sectigo

2026 State of Crypto Agility

From awareness to action



Foreword

Nick France
Chief Technology Officer, Sectigo



Crypto agility has entered its execution era

When we published the inaugural State of Crypto Agility report in 2025, two major shifts were still largely discussed as future challenges: Dramatically shorter SSL/TLS certificate lifespans and the transition to post-quantum cryptography (PQC). One year later, both are becoming active operational priorities, while agentic AI is creating an entirely new class of digital identities to secure.

The conversation has therefore changed. Awareness is no longer the primary hurdle. Organizations increasingly understand the pressures ahead, but the challenge now is turning that awareness into coordinated action across cryptographic discovery, automation, architecture, governance, and investment.

The findings do show encouraging progress. More organizations are assessing quantum-vulnerable systems, allocating budget to quantum-safe initiatives and improving visibility into their certificate environments. This reflects an important shift in how cryptography is viewed inside the enterprise.

Once treated as a largely static component of IT infrastructure, it is increasingly recognized as a strategic business function that underpins digital trust, cybersecurity and operational resilience.

Yet progress does not necessarily mean resilience.

Certificate-related incidents remain common. Automation is improving but remains uneven across the certificate lifecycle. Concern around shorter certificate lifespans is growing.

And while more organizations are evaluating their quantum exposure, the scale and complexity of the transition ahead is becoming clearer. PQC migration will require organizations to understand where cryptography exists, assess vulnerable systems, coordinate across technology providers, and prepare for future changes to PKI architecture, including emerging approaches such as Merkle Tree Certificates (MTCs).

At the same time, the scope of cryptographic operations continues to expand. AI agents require identities that can be authenticated, constrained, monitored, and revoked. The good news is that these requirements do not sit apart from certificate lifecycle modernization or PQC readiness efforts. They depend on many of the same foundational capabilities.

This year's study expands the view, drawing on 500 senior IT and cybersecurity decision-makers across North America, EMEA, and APAC. Because the geographic scope is broader than in 2025, year-over-year comparisons should be viewed as directional. Even so, the overall trend is unmistakable: Organizations are moving from planning to execution.

The central message of the 2026 research is clear. Organizations cannot treat shorter certificate lifespans, quantum readiness, and emerging machine identities as isolated initiatives. The organizations best positioned for what comes next will be those that build an adaptable digital trust foundation capable of supporting continuous change, turning awareness into repeatable operations and confidence into measurable resilience.

