovery increased pressure on organizations which need to manage their certificates at an unprecedented pace in the very near future:

96% of respondents are **concerned about the impact of 47-day certificates** on their organizations [figure 5].

↳ **52%** **Just over half** of respondents are either very or extremely concerned [figure 5].

Alarmingly, **less than 1 in 5 organizations (19%)** feel very prepared to support the change to monthly certificate renewal [figure 4].

When asked about the automation methods or platforms they currently have in place, most organizations reported to be patching together different solutions.

The most common approaches included [figure 6]:

67% Certificate Lifecycle Management (CLM) platform.

58% ACME (Automated Certificate Management Environment) protocol.

57% Custom-built automation tool.

These approaches signal a positive trend, with IT teams recognizing that manually managing certificates is no longer sustainable and opting to invest in automation technologies. Nonetheless, there remains significant room for growth:

53% of organizations use automation to renew certificates [figure 7].

33% use automation for certificate deployment, leaving the other two thirds deploying certificates manually.

32% use automation to perform domain control validation (DCV).

This continued reliance on manual processes raises serious red flags.

"Perhaps because they have been around for three decades, it's like TLS certs have kind of been absorbed into the 'plumbing' that just makes IT work, at least in the perception of many of our respondents. That's why it feels like not enough of them are aware of the 47-day issue that's barreling down the pike towards them, and don't seem to have thought through the need for automation that it is going to impose on their organization."

Rik Turner, Chief Analyst, Cybersecurity, at Omdia

At a 47-day renewal cadence, even a small fraction of overlooked or expired certificates could lead to widespread service outages, lost customer trust, or regulatory consequences.

The lack of preparedness, despite high awareness of the impeding changes, suggests a dangerous gap between knowledge and execution. Many teams may be underestimating the operational lift involved, or worse, delaying automation planning until it's too late.

To avoid a scramble when enforcement dates arrive, with the nearest one being a 6-month renewal cadence by March 2026, leaders must treat certificate agility not as an IT issue, but as a business continuity priority.

CA/Browser Forum Ballot SC081v3

"Requiring more frequent validation of information used in the issuance of certificates and lowering the maximum validity period of certificates reduces the risk of improper validation, the scope of improper validation perpetuation, and the opportunities for misissued certificates to negatively impact the ecosystem and its relying parties."

- While a majority of organizations express intentions to automate certificate management, the reality is that **only 5%** have already fully implemented automation.
- **A staggering 95%** remain at least partially dependent on manual processes as they are planning to increase automation or still evaluating their approach [figure 8].
- **57%** report competing roadmap items as a significant or critical obstacle to adopting automated certificate management [figure 9].

Deadlines are fast approaching; time to act

Early in 2026, public SSL/TLS certificates will require renewals every six months. IT teams still employing manual processes will experience two times the work (and stress) out of the gate. The urgency is real, and organizations that begin planning now can vastly reduce the risk of disruption. Fortunately, the CA/Browser Forum has imposed a clear, phased timeline, giving businesses a predictable path to prepare and adapt.

This phase-down will require organizations to rethink their approach to certificate management. As these accelerated renewal cycles more or less force modernized approaches to certificate management, organizations can use this as an opportunity for long-term improvement. Automation and certificate agility will be essential for the inevitable wholesale migration to PQC. As enterprises gear up for short-lived certificates, they will be wise to look at how these changes will enable their upcoming transition to PQC as well.

The good news is that 90% recognize at least some degree of overlap between their organization's preparedness for shorter certificate lifespans and PQC [figure 10].

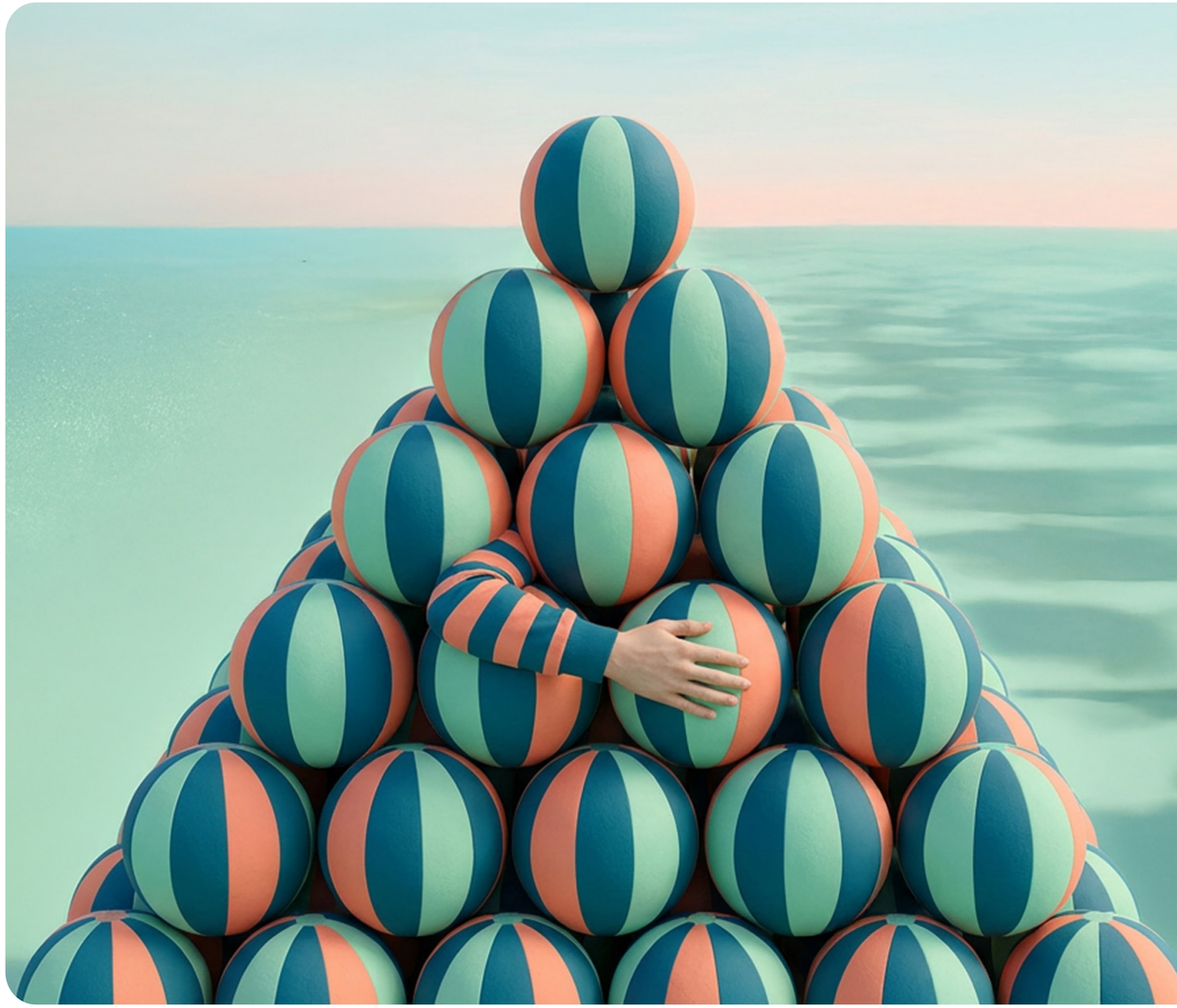
This suggests a growing awareness that while both initiatives are essential, the work done to address one also accelerates progress on the other.

The days of relying on manual certificate renewal are numbered. With lifespans shrinking to just weeks, the volume and frequency of updates will quickly overwhelm traditional processes. Full automation of a certificate's lifecycle is the only way to mitigate the risk of expired certificates, service outages, and security gaps.

Preparing for PQC

Quantum computers, while still evolving, will soon be able to break the encryption that secures online communications and vast amounts of sensitive data stored today. NIST recommends the deprecation of RSA and ECC by 2030. Cryptographic failure at scale could undermine the infrastructure that keeps economies and governments functioning.

Sometimes referred to as the “Quantum Apocalypse,” this scenario describes the cascading consequences that would occur with unmitigated quantum decryption: the collapse of encrypted communications, financial authentication failures, and the complete loss of digital trust in global systems.



1994
Shor's algorithm

Peter Shor develops an algorithm for factoring large integers exponentially faster than classical algorithms, a major breakthrough with implications for RSA and ECC.

1994
Grover's algorithm

Lov Grover introduces a quantum algorithm for searching unsorted databases quadratically faster than classical methods.

2001
First quantum algorithm implementation

IBM and Stanford demonstrate Shor's algorithm on a 7-qubit NMR quantum computer.

2016
NIST PQC initiative

NIST launches a public call for PQC algorithm submissions, the first major government effort to replace RSA and ECC with quantum-resistant alternatives.

2022
NIST selects PQC algorithms

In July 2022 NIST announces the first group of PQC standards: CRYSTALS-Kyber (encryption/key exchange), CRYSTALS-Dilithium, FALCON, and SPHINCS+ (digital signatures). Will later be changed.

2024
NIST releases PQC standards

NIST releases standards for three winning algorithms: FIPS-203 (ML-KEM, formerly CRYSTALS-Kyber), FIPS-204 (ML-DSA, formerly CRYSTALS-Dilithium), and FIPS-205 (SLH-DSA, formerly SPHINCS+). FIPS-206, formerly known as FALCON, is yet to be released.

2029
Gartner's forecast for quantum decryption

Gartner predicts quantum computers will break RSA and ECC by 2029, urging organizations to adopt crypto agility and prepare for quantum-safe encryption.

2030
NIST deprecates RSA and ECC

NIST plans to formally deprecate RSA and ECC by 2030, with full disallowance by 2035, marking the end of classical public-key cryptography for federal use.

This urgency is further underscored by the actions of institutions like NIST, which has released a set of standardized PQC algorithms with more on the way.

With the selection of algorithms such as ML-KEM, ML-DSA, SLH-DSA and FN-DSA, NIST has laid the foundation for fortifying our digital infrastructure against quantum attacks. However, the cryptographic transition is expected to be the most complex in history, and most organizations are still early in their response.