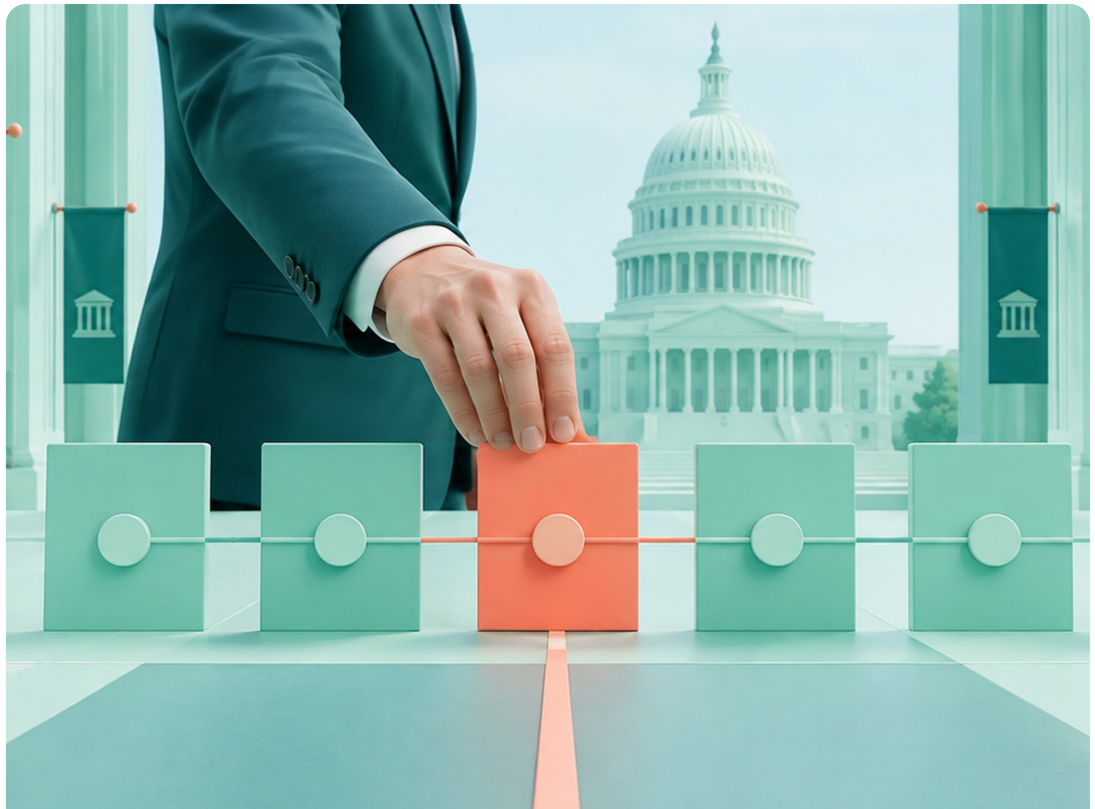


Table of contents

Introduction: The pressure to act is accelerating 5

PQC readiness will require a new PKI architecture 8

Shorter certificate lifespans are testing operations now 15

Agentic AI creates a new digital identity imperative 19

Conclusion: Build one foundation for continuous change 21

Resources 22

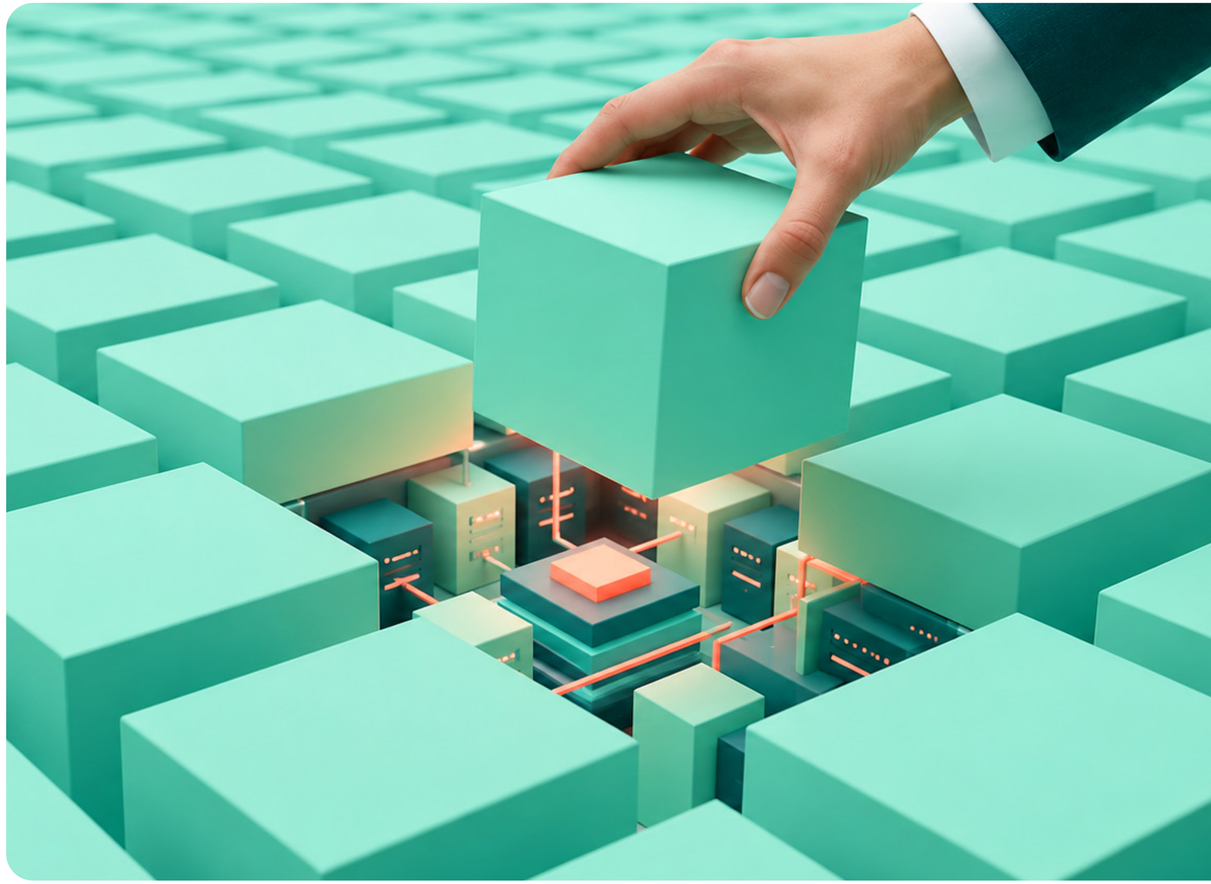
Methodology 23

Introduction

The pressure to act is accelerating

Crypto agility has moved from an industry aspiration to an operating requirement. Over the past year, the timelines, technology shifts, and security developments surrounding cryptography have compressed. NIST standards are available for implementation. Government and major technology-provider roadmaps are creating concrete migration horizons. Just as importantly, organizations increasingly recognize that waiting for a cryptographically relevant quantum computer to arrive is not a viable strategy. The migration itself is expected to take years, while data stolen today may retain value long enough to be decrypted in the future.

At the same time, organizations are already experiencing another major cryptographic shift: Shorter certificate lifespans. Certificate validity periods are shrinking in stages, increasing the operational demands of certificate management and exposing the limitations of manual processes. What was once an annual renewal exercise is becoming a continuous operational discipline that depends on visibility, automation, and governance across the certificate lifecycle.



A third trend is beginning to emerge alongside these changes. As agentic AI adoption accelerates, organizations must prepare to manage identities not only for people and machines, but also for autonomous software agents. These agents will require authentication, authorization, monitoring, and revocation, extending digital trust requirements to an entirely new class of identity.

These developments are different in form, but they point to the same conclusion: Organizations can no longer manage cryptography as static infrastructure. Algorithms, certificates, keys, and identities must be discoverable, governed, and capable of changing without disrupting the business.

The 2026 findings suggest that message is landing. Organizations report active assessment of quantum-vulnerable systems, strong investment intent, and growing automation. But movement does not yet equal resilience. Many teams still face outages, incomplete automation, and architectural constraints that will become more consequential as changes accelerate.



Three pressures define this year's report. First, PQC is moving from awareness to architecture and migration. Second, shorter certificate lifespans are exposing the operational consequences of manual or fragmented certificate management. Third, agentic AI is creating a new identity challenge at machine scale. The organizations best positioned for all three will be those that treat crypto agility as a shared capability rather than a collection of separate projects.



The next measure of readiness is not whether organizations recognize the risks. It is whether they can translate recognition into repeatable, testable, and scalable operations.

78%

believe today's PKI will need to change to a great or very great extent to support PQC [Q9]

Only

38%

have fully assessed systems vulnerable to quantum attacks [Q10]

Among those with PQC budgets allocated over the next year

93%

expect PQC investment to increase over the next two to three years [Q12]

61%

experienced a certificate-related outage or incident in the past 12 months [Q3]

PQC readiness will require a new PKI architecture

The transition is moving from planning to execution

Last year, our research found that organizations viewed PQC as a strategic priority, often placing greater focus on future quantum threats than on near-term cryptographic challenges like shorter certificate lifespans. At the time, the conversation centered largely on awareness. Organizations understood the potential impact of quantum computing, but many were still determining what preparation would require in practice.

Active quantum threats

The quantum threat is not a future problem alone. Data encrypted today can be harvested now and decrypted in the future, creating risk long before quantum computers can directly break current cryptographic algorithms. Through harvest-now, decrypt-later (HNDL) attacks, adversaries can collect encrypted information now with the expectation that future quantum computers will eventually be capable of decrypting it. Similarly, trust now, forge later (TNFL) attacks create risk when adversaries capture digitally signed assets today with the expectation that future quantum capabilities could enable them to forge signatures and undermine the trust those assets rely on later. For organizations managing sensitive data with long-term value, the risk horizon begins long before a cryptographically relevant quantum computer arrives.



63% are extremely or very concerned about the threat of HNDL attacks

60% are extremely or very concerned about TNFL attacks

[Q14]

In comparison, 66% 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.

Just as importantly, the transition itself is expected to take years. Organizations must identify where cryptography is used, assess vulnerable systems, evaluate vendor readiness, test replacements, and deploy new technologies at scale. For many organizations, the migration to PQC is likely to be a complex undertaking that will take longer than the arrival of the threat itself.

The 2026 findings indicate that organizations are beginning the initial stages of that migration [Q10]:

Only **38%** report having fully assessed systems vulnerable to quantum computing attacks, up from 14% in 2025

Another **44%** say their assessment is mostly complete, while 14% have completed a partial assessment

This is one of the strongest signs that PQC planning is becoming operational. Together, the findings indicate that a substantial majority of organizations have begun the foundational work required to understand their exposure. Assessment turns an abstract threat into an actionable map: Which systems use RSA or ECC, what data must remain confidential, which certificates and keys support critical services, which vendors control migration timelines, and where replacement will be technically difficult.

Investment intent remains high:

83% have budget allocated to quantum-safe security initiatives over the next year [Q11]

Among those with budgets, 93% expect PQC investment to increase over the next two to three years, including 40% expecting an increase of 5% or more [Q12]

External timelines are getting harder to ignore

Organizations do not control the timeline for PQC adoption entirely themselves. Governments, standards bodies, national cybersecurity agencies, and major technology providers are establishing their own transition milestones, and those dates increasingly converge around the end of this decade.

The timelines vary in scope. Some apply to government or national security systems, some prioritize critical infrastructure, and others represent technology-provider roadmaps rather than regulatory mandates. But collectively, they create a clear planning horizon: Cryptographic discovery, testing, and migration must begin well before 2030.

These are not interchangeable mandates, nor do they apply equally to every organization.

Together, however, they show why waiting for a single universal deadline is risky. For multinational organizations and companies dependent on government, cloud, browser, security, and infrastructure providers, the earliest applicable milestone may become the effective operational deadline.

While these developments are often discussed separately, they are increasingly converging around the same planning horizon. Standards bodies such as NIST are defining the cryptographic algorithms that will replace RSA and ECC, the CA/Browser Forum is reducing certificate validity periods, and governments are establishing migration requirements for critical systems. Together, these changes reinforce a common message: Organizations need cryptographic infrastructure capable of adapting continuously, rather than responding to one-off transitions.

Government and industry signals are increasing the pressure to move towards PQC. NIST's transition plan requires organizations to begin transitioning, with legacy public-key algorithms officially deprecated by 2030 and fully disallowed by 2035. In June 2026, U.S. Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," was signed, directing federal agencies to transition information systems toward NIST-approved PQC standards and emphasized the present risk of adversaries collecting sensitive information for later decryption.

- **December 31, 2030:** Federal high-value assets must migrate to PQC for key establishment/encryption.
- **December 31, 2031:** Federal high-value assets must migrate to PQC for digital signatures.

Major technology providers are also setting more aggressive internal targets.

In March 2026, Google announced a 2029 timeline for PQC migration, citing risks to encryption and digital signatures, and prioritizing quantum-safe authentication services. Cloudflare followed with a target to become fully post-quantum secure, including authentication, by 2029.

70% were aware of Google's accelerated timeline before taking the survey



Yet that leaves **three in ten** organizations were not aware of one of the industry's most visible PQC migration signals.

[Q13]

Despite growing momentum, awareness gaps remain. For organizations dependent on cloud, browser, platform, security, and infrastructure vendors, external roadmaps can reshape technical requirements well before a formal regulatory deadline arrives.

The challenge extends beyond an algorithm swap

PQC migration is often described as replacing vulnerable algorithms with quantum-resistant alternatives. In practice, the change reaches much further. PKI is the system that turns cryptography into operational trust by supporting certificates, authentication, encrypted communications, code signing, and machine identity. If post-quantum keys and signatures are larger or behave differently, the infrastructure that issues, transports, validates, and manages them must adapt as well.

Respondents recognize the scale of that change:

78% believe today's PKI will need to change to a great or very great extent to support PQC

Virtually no respondents believe the current PKI model can remain unchanged as organizations move toward a post-quantum future.

[Q9]



The finding suggests a growing understanding that PQC is not simply a cryptography project but a trust infrastructure project. For many organizations, that infrastructure extends far beyond publicly trusted TLS certificates to include private PKI systems supporting workforce identity, machine identity, code signing, network authentication, and internal applications. This shift is already driving interest in new approaches to digital trust. Rather than focusing solely on quantum-resistant algorithms, the industry is increasingly exploring how the underlying PKI itself may need to evolve to support a post-quantum world.

Merkle Tree Certificates (MTCs) point to the architectural choices ahead

MTCs and the Future of PKI

As organizations prepare for PQC, attention is expanding beyond algorithms to the future of PKI itself. One emerging concept attracting attention is MTCs, a proposed certificate architecture currently being developed through the Internet Engineering Task Force (IETF).

What is an MTC?

An MTC is a new kind of server certificate designed to keep secure connections fast in the coming era of quantum computers. Today, a website server proves its identity by presenting a certificate that carries several digital signatures, and the quantum-resistant versions of those signatures are so bulky they would slow down every secure connection on the internet. An MTC solves this by having the certificate authority record everything it issues in a public, tamper-evident log, organized as a Merkle Tree.

Rather than carrying heavy signatures, the website presents a short trail of digital fingerprints showing its certificate sits in that log, and the browser checks the trail against a summary of the log it already received through its normal software updates. The result is a certificate that stays small, stands up to quantum computers, and is publicly verifiable by default.

A single ML-DSA signature alone runs roughly 2.4 kilobytes; a Merkle inclusion proof typically comes in under a kilobyte. Cryptographers at Google and Cloudflare, with contributions from Sectigo, have been developing this approach specifically to keep the post-quantum internet fast without sacrificing security, and as a side effect, it makes Certificate Transparency logging inseparable from issuance itself, closing a blind spot in how certificates are monitored today.



Among respondents familiar with the proposed MTC architecture,

Only **40%** believe they have a clear understanding of what changes to their organizations' systems, processes, and environments would be required to support this new certificate type [Q16]

As post-quantum planning matures, the conversation is increasingly shifting from which algorithms organizations will use to how PKI and digital trust can scale efficiently in a post-quantum world. MTCs represent one example of the innovation and architectural thinking that may help enable that transition. Just as importantly, the findings suggest that even among organizations familiar with the proposed MTC architecture, there is still significant uncertainty about what changes to their systems, processes, and environments would be required to support it.

Confidence must be tested through execution

The findings throughout this chapter point to an interesting dynamic. Organizations increasingly recognize that PQC is not simply an algorithm replacement exercise. Most expect meaningful changes to PKI, many are actively assessing quantum-vulnerable systems, and external migration timelines continue to accelerate. Yet despite the scale and complexity of the work ahead, confidence remains remarkably high.

The question is whether that confidence reflects genuine readiness or organizations still underestimate the operational realities of large-scale cryptographic transformation.

28% are extremely confident their current systems can integrate PQC without major disruption, up from 15% in 2025. Another 46% are very confident [Q15]

That confidence is a positive signal, but it should be tested against implementation evidence. At the end of the day, the goal should not be confidence in a roadmap. It should be demonstrated migration capability: Complete cryptographic inventory, prioritized systems, tested algorithms, vendor commitments, documented rollback, measurable performance, and an operating model that can change again if standards or threat assumptions evolve.

Shorter certificate lifespans are testing operations now

The transition is already visible in renewal workloads

PQC may be the largest architectural transformation ahead, but shorter certificate lifespans are the pressure organizations are already feeling.

The 47-day certificate era is a transition already in motion. On March 15, 2026, the maximum validity period for publicly trusted TLS certificates fell from 398 days to 200 days, requiring certificate renewals every six months. It will fall again to 100 days, or renewals every three months, on March 15, 2027, before reaching 47 days on March 15, 2029. The reuse period for domain control validation will also shrink to just 10 days in 2029. The operational model that supported annual certificate renewals is being dismantled in stages and will place significantly greater demands on existing processes.

The practical consequence is not simply more renewals. Shorter lifespans reduce the margin for errors across validation, issuance, deployment, monitoring, and revocation. A missed step that was recoverable within an annual cycle can become an outage when the same process repeats every few weeks.

Visibility is improving, but outages reveal the work is not done

The foundation of any certificate management strategy is knowing what certificates exist, where they are deployed, who owns them, and when they expire. On that measure, organizations report significant improvement. Confidence in tracking has also risen alongside visibility.

62% say they have a complete, up-to-date inventory of all public SSL/TLS certificates, more than doubling from 28% in 2025 [Q1]