Organizations appear to be taking PQC preparation more seriously than the upcoming shift to 47-day certificate lifespans, even though the deadlines attached to certificate lifespans occur sooner. This disparity suggests that PQC is viewed as a strategic, long-term imperative tied to existential threats, whereas the 47-day change is seen as a more tactical, operational hurdle. However, this framing may underestimate the urgency of near-term risks: Failure to prepare for shortened certificate lifespans is far more likely to result in immediate outage, application failure, and trust disruption.

Crucially, addressing shorter certificate lifespans is a solvable problem and one that can be automated and resolved now, for good. While PQC represents a future-breaking threat, the 47-day challenge poses a present-breaking one, and both require equal prioritization in any robust crypto agile strategy.

14%

of organizations have conducted a full assessment of quantum-vulnerable systems [figure 11].

90%

have budgets allocated to PQC preparedness initiatives within the next 12 months [figure 12].

92%

expect to increase investment in PQC over the next 2-3 years [figure 13].

From awareness to action: Where PQC plans stand today

Gaining insight into organizations' key focus areas sheds light on how they're tackling the complex challenge of PQC. The data shows that most are still in the early stages of their PQC journey, and when asked to identify their primary areas of focus, organizations consistently pointed to information gathering and internal assessments as foundational steps driving their current efforts [figure 14]:

51% Inventorying cryptographic assets.

51% Conducting risk assessments related to PQC.

47% Researching PQC algorithms.

41% Developing migration roadmaps.

While these are critical first steps, they also highlight a significant gap between planning and execution. Far fewer organizations have moved into the next phase – the actual deployment phase – which would include priorities like [figure15]:

21% Engaging vendors.

19% Training and upskilling internal teams.

16% Launching pilot projects.

This suggests that while awareness is growing and groundwork is being laid, the actual implementation of quantum-safe systems remains a future milestone for most. Considering how recently PQC has broken into mainstream IT awareness and the very new nature of directives and guidelines about PQC preparedness, it is not surprising that most organizations are still in the information-gathering stage. It will be revealing to see how these activities change over time as organizational knowledge increases and deadlines loom closer.

When asked to describe their organization's current approach to PQC migration:

80% have some form of PQC migration strategy in mind.

- **27%** With the most popular strategy being one of a gradual phase-in of technology.

The remainder of the results showed some concerning data:

43% of respondents were in a "wait and see" holding pattern.

- **20%** of them did not have any current strategy in mind.
- **23%** of them are waiting for more mature solutions to become available [figure 15].

Planning for PQC is one step, but executing that plan across tangled legacy systems, outdated cryptographic libraries, and underresourced teams is where most organizations are stalling, hoping for a silver bullet solution.

Quantum Momentum: Recent key hardware & roadmap milestones

As the race toward practical quantum computing accelerates, several major players have unveiled breakthroughs that signal a new era of scalability and reliability:

Google Willow chip

In December 2024, Google introduced Willow, a 105-qubit superconducting chip that achieved a landmark in quantum error correction. Willow demonstrated exponential error reduction as it scaled and completed a benchmark computation in under five minutes, something a classical supercomputer would take 10 septillion years to solve.

Microsoft Majorana 1

In February 2025, Microsoft launched Majorana 1, the world's first quantum processor powered by topological qubits. Built using a novel material called a topoconductor, this chip is designed to scale to a million qubits on a single chip, an essential threshold for fault-tolerant, industrial-scale quantum computing.

IBM Quantum Starling

In June 2025, IBM announced its detailed roadmap to have a practical quantum computer by 2029 and a much larger system, Starling, which will have about 200 logical qubits, by 2033.

What's really driving PQC migration?

Looking at the major drivers for PQC migration revealed that compliance, not risk, is the primary driver behind most organizations' PQC planning.

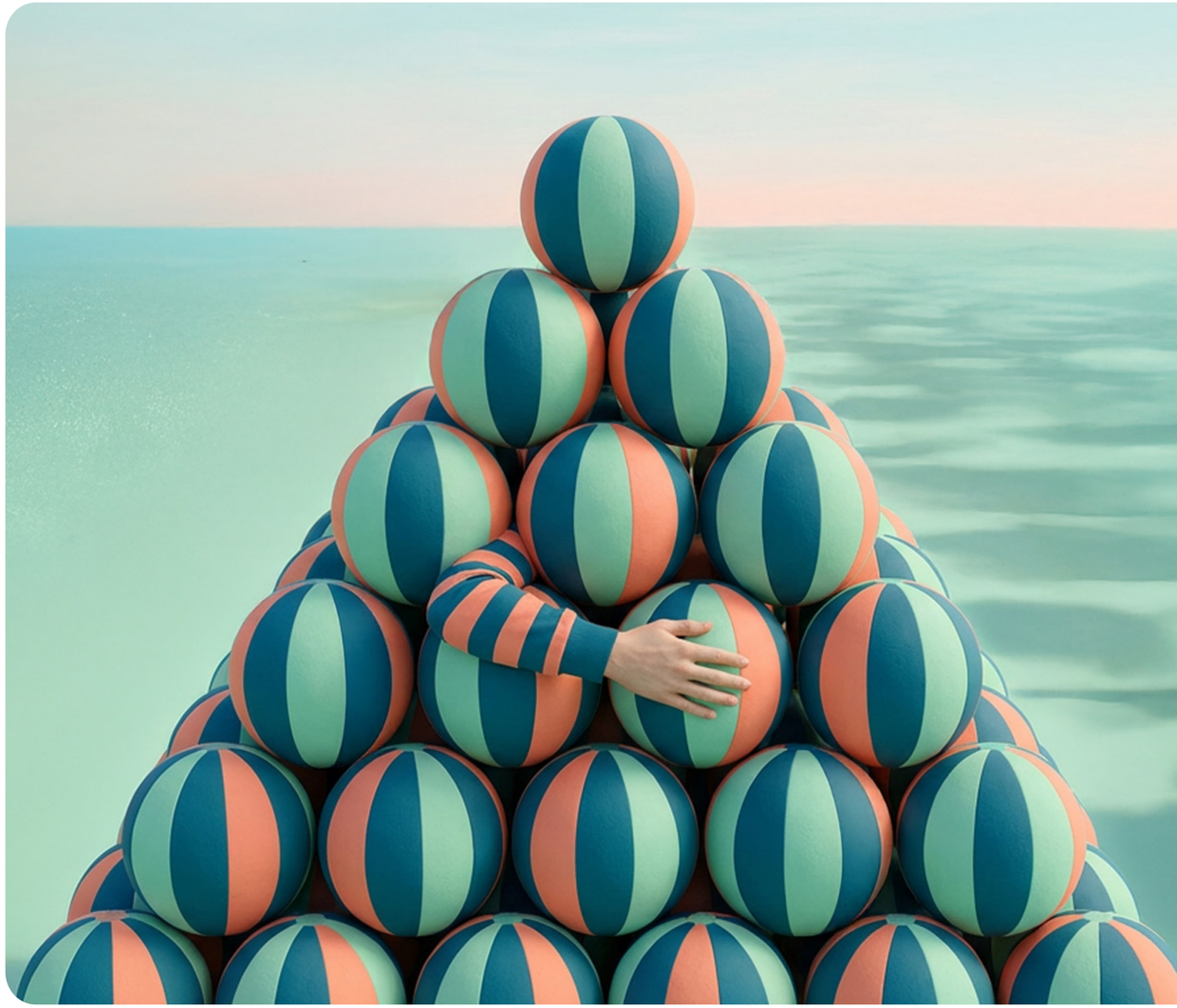
Exactly half of organizations cited NIST's deprecation of RSA 2048 and ECC 256 as the most influential factor driving the need to adopt PQC.

48%

Followed closely with wanting to proactively prepare to meet upcoming standards/new government mandates.

22%

Interestingly, actual mitigation of current quantum threats, in particular Harvest Now, Decrypt Later (HNDL), was only at 22% [figure 16].



Active quantum threats

Quantum computing threats are not just hypothetical. Criminal organizations and state actors are already actively engaged in establishing exploits. One of the most urgent and actionable risks today is the “harvest now, decrypt later” (HNDL) attack. In an HNDL scenario, malicious actors intercept and store encrypted data now, with the intent to decrypt it once quantum computers are powerful enough to break today’s encryption algorithms.

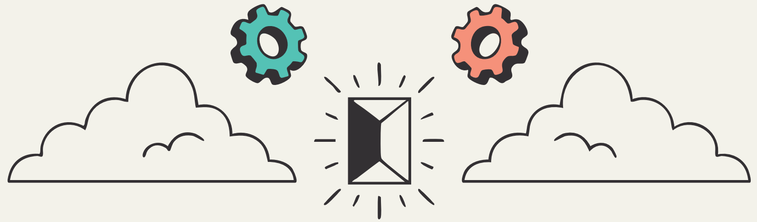
This creates a silent and invisible threat: Even if data appears safe today, it may be fully exposed tomorrow. Sensitive information such as financial transactions, intellectual property, or national security data, that can be stolen today will be retroactively exposed, undermining decades of confidentiality protections.

60%

of organizations are very or extremely concerned about HNDL attacks, signaling that this threat has moved from theoretical to tangible [figure 20].

59%

are very or extremely concerned about “trust now, forge later” attacks, in which adversaries steal digitally signed documents today with the intent to forge or impersonate long-lived private digital signatures in the future.



In comparison, 68% express concern over man-in-the-middle (MitM) attacks, one of the most widely understood threats today. Given that both quantum threats are relatively new and esoteric, their concern levels being nearly on par with MitM in the context of PQC highlights the significant attention these quantum-era threats are already receiving.

This underscores a critical insight

While organizations are indeed moving toward PQC, they are doing so largely because standards are compelling them to do so. And that’s precisely the point of mandated standards: to drive the right behavior. The relatively low prioritization of HNDL in figure 16 suggests that, left to their own devices, many organizations might delay action, assuming quantum threats are a distant or external concern. Standards help break this short-term mindset by imposing requirements that demand long-term resilience, ensuring that organizations take proactive steps today to secure their future.