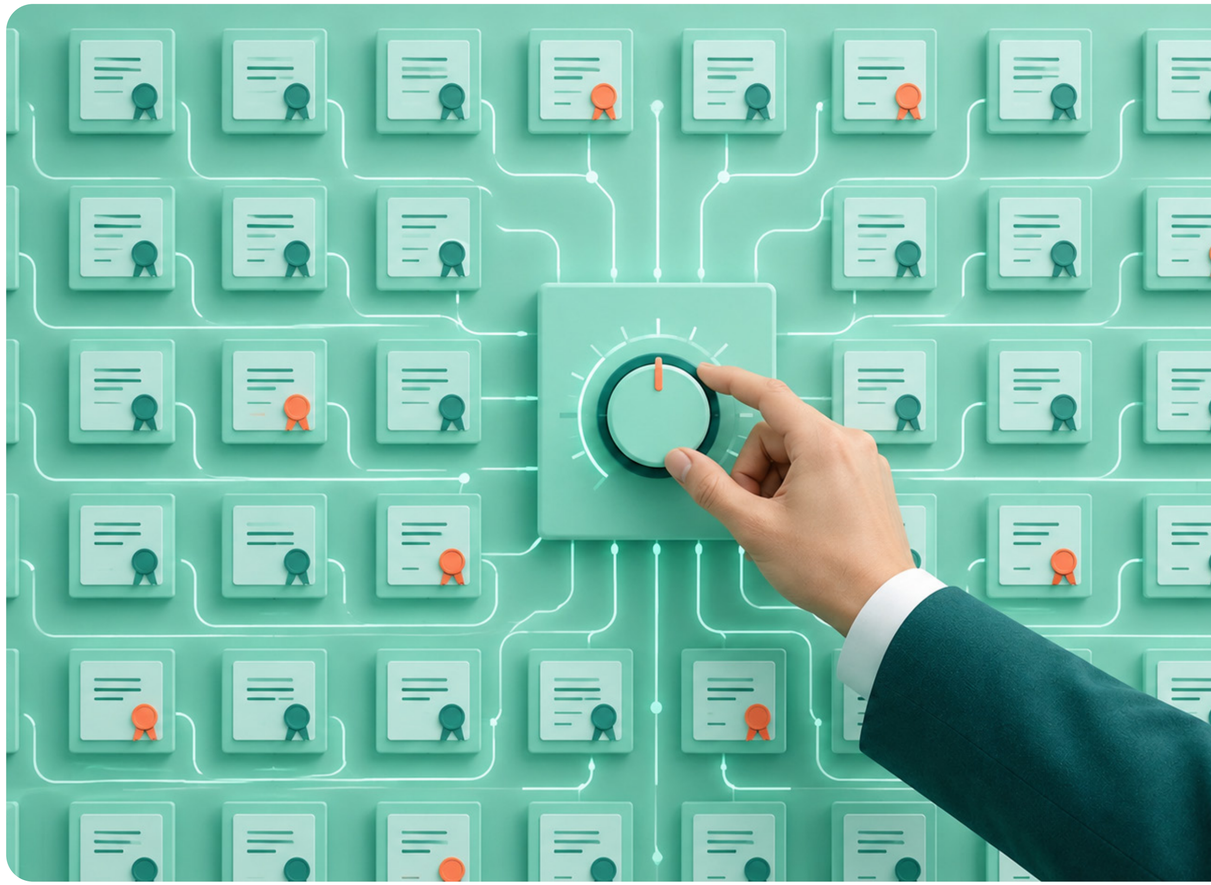
33% are extremely confident they are tracking all certificates, including rogue certificates, up from 13% in 2025 [Q2]

This progress matters

Certificate discovery and inventory create the foundation for management. You simply can't manage what you don't know you have. But visibility alone does not eliminate risk. Organizations may have a clearer picture of their certificate environments than they did a year ago, yet operational failures and outages remain common.

61% experienced a certificate-related outage or incident in the past 12 months [Q3]

The result sits uneasily besides the sharp rise in reported visibility and confidence. The data shows that visibility alone is not enough. Organizations also need reliable renewal, validation, issuance, deployment, monitoring, and revocation. If those processes remain disconnected, simply having a complete inventory may be insufficient to prevent operational risk.



Preparedness and concern are rising together

The good news is that general feelings of preparedness to handle monthly certificate renewals grew significantly year-over-year. At the same time, concern about the operational impact of shorter certificate lifespans also increased. Rather than signaling conflicting views, these findings suggest organizations are developing a more realistic understanding of what the transition entails. As teams move from planning to implementation, they gain a clearer view of the dependencies, exceptions, and potential failure points that accompany more frequent certificate changes.

40% of organizations now describe themselves as very prepared to manage monthly renewals because they already have automated systems in place, up from 19% in 2025 [Q4]

94% have some degree of concern about the impact of 47-day certificate lifespans on their organization [Q5]

61% are very or extremely concerned about the impact of 47-day certificate lifespans on their organization, an increase from 52% in 2025.

Shorter certificate lifespans do not simply create more renewals. They reduce the margin for error. Failed validation, issuance, deployment, or revocation that have been manageable under annual renewal cycles become far more consequential when certificates are renewed every few weeks. As renewal windows shrink, even organizations that feel prepared are recognizing the operational discipline required to sustain certificate management at scale.

Automation must extend across the lifecycle

Last year, we explored how continued reliance on manual certificate management raised serious operational concerns and highlighted the need for greater automation. One year later, the conversation has evolved. The challenge has now progressed to how to automate effectively across increasingly complex environments.

Automation within certificate management is expanding, but not uniformly. While certificate renewals remain the most automated certificate management task, organizations are increasingly extending automation into other areas of the certificate lifecycle.

Automation of provisioning, deployment, revocation, and domain control validation (DCV) all saw year-over-year gains, suggesting organizations are beginning to view certificate management as more than a renewal problem [Q6]:

- Provisioning has increased **to 40% from 32%**
- Deployment has increased **to 42% from 33%**
- Revocation has increased **to 37% from 27%**
- DCV has increased to **42% from 32%**

That broader growth is encouraging because renewal alone does not complete the certificate lifecycle. A certificate can renew successfully and still cause an outage if it is not deployed to the correct endpoint, if an application reload fails, if a private key is mishandled, or if validation requires a manual intervention that no one completes on time.



Nearly three-quarters
73%
plan to increase certificate management automation because of shorter lifespans.

But only
4%
say they are already fully automated.

[Q7]

For most organizations, the next stage is not simply adopting an automation tool. It is connecting discovery, policy, issuance, validation, deployment, monitoring, revocation, and reporting into a governed operating model that provides visibility and consistency across the entire certificate lifecycle.

Agentic AI creates a new digital identity imperative

Autonomous action requires accountable identity

PQC and shorter certificate lifespans are not the only forces changing cryptographic operations. Agentic AI introduces a new class of non-human identity (NHIs) that functions as autonomous digital workers rather than static service accounts.

Traditional machine identities already outnumber human identities in many enterprise environments. Agentic systems raise the stakes, in particular with governance, because an identity may not simply authenticate to a service; it may act on behalf of a person, application, team, or organization. The security challenge is therefore not only determining whether an agent is legitimate; it is establishing what the agent is authorized to do, who delegated that authority, which credentials it can use, how long those credentials remain valid, and how actions can be traced and revoked.



The risk is action without trustworthy identity

An AI agent does not have to be malicious to create damage. A legitimate agent may take unintended action because its instructions, context, or permissions are flawed. But at the same time, an attacker may also impersonate an agent, steal its credentials, alter its instructions, or exploit excessive privileges. Without strong identity and policy controls, organizations may struggle to distinguish an authorized autonomous action from abuse. Concern about identity-based attacks against agentic AI is already on par with the quantum-era threats examined in Chapter 1.

Nearly two-thirds of organizations

65% are extremely or very concerned about attacks on agentic AI systems involving identity spoofing, impersonation, or misuse of digital credentials [Q17]

While PKI can provide an important foundation for agent identity because it binds identities to cryptographic keys and enables authentication, it will still require more than simply issuing another long-lived certificate. Agent identities may need to be short-lived, scoped to a specific task, bound to a workload and execution environment, and governed by policies that limit delegation.

Agents may be granted privileged identities to perform approved tasks, but they should not be able to request or assign those privileges to themselves. Credentials would need to be rotated automatically and revoked quickly. Logs would need to be preserved with a verifiable chain between the human or system that delegated authority, the agent that acted, the tools it used, and the outcome it produced.

Applied correctly, cryptographic identities can help systems verify which agent is connecting, which organization or workload authorized it, and whether a request has been altered.

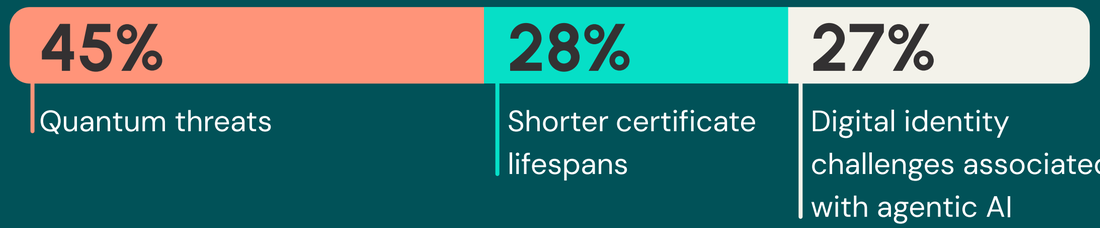
Treating agent identity as a separate AI-security project risks creating another silo. The capabilities needed for shorter certificate lifespans and PQC migration, including discovery, automated issuance, short-lived credentials, policy-based lifecycle management, algorithm flexibility, centralized visibility, and rapid revocation, will also support trusted agent operations.

Conclusion

Turn awareness into a repeatable operating model

The defining insight of this year's research is not a single statistic. It is the convergence of multiple cryptographic transformations. PQC is forcing organizations to reassess algorithms and architecture. Shorter certificate lifespans are increasing operational frequency and reducing tolerance for manual processes. Agentic AI is expanding the number and complexity of identities that must eventually be authenticated and governed. Whether those identities are public-facing certificates, internal systems, machines, users, workloads, or AI agents, they increasingly depend on the same underlying trust infrastructure.

Organizations face competing cryptographic priorities. When asked to rank these three challenges based on which they believe poses the highest risk to their organization, quantum threats emerged on top [Q18]:



Those priorities may compete for budget and attention, but addressing them requires many of the same underlying capabilities, and that overlap creates an opportunity. Instead of building three disconnected programs, organizations can use each initiative to strengthen a shared digital trust foundation. The research shows that organizations already recognize an important connection between two of these challenges:

96% see at least some overlap between readiness for shorter certificate lifespans and PQC [Q8]

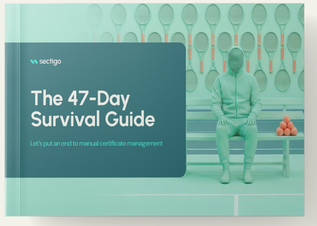
While this finding specifically connects certificate lifespans and PQC, that recognition provides a starting point for a more coordinated operating model, one that can also support the emerging identity demands of agentic AI.

The practical lesson is to invest in capabilities that remain useful as requirements change: Complete discovery, end-to-end automation, centralized policy, algorithm flexibility, rapid revocation, vendor accountability, and measurable resilience.

The industry has moved beyond awareness. The next stage is action that can be repeated, tested, and scaled. Crypto agility is the discipline that makes that possible.

Resources

Moving from awareness to a repeatable operating model starts with practical guidance. Explore these Sectigo resources to help connect your priorities, shape your next steps, and build a stronger digital trust foundation, connecting near-term certificate management needs with longer-term cryptographic readiness.



The 47-Day Survival Guide

Prepare for shorter certificate lifespans with guidance on automation and certificate management to help maintain trust and avoid disruption.

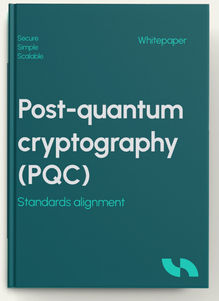
Download the guide



Merkle Tree Certificates eBook

Learn how the IETF is developing Merkle Tree Certificates, how they work, and why they make certificate automation essential.

Download now



PQC Standards Alignment

Understand how NIST standards, CA/B Forum rulings, and federal timelines are shaping cryptographic planning and certificate management.

Explore the whitepaper



Sectigo Orchestration Gateway eBook

Explore how centralized, automated SSL/TLS certificate management can help address shorter certificate lifespans and reduce outage risk.

Download the eBook

Methodology

Censuswide collected 500 survey responses in July 2026 from C-level, vice-president, and director-level leaders in IT, technical operations, cybersecurity, and risk across a mix of industries and business sizes in North America, EMEA, and APAC. Data was collected from July 2 to July 21, 2026.

The 2026 research expanded its geographic scope to include APAC respondents, including participants from India, Australia, New Zealand, and Singapore. Because the 2025 and 2026 samples are not strictly like for like, year-over-year comparisons should be interpreted as directional indicators rather than precise measures of market-wide change. Percentages may not total 100% because of rounding. Questions allowing multiple responses may total more than 100%.

About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM), helping organizations secure human and machine identities while reducing the hidden risks of modern digital trust. As certificate volumes grow and lifespans shrink, unmanaged certificates are becoming a source of outages, compliance exposure, and operational disruption. Sectigo uses Orchestrated Automation to deliver Simplicity at Scale through its cloud-native CLM platform, bringing visibility, control, and lifecycle management together across complex environments. With more than 700,000 customers, including 65% of the Fortune 500, Sectigo is one of the largest and longest-standing certificate authorities, with over 20 years of delivering unparalleled digital trust.

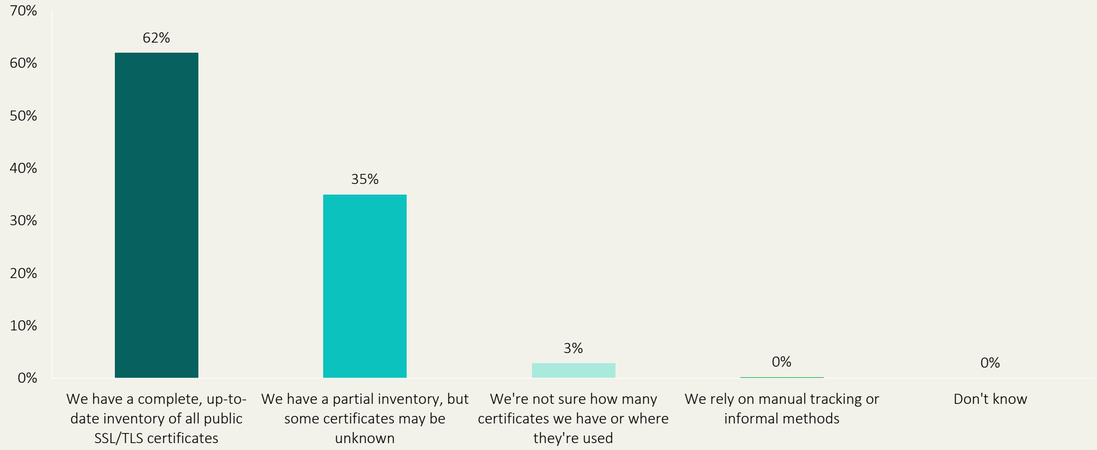
For more information, visit www.sectigo.com or follow us on LinkedIn.

Get in touch

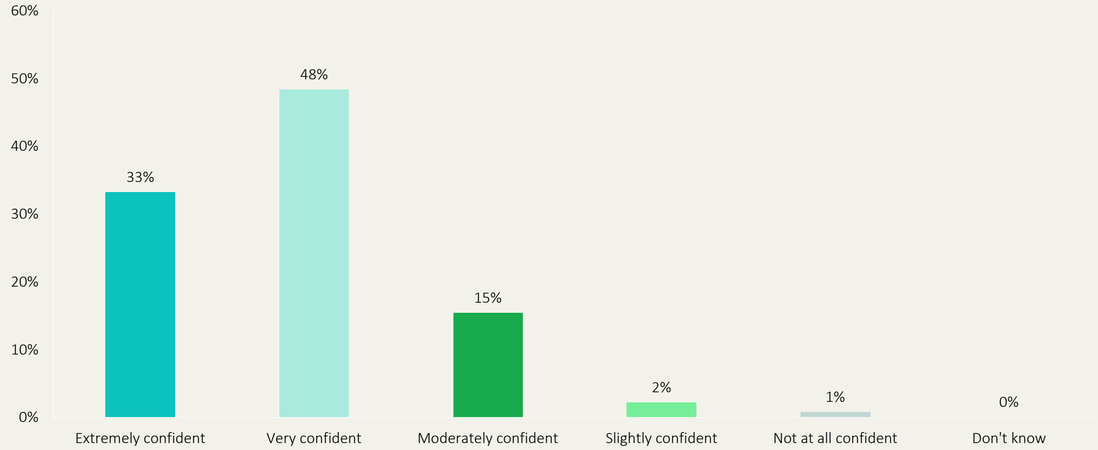
© 2026 Sectigo. All rights reserved.