This emphasis on compliance and standards-driven motivation reveals a broader organizational mindset, one that is often reactive rather than proactive. While many are beginning to prioritize PQC migration, the road ahead is anything but straightforward. The next major hurdle lies not in the why, but in the how.

Coordinating complexity: Why PQC demands a centralized, strategic response

The transition from RSA and ECC to quantum-secure algorithms will be complicated by the scope, complexity, and heterogeneity of the digital systems powering nearly all enterprises today. Technical departments are likely to choose a mixed approach to transitioning to PQC in direct response to this challenge, prioritizing systems, processes, and environments for PQC adoption based on their ease of migration and criticality of what they protect.

When asked about how they would prioritize systems for PQC migration, IT teams prioritized based on [figure 17]:

56%
Data sensitivity

57%
Compliance requirements

57%
Risk level

When asked to choose the organizational areas they want to prioritize for PQC implementation, the following were most popular [figure 19]:

50%
Critical infrastructure

49%
Authentication

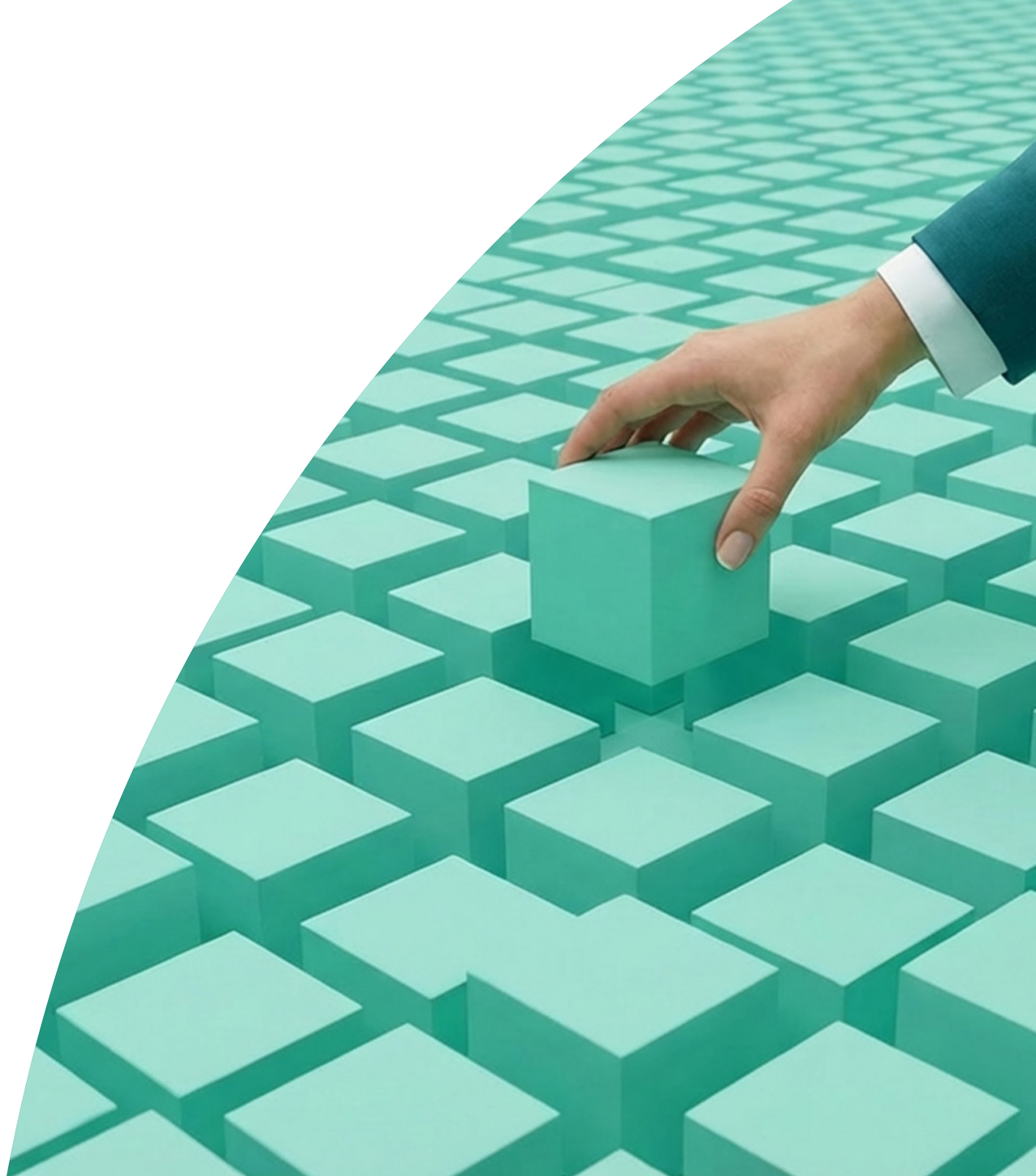
50%
Digital signatures

59%
Digital storage

IT organizations will need to build certain technical capabilities to conduct this migration and then to maintain robust cryptographic standards in a future where significant cryptographic updates become a regular part of doing business. However, modern enterprise environments add significant layers of complexity to PQC migration.

Organizations must navigate a patchwork of heterogeneous systems, decentralized development teams, and deeply interdependent platforms, many of which follow their own release cycles and operate with limited alignment on risk, timelines, or priorities. In this fragmented landscape, even small cryptographic changes can create ripple effects across business units or critical operations. Legacy infrastructure further compounds the challenge: Many business-critical applications still rely on hardcoded cryptographic functions written in aging languages like COBOL or Perl.

These systems often lack modular cryptographic design, making algorithm replacement risky or poorly understood. And with minimal tolerance for downtime, progress is both high-stakes and resource-intensive.



"It seems to me that there are two reasons not to simply wait till Q-Day. One is that technology has the ability to surprise us: witness the absolute explosion in AI adoption since ChatGPT was launched on an unsuspecting world in November 2022. The other is the suspicion that the bad guys aren't waiting. In other words, threat actors may be harvesting your most heavily encrypted data now, in the expectation of being able to decrypt it as soon as they get their hands on a QC. And of course, if they are backed by nation-states, they'll gain access to one long before the average company does"

Rik Turner, Chief Analyst, Cybersecurity, at Omdia.

This complexity is reflected clearly in the data

98%
of organizations have or expect to experience challenges with PQC implementation [figure 21].

92%
expect to encounter some sort of barriers during implementation [figure 23].

Top challenges include [figure 21]:

56%
Coordination across teams

50%
System complexity

49%
Lack of expertise

The most frequently cited barriers expected during PQC implementation with legacy systems include [figure 23]:

53%
Integration complexity

49%
Risk of downtime

49%
Compatibility issues

97% of organizations report significant skills gaps related to PQC.

With the most acute shortages in [figure 22]:

56%
Implementation experience

52%
Cryptography expertise

47%
Strategic planning

These figures highlight the urgent need for structured, coordinated approaches. Setting up a Center of Cryptographic Excellence (CryptoCOE) is an essential response to most of these challenges. Cryptography is woven through legacy infrastructure, modern applications, and third-party services, each owned by different teams with different priorities. This heterogeneity makes coordination difficult, and without a centralized approach, efforts to implement PQC can quickly become fragmented.

A CryptoCOE is the healthy, strategic response to this complexity and brings structure, alignment, and long-term focus to an otherwise chaotic landscape.

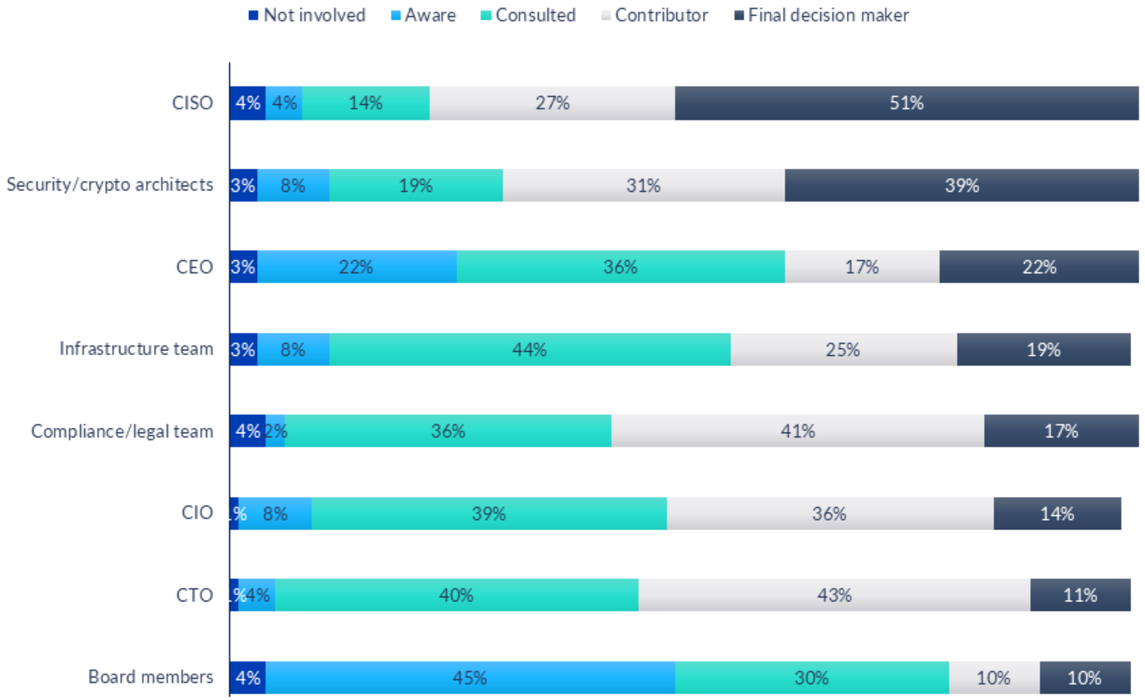
A CryptoCOE offers a structured, yet dynamic framework to drive the strategic development, management, and enforcement of cryptographic policies and best practices across entire organizations. According to Gartner, by 2028, organizations with a CryptoCOE will save 50% of costs by switching to post-quantum cryptography, compared to those organizations without[1].

Whose responsibility is PQC?

Currently, the push for PQC migration is being led primarily by CISOs and security teams, those closest to the threat and most aware that today's cryptography won't withstand tomorrow's quantum attacks. But while they're sounding the alarm, the path forward is anything but simple. Roadmap complexity, budget constraints, legacy infrastructure, and the need for cross-team coordination all make this a heavy lift. Without strong backing from the CEO and board, who currently show lower levels of involvement, these efforts risk stalling. To succeed, PQC must become a business priority, not just a security initiative.

[1][Source: Gartner, "Infographic: Why You Need a Crypto Center of Excellence Now" by Mark Horvath; July 18, 2024.]

What level of involvement do the following stakeholders have in PQC decisions at your organization? [figure 18]



This lack of executive engagement has real consequences. Without clear business prioritization and top-down support, PQC initiatives face significant risk of delay or disruption. This is reflected in the data:

15% of organizations feel “extremely confident” in their ability to integrate PQC without major disruption.

The remaining majority are navigating uncertainty, underscoring the need for stronger leadership alignment and strategic investment to ensure successful migration [figure 24].

As organizations begin planning for PQC, their priorities reveal that PQC is an entire operational transformation. The shift to quantum-safe algorithms touches every layer of the enterprise, from infrastructure and tooling to governance and cross-team coordination. Most organizations can't simply "swap out" algorithms; they must rethink how the integrate, manage, and scale cryptography across their environments.

When asked what matters most in a PQC solution, respondents emphasized practical, enterprise-wide capabilities [figure 25]:

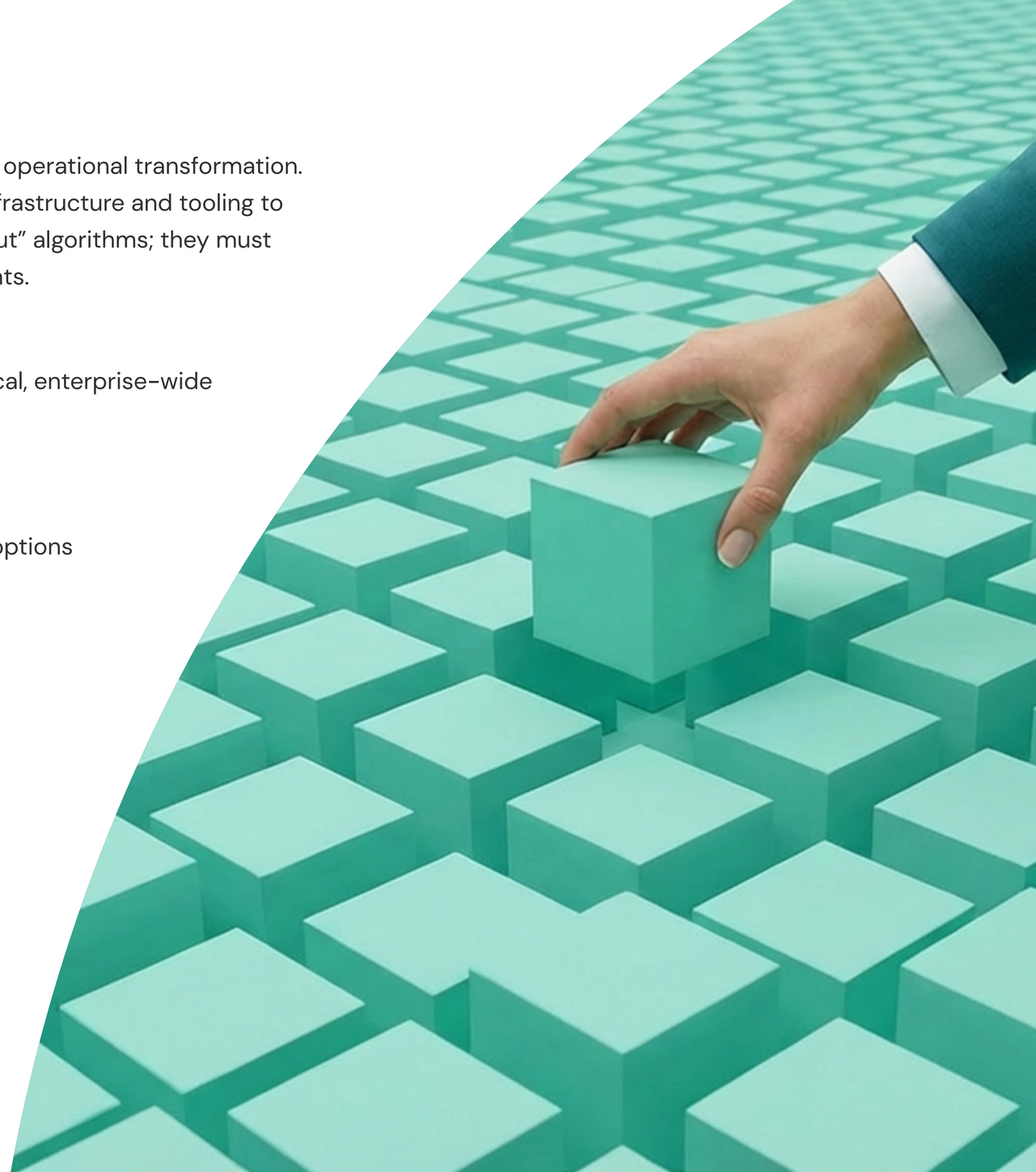
58%
Integration with existing platforms

55%
Ease of implementation

49%
Automation options

These are enterprise-wide requirements that demand coordination across IT, security, and business leadership. PQC must be treated as a shared responsibility, one that spans leadership, strategy, and execution. The path to achieving crypto agility is not a single leap but a series of deliberate, coordinated steps. While most organizations are still in the early stages, focused on discovery, planning, and internal alignment, the urgency remains clear.

The organizations that succeed will be those that treat PQC not as a one-time upgrade, but as a long-term operational shift. By investing now in automation, visibility, and cross-functional collaboration, enterprises can turn today's uncertainty into tomorrow's resilience.



Securing tomorrow's future by solving today's challenge

The shift to 47-day certificate lifespans should be treated as a wake-up call, signaling that manual approaches to certificate management are no longer sustainable. With major deadlines as early as 2026, organizations need to act now or risk avoidably outages. Manual processes simply won't keep up.

The upside? Preparing for this shift doesn't just solve a short-term operational challenge; it accelerates long-term crypto agility and better prepares organizations for PQC. By embracing automation, improving visibility, and achieving certificate agility today, organizations build the foundation for a more secure, resilient, and quantum-ready future.

The choices organizations make now will not only address today's pressures, but they'll define their ability to meet tomorrow's quantum threats with confidence.

Y2K vs Q-Day

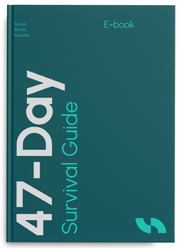
Some compare the urgency around the Quantum Apocalypse (also referred to as Q-Day) to the Y2K panic, suggesting it might be overblown. But that comparison misses a critical point: Y2K was a non-event because the world invested massive resources, including hundreds of billions of dollars and millions of labor hours, to prevent disaster. With Q-Day, we haven't made that investment yet. Today's systems are far more interconnected and most of our cryptographic infrastructure is not quantum-resistant.

	Y2K	Q-Day
Target date	Well-known January 1, 2000.	Unknown: estimated 2030.
Threat duration	Finite: no pre-Y2K threat, ended within months.	Ongoing: active attacks now, threats ongoing past Q-day.
System impact	Limited: application, data updates.	Broad: all interconnected systems, networks, applications and data infrastructure.
Advanced implementation timeline	6-12 months in advance.	Years in advance.
Remedy level of effort	100s billions of dollars, millions of labor hours.	Completely unknown.

Resources

Accelerate your crypto agility journey.

For organizations looking to move from planning to execution, several practical resources are available to help guide the way. Sectigo has developed a suite of tools and guides tailored to the most pressing challenges in cryptographic transformation. These resources are designed to help teams move beyond awareness and into action, equipping them with the knowledge, tools, and confidence to build a crypto agile future.



The 47-Day Survival Guide

A tactical playbook for adapting to shortened certificate lifespans, this guide outlines the operational changes, automation strategies, and best practices needed to thrive in a 47-day renewal world.

Read Now

Embracing Quantum Readiness

This eBook offers a strategic framework for preparing your organization for PQC migration, including risk assessments, roadmap development, and stakeholder alignment.

Download Now

Choosing a Reputable Certificate Authority (CA)

As cryptographic complexity increases, selecting the right CA becomes more critical than ever. This guide helps organizations evaluate CAs based on trust, compliance, and future-readiness.

Explore the Guide

Methodology

Omdia collected a total of 272 survey responses in June 2025 from C-level, vice-presidents and director leaders in IT, technical operations, cybersecurity and risk departments across a mix of industries and business sizes across the U.S. and EMEA. Omdia used its proprietary access to lists, panels and databases to gather quality responses and cleaned the data throughout fielding to ensure data quality.

Analysts involved with research and analysis:

Rik Turner, chief analyst, cybersecurity

Alexander Harrowell, principal analyst, advanced computing for AI

sectigo

About Sectigo

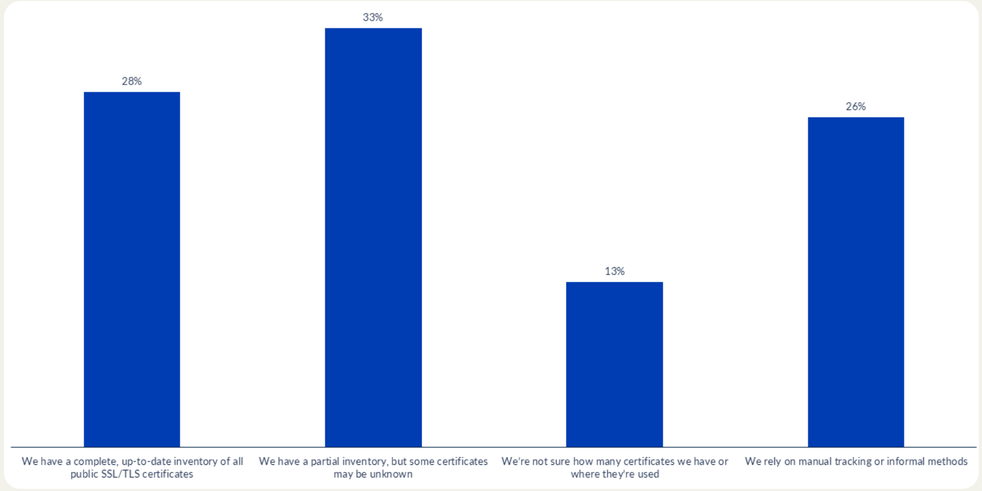
Sectigo is the most innovative provider of certificate lifecycle management (CLM), delivering comprehensive solutions that secure human and machine identities for the world's largest brands. Sectigo's automated, cloud-native CLM platform issues and manages digital certificates across all certificate authorities (CAs) to simplify and improve security protocols within the enterprise. Sectigo is one of the largest, longest-standing, and most reputable CAs with more than 700,000 customers and two decades of delivering unparalleled digital trust.