Appendix

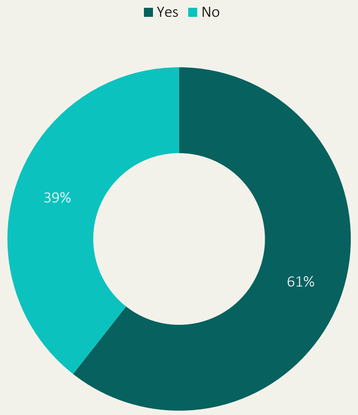
Q1. What best describes your organization's understanding and tracking of public SSL/TLS certificates currently in use?



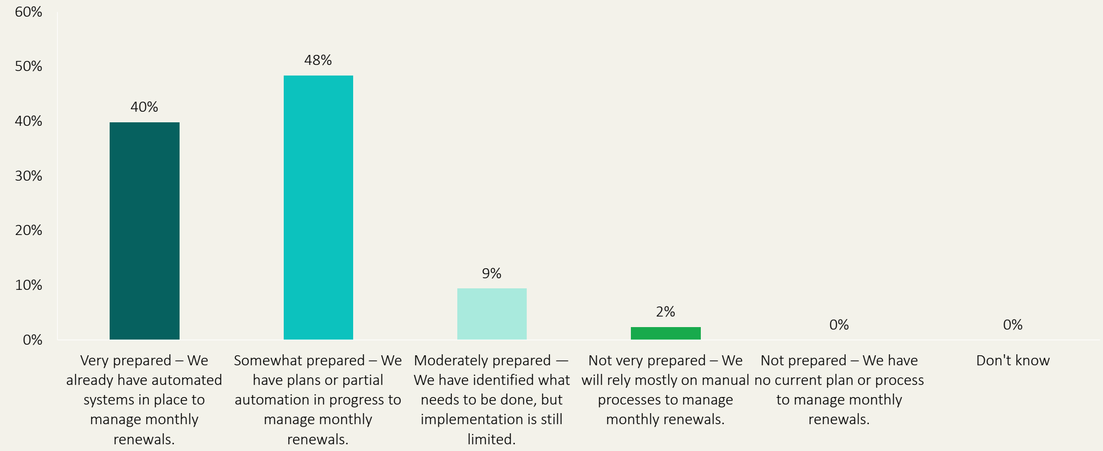
Q2. How confident are you that your organization is tracking ALL certificates, even rogue certificates?



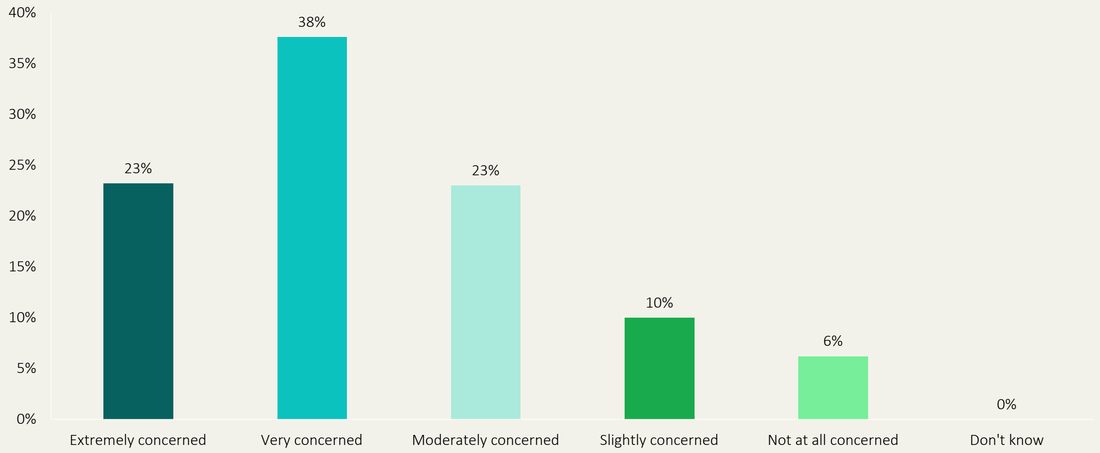
Q3. As far you are aware, has your organization experienced a certificate-related outage or incident in the past 12 months?



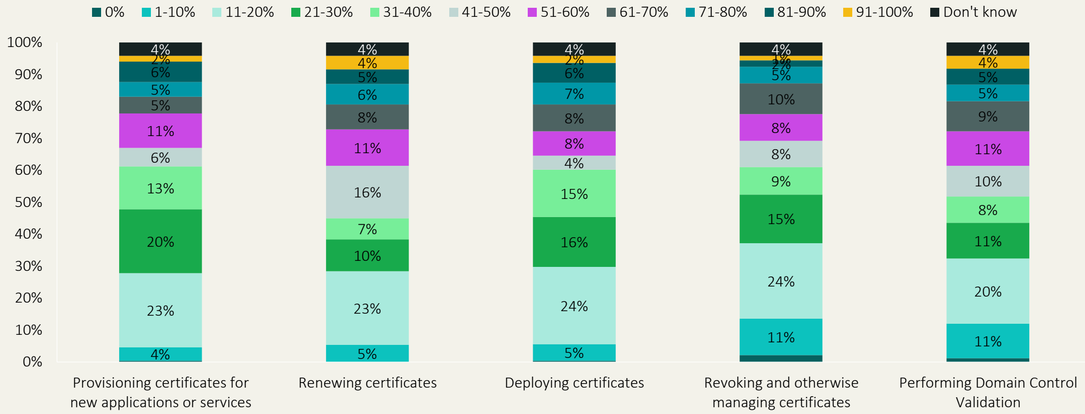
Q4. Industry guidelines will reduce the maximum validity period of public SSL/TLS certificates to just 47 days by 2029. How prepared is your organization to transition towards renewing all public SSL/TLS certificates on a monthly basis to satisfy this requirement?



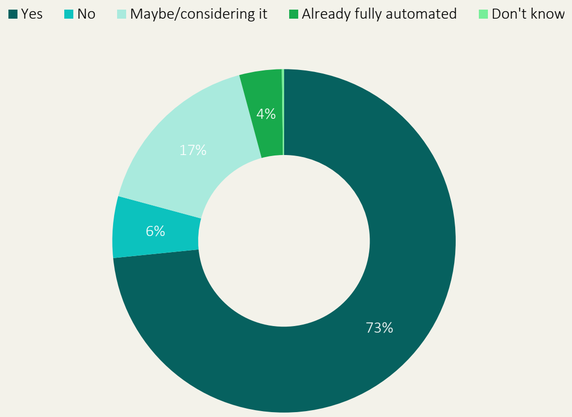
Q5. How concerned are you about the impact of 47-day certificate lifespans on your organization?