Get in Touch

Appendix

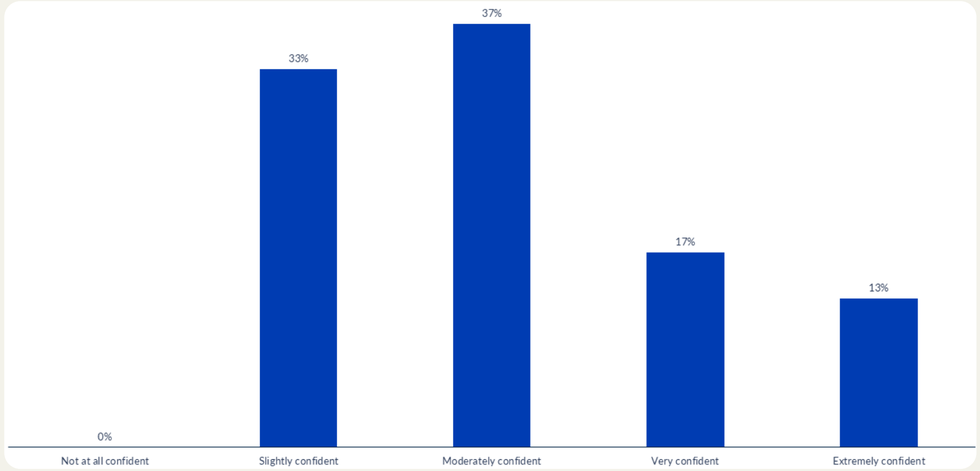
[figure 1]

Which best describes your organization's understanding and tracking of public SSL/TLS certificates currently in use?



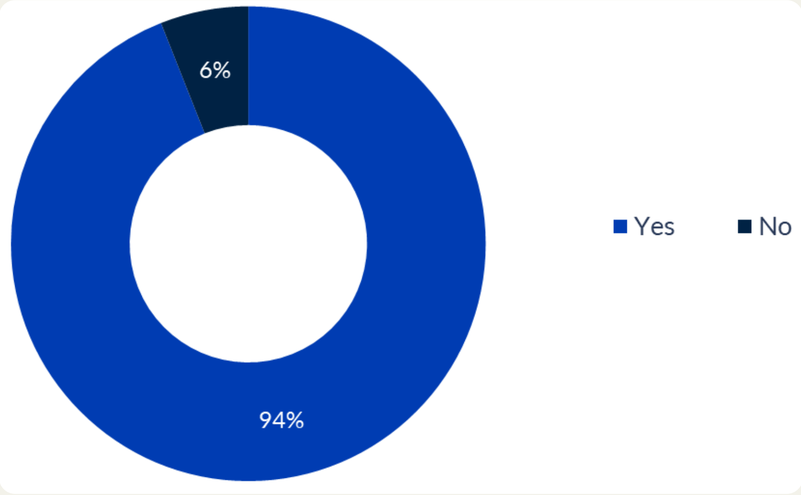
[figure 2]

How confident are you that your organization is tracking ALL certificates, even rogue certificates?



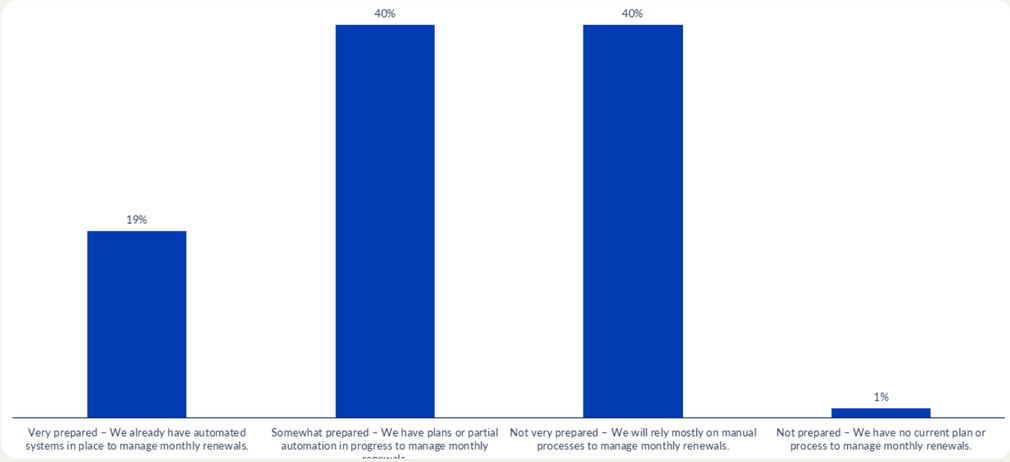
[figure 3]

New industry guidelines will reduce the maximum validity period of public SSL/TLS certificates to just 47 days by 2029. Were you previously aware of this change?



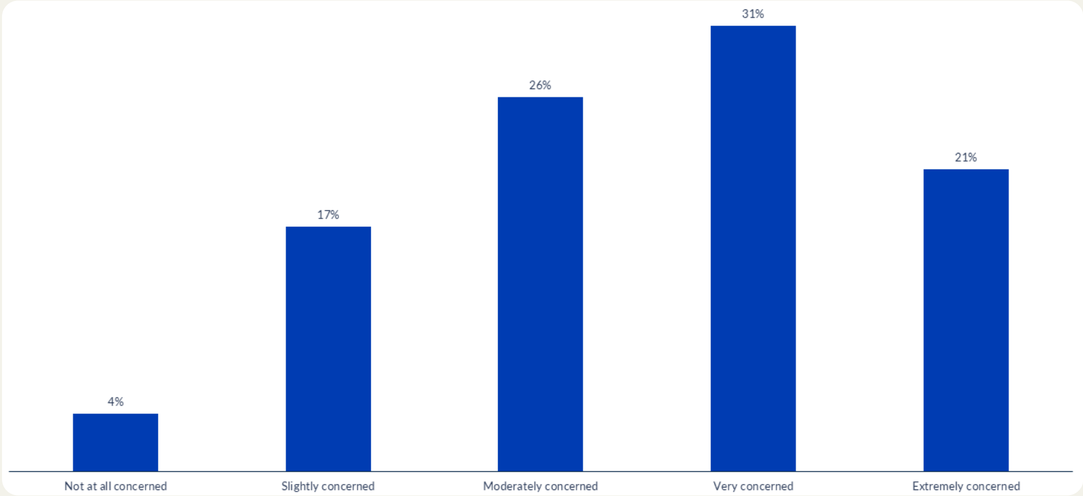
[figure 4]

How prepared is your organization to transition toward renewing all public TLS/SSL certificates on a monthly basis to satisfy this requirement?



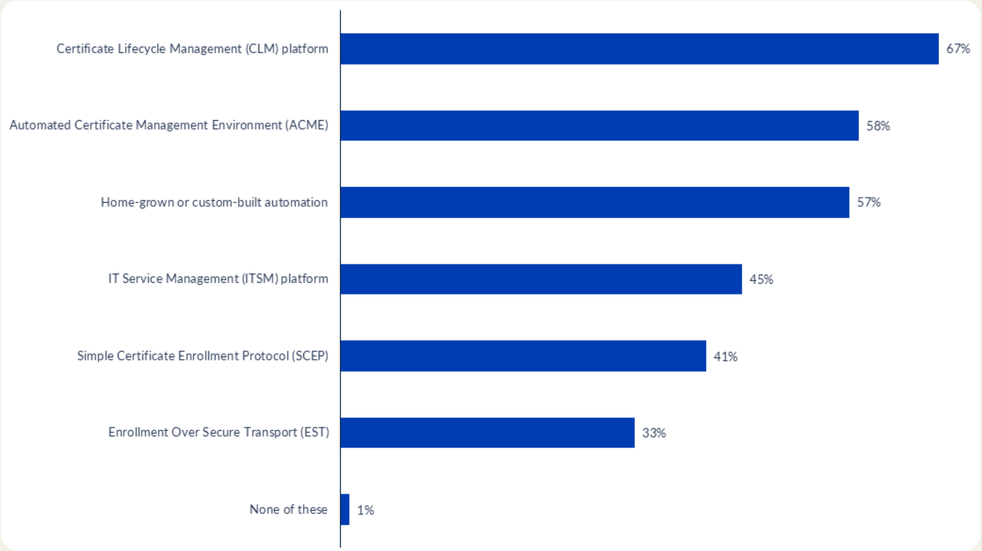
[figure 5]

How concerned are you about the impact of 47-day certificate lifespans on your organization?



[figure 6]

Which automation methods or platforms does your organization currently use for certificate management?



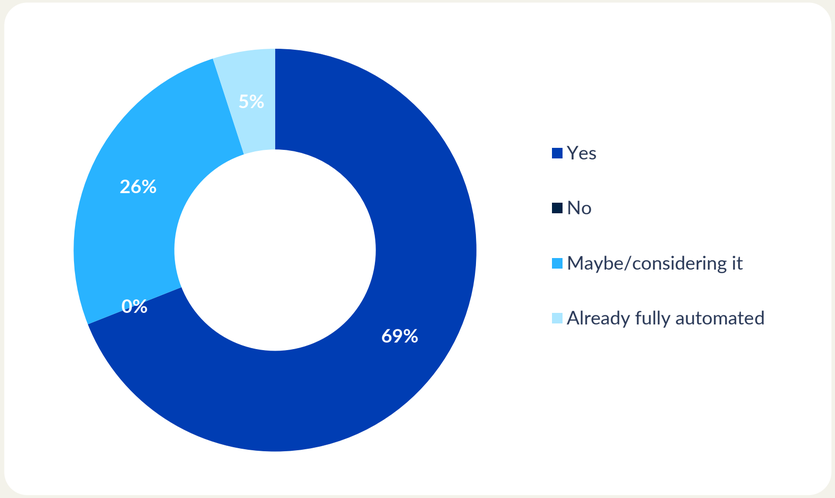
[figure 7]

What percentage of your organization's SSL/TLS certificates are automated for each of the following tasks? (Average)

Task	Average
Provisioning certificates for new applications or services	32%
Renewing certificates	53%
Deploying certificates	33%
Revoking and otherwise managing certificates	27%
Performing Domain Control Validation	32%

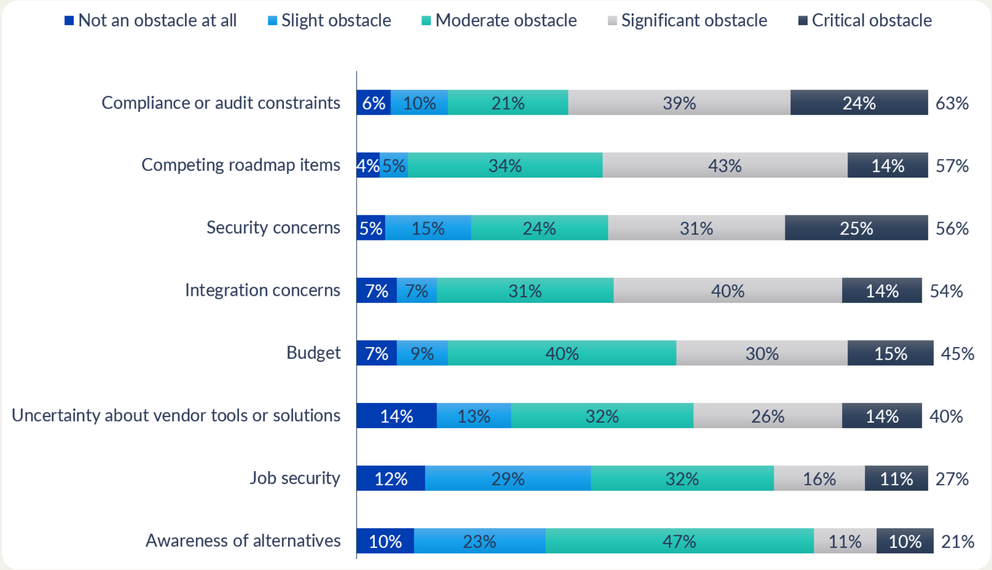
[figure 8]

Will you increase automation in certificate management because of shorter certificate lifespans?



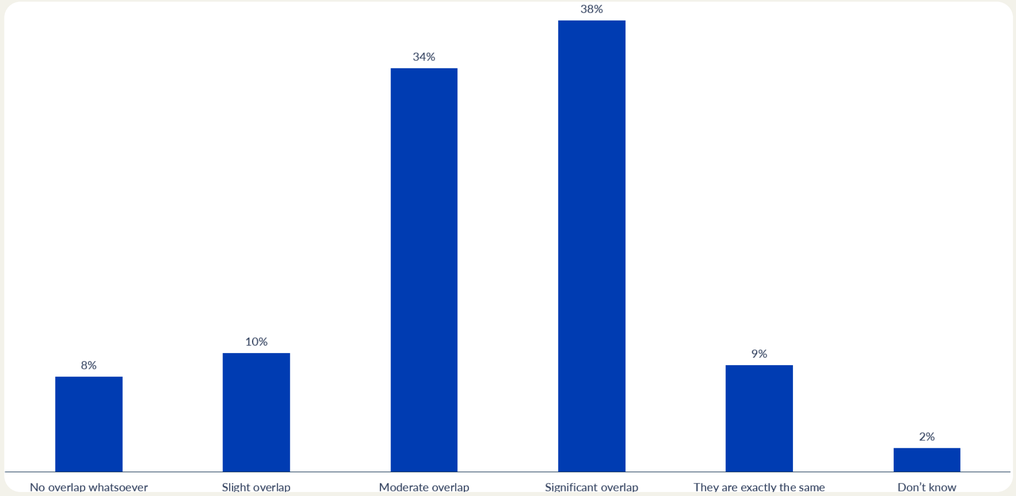
[figure 9]

To what degree are the following aspects obstacles in your organization's adoption of automated certificate management?



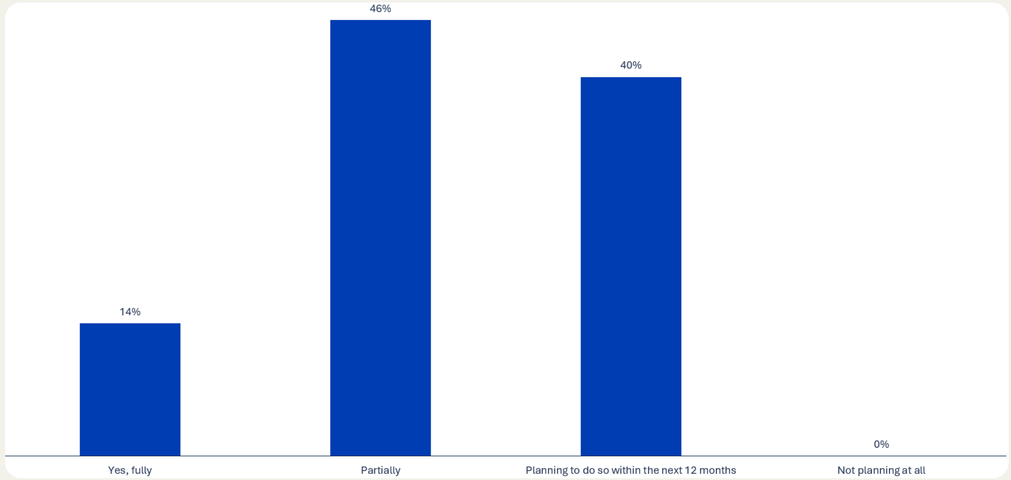
[figure 10]

To what degree do you see overlap in your organization's preparedness for 47-day public SSL/TLS certificates and post-quantum cryptography?



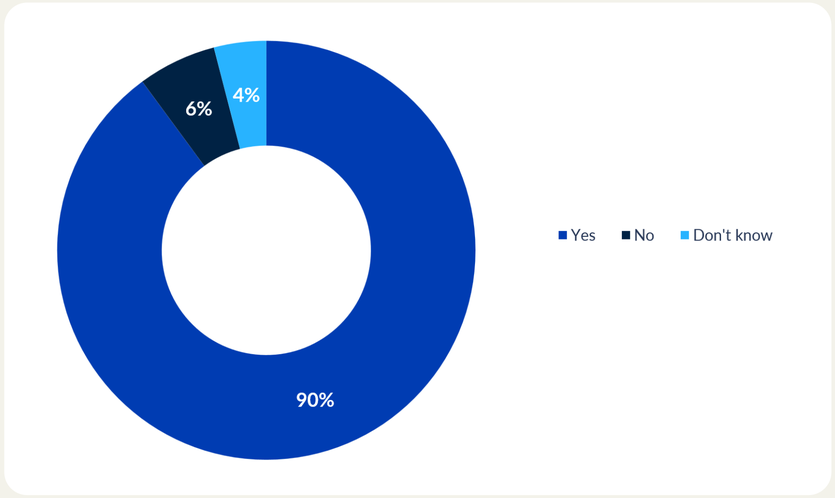
[figure 11]

Has your organization conducted an assessment of systems vulnerable to quantum computing attacks?



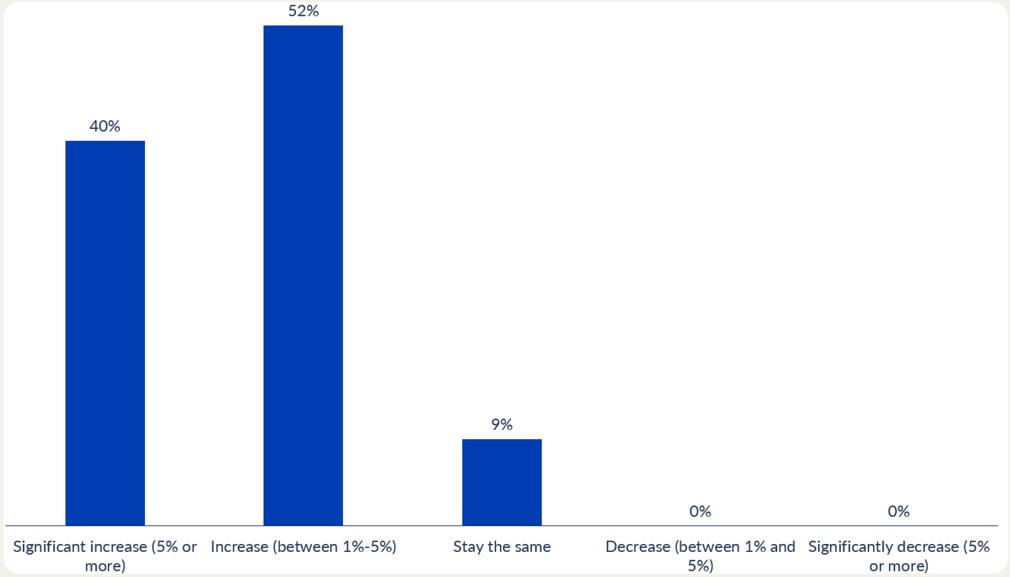
[figure 12]

Do you have a budget allocated to quantum-safe security initiatives over the next year?