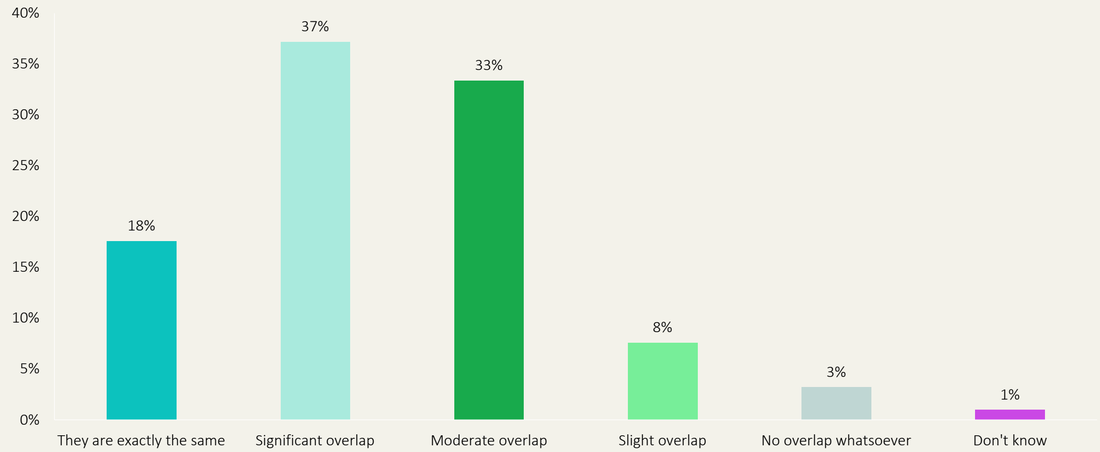
Q6. What percentage of your organization's SSL/TLS certificates are automated for each of the following tasks?



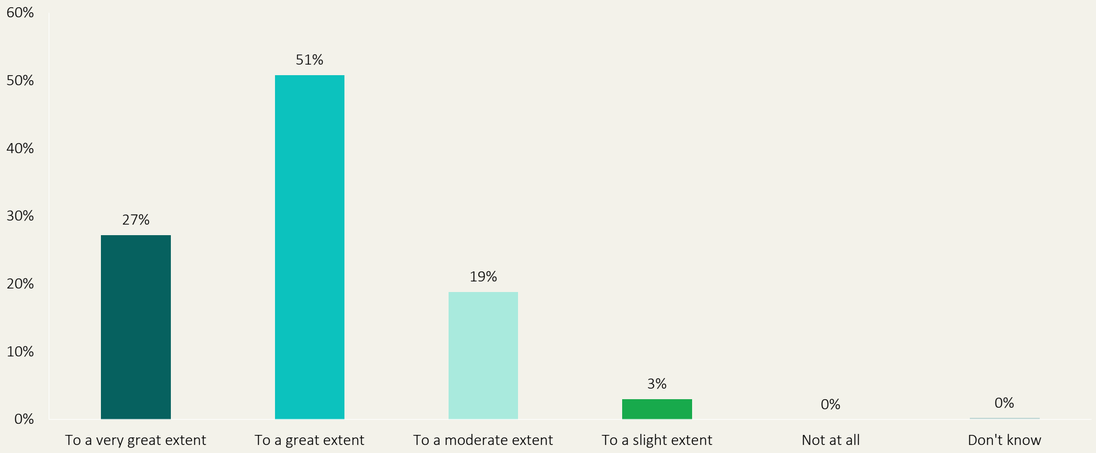
Q7. Are you planning to increase automation in certificate management as a result of shorter certificate lifespans?



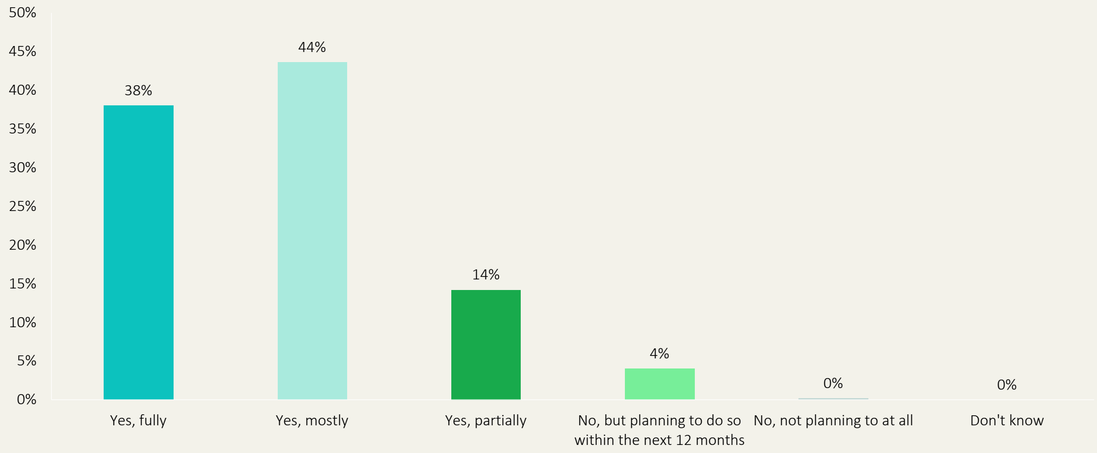
Q8. To what degree do you see overlap in your organization's preparedness for 47-day public SSL/TLS certificates and post-quantum cryptography?



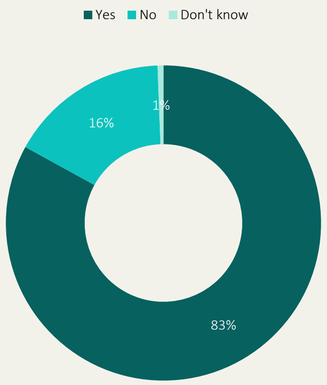
Q9. To what extent do you believe today's public key infrastructure (PKI) will need to structurally change to support post-quantum cryptography (PQC)?



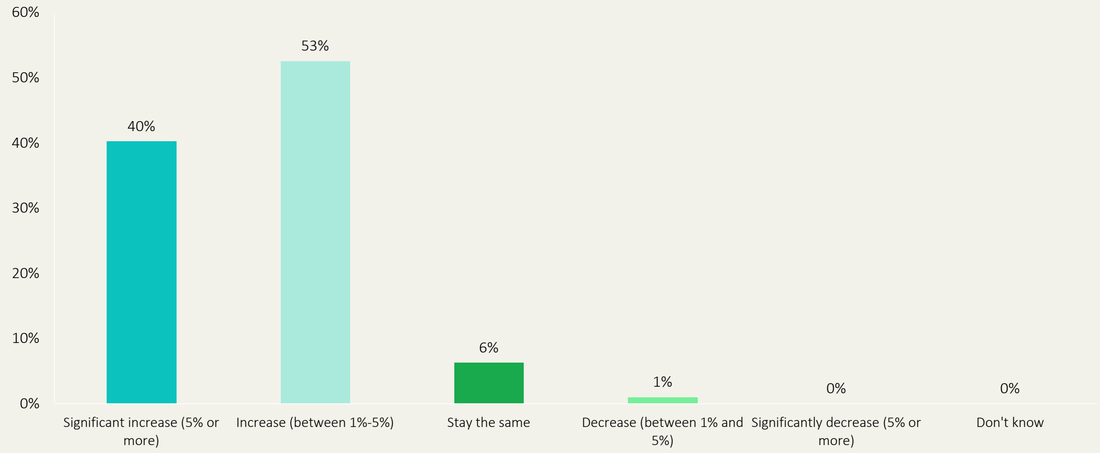
Q10. Has your organization conducted an assessment of systems vulnerable to quantum computing attacks?



Q11. Do you have a budget allocated to quantum-safe security initiatives over the next year?

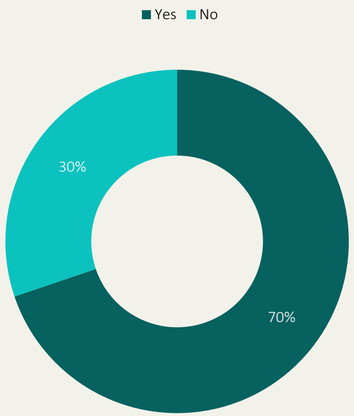


Q12. How do you expect your organization's PQC investment to change over the next 2-3 years?