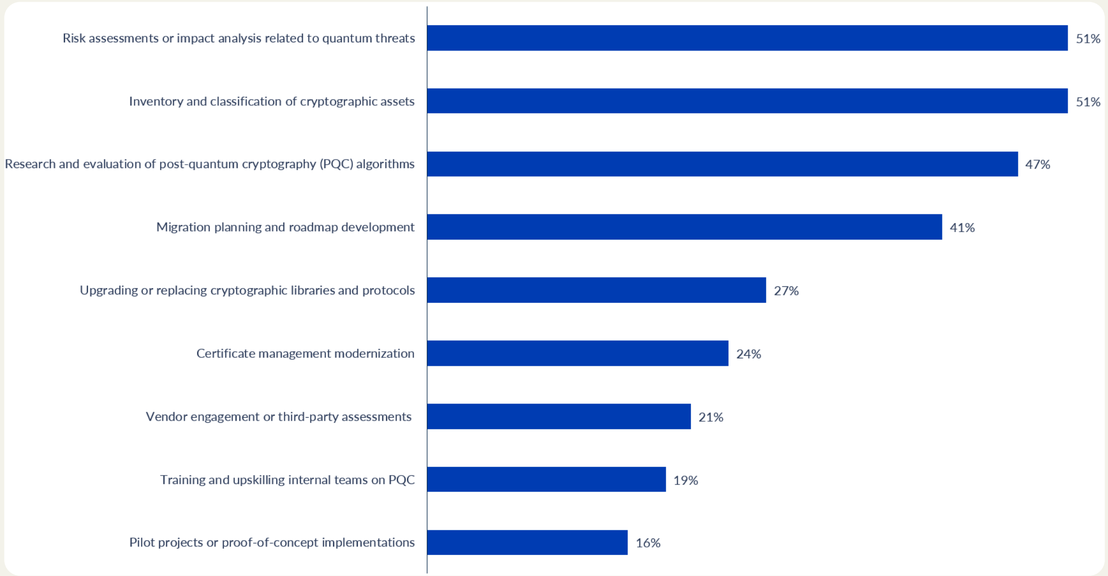
[figure 13]

How do you expect your organization's PQC investment to change over the next 2-3 years?



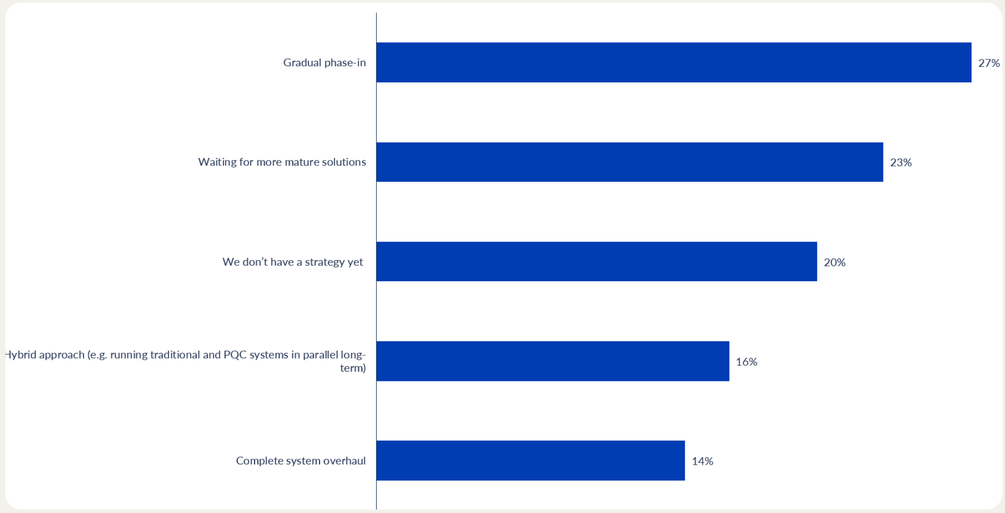
[figure 14]

What are your organization's top quantum-safe priorities?



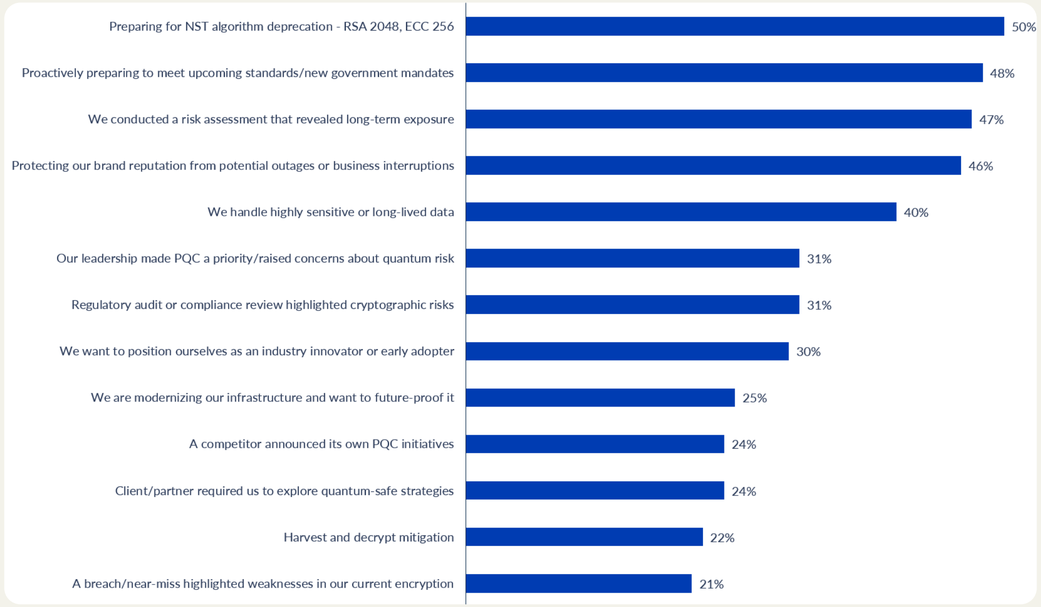
[figure 15]

Which best describes your organization's current approach to PQC migration?



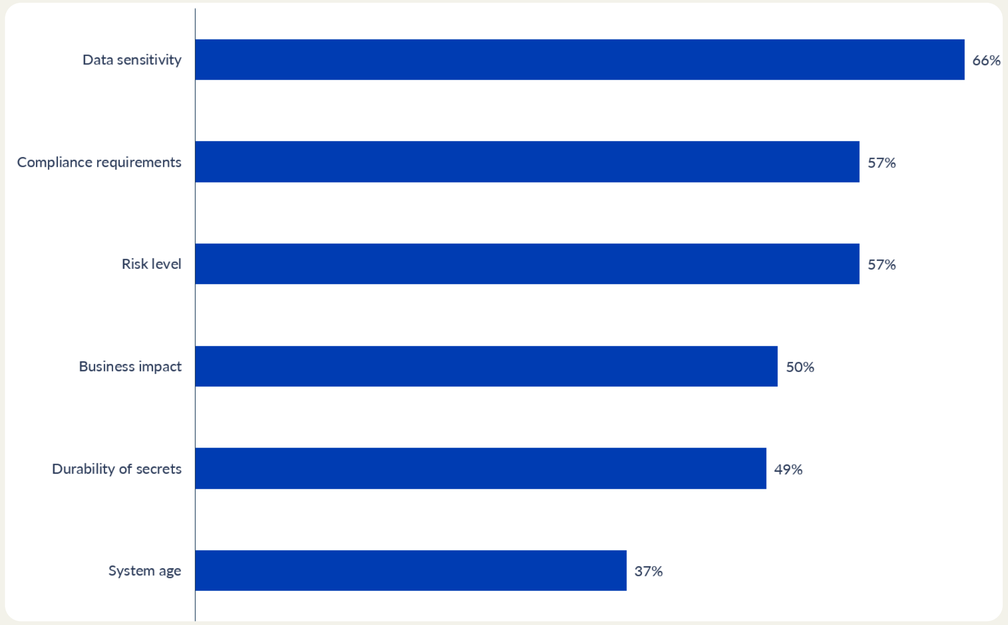
[figure 16]

What are the most influential factors driving your organization's need for PQC adoption?



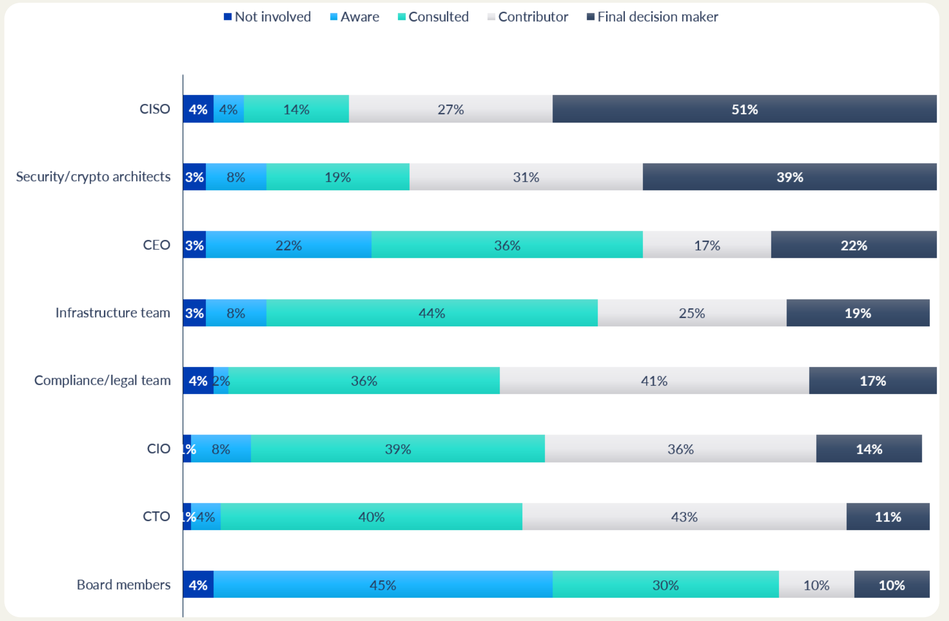
[figure 17]

How are systems prioritized for PQC migration?



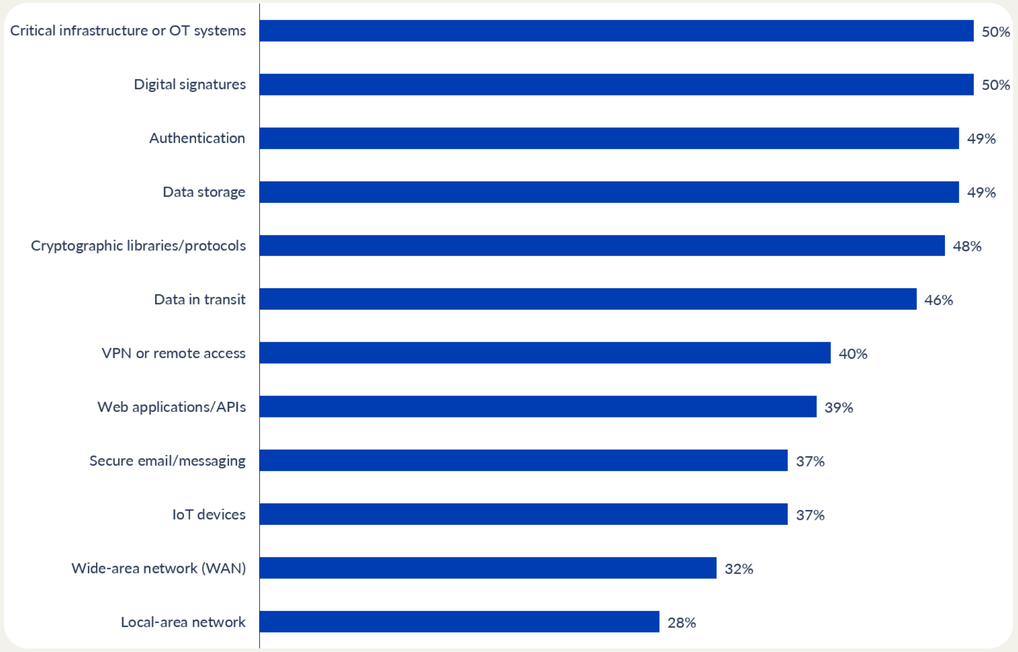
[figure 18]

What level of involvement do the following stakeholders have in PQC decisions at your organization?



[figure 19]

Which areas has your organization prioritized for PQC implementation?

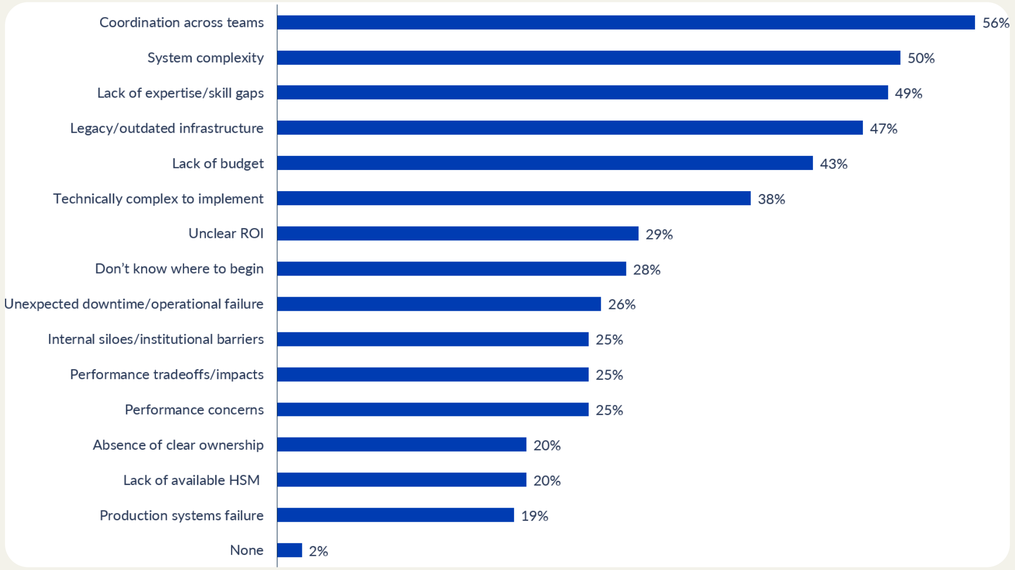


[figure 20]

How concerned are you about the following quantum computing threats?

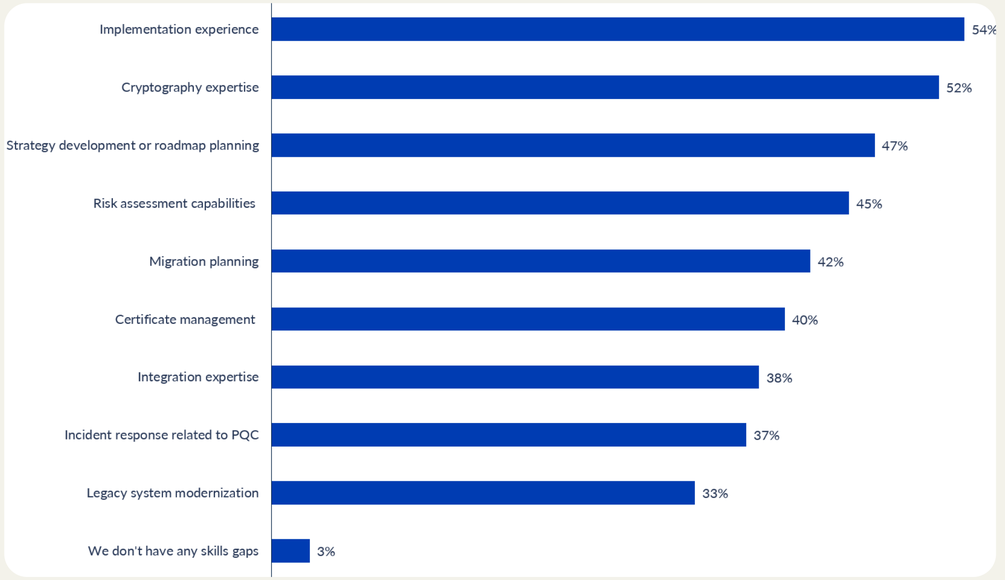
[figure 21]

What challenges have you experienced, or do you expect to experience, when implementing PQC?



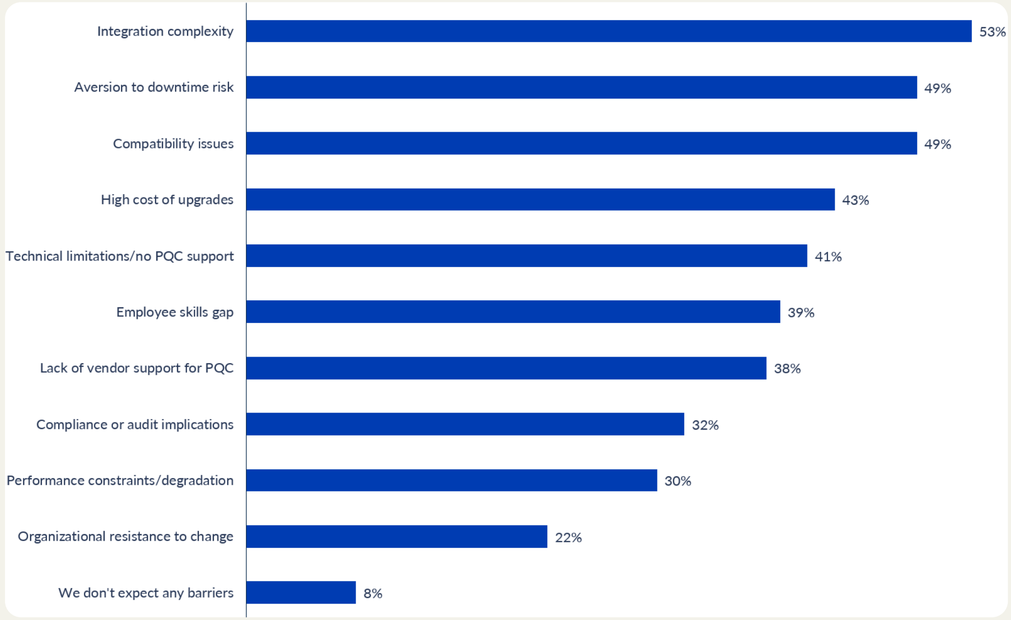
[figure 22]

Where does your organization face the most significant PQC-related skills gaps?



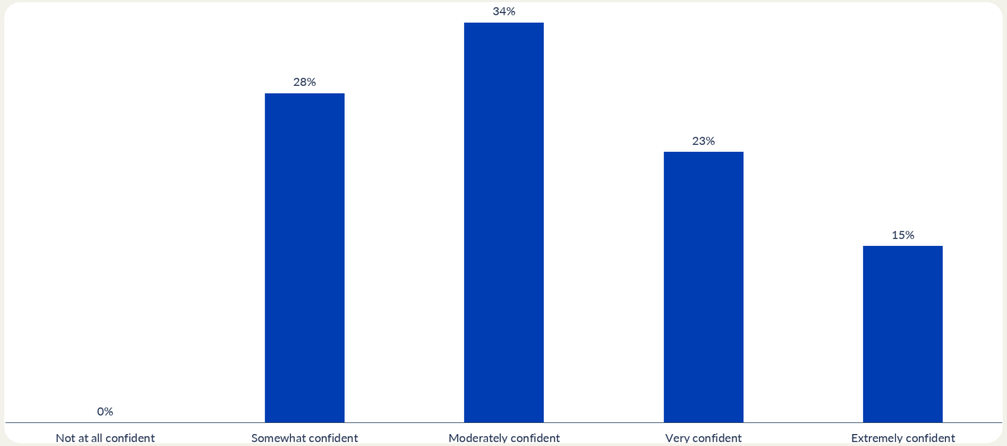
[figure 23]

What barriers do you expect to experience during PQC implementation with your legacy systems?



[figure 24]

How confident are you in your current systems' ability to integrate PQC without major disruption?



[figure 25]

What are the most important factors/features when selecting PQC solution support?