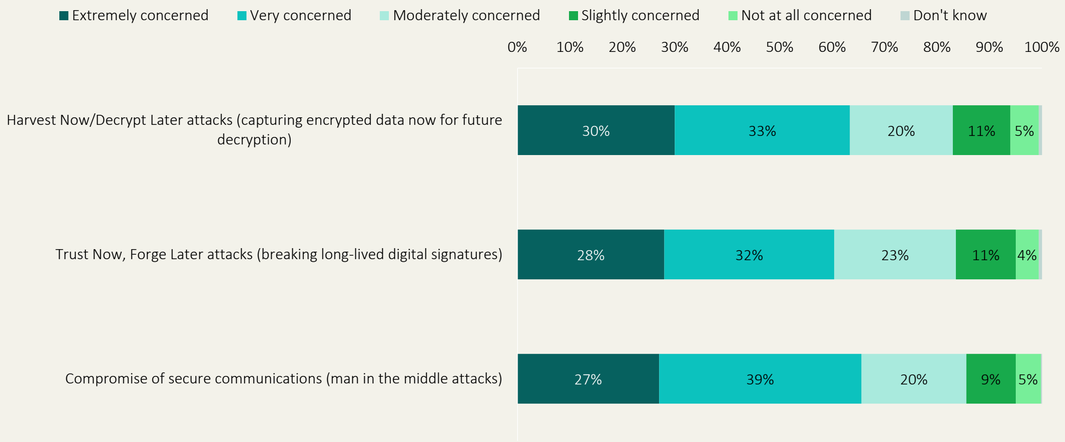


**Those who have a budget allocated to quantum-side security initiatives over the next year*

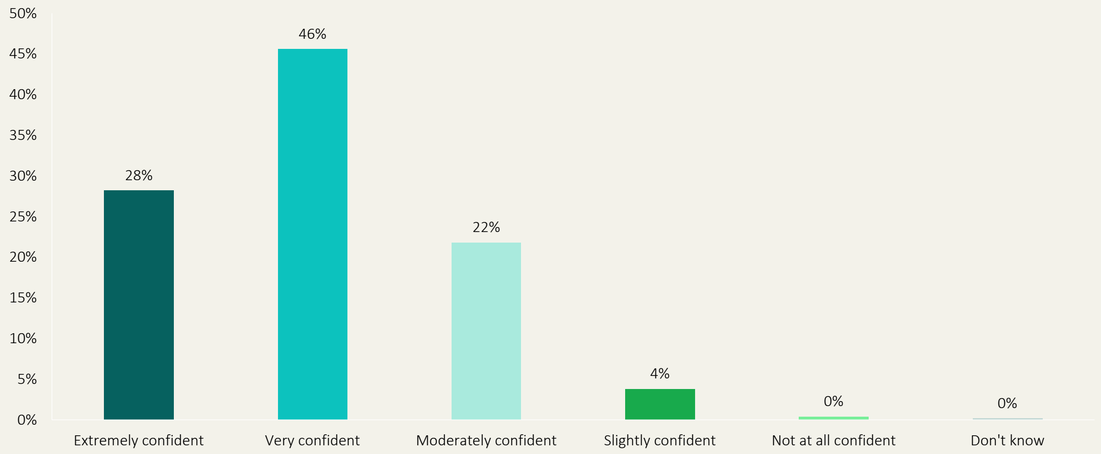
Q13. Before today, were you aware that Google has accelerated its internal PQC migration timeline to 2029?



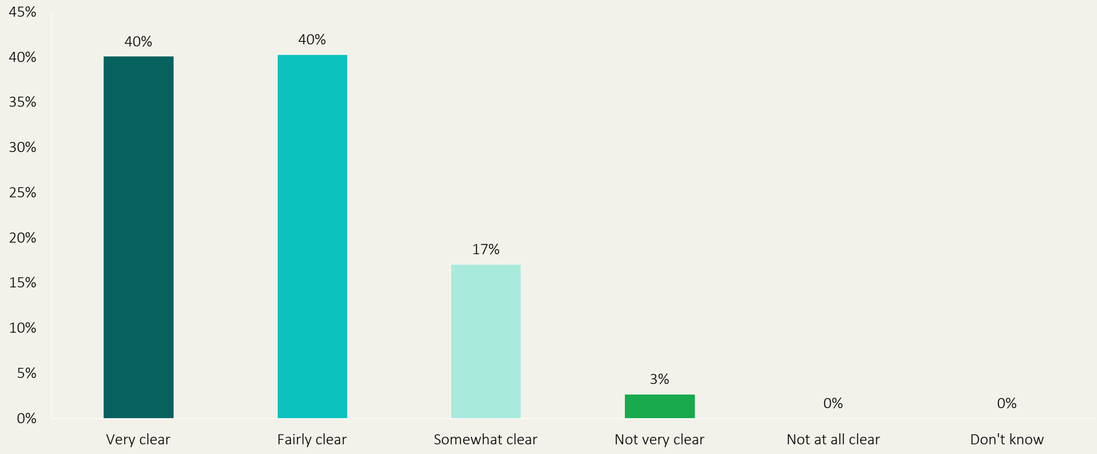
Q14. How concerned are you about each of the following quantum computing threats?



Q15. How confident are you in your current systems' ability to integrate PQC without major disruption?

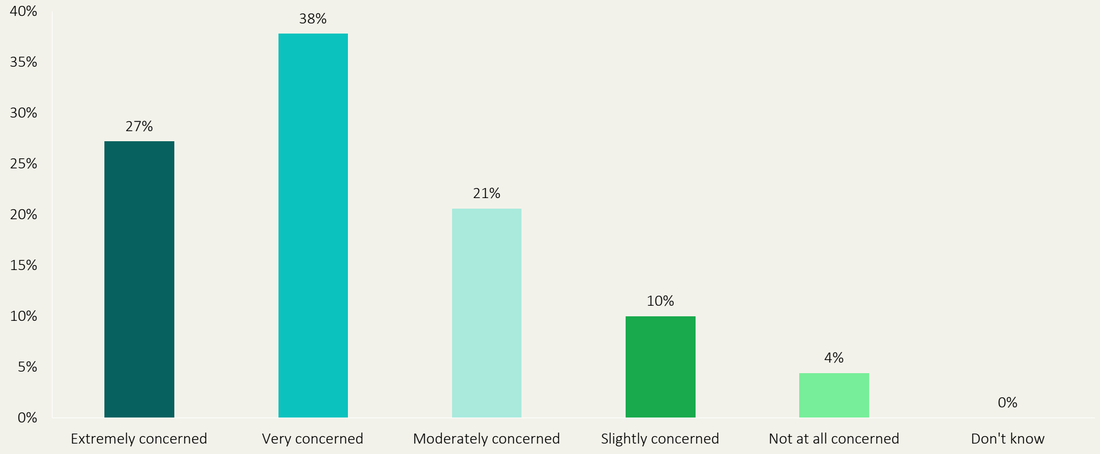


Q16. How clear is your organization on what changes will be needed across its systems, processes, and environments to support MTCs?



**Those who are familiar with Merkle Tree Certificates (MTCs)*

Q17. How concerned are you about attacks against agentic AI systems in your organization that use identity spoofing, impersonation, or misuse of digital credentials?



Q18. Rank the following based on the level of risk you believe they pose to your organization where 1 = Highest Risk and 3 = Lowest Risk:

