2026 Global State of Post-Quantum and Cryptographic Security Trends

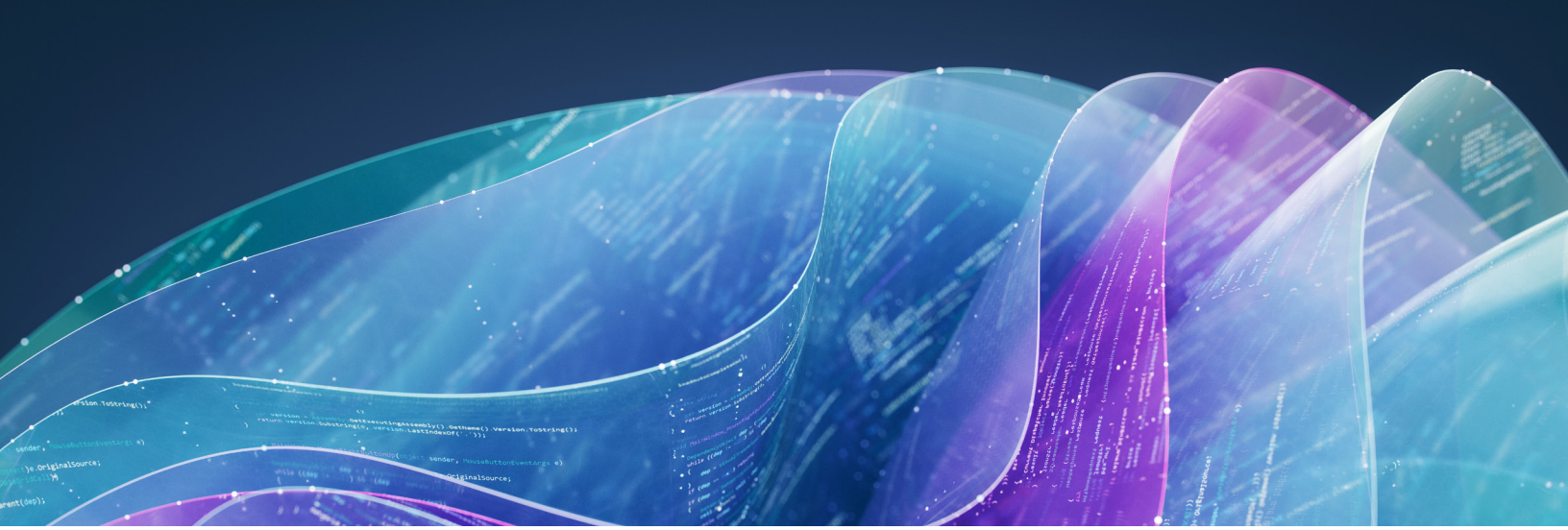
JANUARY 2026

SPONSORED BY ENTRUST

Independently conducted by Ponemon Institute LLC

ENTRUST
SECURING A WORLD IN MOTION

Ponemon INSTITUTE



Contents

ENTRUST

FOREWORD

Cryptographic Security Is at a Tipping Point

Cryptographic security has quietly become one of the most critical – and least visible – foundations of modern business. It underpins identity, access, data protection, and system availability across every digital interaction. Yet today, that foundation is under unprecedented strain. External mandates, accelerating threat timelines, and expanding cryptographic sprawl are converging faster than most organizations can adapt.

This year's study examines how organizations are responding to these shifts. Enterprises face immediate operational pressure from rapidly shortening certificate lifecycles, growing volumes of keys and secrets, and increasingly fragmented cryptographic ownership across hybrid environments. Furthermore, the post-quantum (PQ) threat is no longer theoretical. Organizations are being asked to prepare for the eventual failure of RSA and ECC encryption – while still maintaining security, uptime, and compliance today.

What makes this moment especially challenging is not any single change, but the compounding effect of many changes happening at once. Short-lived certificates dramatically increase operational workload. PQ migration introduces new architectural and governance complexity. Expanding use of encryption across cloud, DevOps, and Zero Trust initiatives multiplies key volumes. And limited visibility across cryptographic assets makes all of this harder to manage. Together, these forces are transforming cryptographic security to a tipping point – where legacy approaches can no longer keep pace.

In the 2026 Global State of Post-Quantum and Cryptographic Security Trends, we asked the Ponemon Institute to examine how organizations are navigating this convergence of pressures. Drawing on insights from 4,149 senior IT, security, and risk leaders, across the United States, United Kingdom/Ireland, Canada, DACH, Indonesia, and Singapore, the report reveals where readiness is advancing, where it is falling behind, and why visibility, governance, and crypto-agility have become essential capabilities for resilience in the years ahead.

The Quantum Threat Is Here, But How Prepared Are We?

Against the backdrop of rising operational strain, the post-quantum threat adds a new and urgent dimension. While PQ often dominates headlines, the study shows it's colliding with existing cryptographic challenges – not replacing them.

From "harvest now, decrypt later" style attacks that target long-life data and devices to the availability of NIST post-quantum cryptography (PQC) standards, the PQ era is effectively here. Indeed, 24% of global respondents expect the arrival of cryptographically relevant quantum computers (CRQCs) that will break traditional public key cryptography such as RSA and ECC within 10 years, with a resounding 51% forecasting that this will happen in as soon as five years.

Quantum-safe encryption, also referred to as PQC, is the use of new cryptographic algorithms for the continued protection of our digital universe from this imminent quantum threat. General global guidance is that high-priority systems must be migrated to PQC by 2030 or 2031, with all systems migrated by 2035. Yet only 36% of respondents cite government policy and public-private coordination on quantum readiness as more than adequate today.

In the U.S., the NSA, NIST, and CISA are all urging organizations to start their migration now. The NSA has advised that all U.S. national security systems will be quantum-safe by 2033. Also, NIST's initial

public draft of the Transition to Post-Quantum Cryptography Standards, or NIST Interagency Report 8547, states the intent to deprecate classical asymmetric algorithms – like RSA – by 2030, then fully disallowing them by 2035.

EU-specific guidance is that organizations perform a quantum threat analysis by 2026, migrate all high-risk use cases to PQC by 2030, and transition all medium-risk use cases by 2035. In the UK, the National Cyber Security Centre (NCSC) has advised organizations to complete a full cryptographic inventory and PQC migration plan by 2028, migrate critical systems and highest priority data to PQC by 2031, and complete their migration by 2035.

Despite strong government guidance, only 38% of organizations report that they are actively preparing for PQ, which is also a slight 3% year-over-year drop. Yet half of respondents also indicated that a quantum attack would have a serious impact on their organization and industry, including 58% that thought such an attack could result in the loss of access to encrypted critical infrastructure and 59% expressing concern over the exposure of long-term sensitive data such as health records and trade secrets.

Crypto-Agility Is the Foundation of PQC Migration

For organizations actively preparing for PQ, progress varies significantly. While many have begun building cryptographic strategies, far fewer have established the foundational crypto-agility needed to execute those plans at scale. Of those actively preparing for PQ, 44% are building their cryptographic strategy, while 32% are compiling their cryptographic inventory and/or ensuring organization crypto-agility. The latter represents a 5% year-over-year drop, signaling that the biggest challenge to attaining quantum resistance today is a lack of crypto-agility. Only 26% of organizations report having a fully implemented crypto-agility strategy, with another 31% having a partially implemented one.

This inability to discover, or inventory, an organization's cryptographic estate including algorithms, protocols, libraries, keys, and dependencies like APIs and third-party integrations makes it extremely difficult to transition from one cryptographic system to another without impacting all the infrastructure around it. Typical blind spots include legacy systems, shadow IT, and supply chain partners. Quite simply, you can't migrate what you can't see. Indeed, 41% of respondents say that the inability to improve visibility into their cryptographic inventory is their top impediment to attaining quantum resistance, roughly on par with 43% last year. Use of a Cryptographic Security Platform (CSP) to unify cryptographic hardware, software, and credentials can be invaluable to this effort and will also help keep the inventory current, essentially providing a living cryptographic bill of materials.

Changing Pain Points on the Path to Quantum Resistance?

Two other concerns respondents cited on their path to quantum resistance that have significantly increased in relative importance year-over-year are a lack of adequate budget (39% vs. 31%) and insufficient in-house expertise (38% vs. 28%). However, these shifts likely have less to do with real increases in importance and more to do with previous concerns being somewhat mitigated over the past year. Respondents reported decreased concern over not having the right scale and technologies to support the extra computing power required by new algorithms (31%, down from 38%) which is likely related to rapid developments in the power and scale of AI over the past year. Also, there

was decreased concern regarding the security of new cryptographic algorithms (32%, down from 40%) that likely reflects an increased comfort level with the NIST PQC algorithms that have been available since August 2024.

DACH Overtakes U.S. Lead in PQ Preparedness

38% of organizations globally are actively preparing for PQ – ranging from a high of 45% in the DACH to just 31% in the UK/Ireland. Last year, the U.S. led the global pack in PQ preparedness at 48% but has since declined to 40%, and while still second overall this eight-point drop puts it significantly behind organizations in the DACH region. One possible explanation is that organizations in the DACH region are subject to more stringent European privacy laws, creating added urgency to attain quantum resistance.

The quasi-good news is that another 29% globally have at least evaluated the potential impact of PQ, ranging from a high of 31% in the U.S. and Singapore to a low of 26% in Indonesia. However, it is more than a little disconcerting that 31% of organizations have not even considered the potential impact of the quantum threat. Yet those who report being entirely unsure if/what to do regarding PQ has dropped significantly from 9% to 2% year-over-year.

On the Road to Quantum Resistance

Of those preparing for PQ, 38% are testing PQC while 33% are implementing PQC. Respondents are relatively evenly split between the adoption of a hybrid approach that combines PQC with traditional public key cryptography (36%) vs. pursuing a pure PQC approach (35%). Of note here is NIST's initial public draft of the Transition to Post-Quantum Cryptography Standards (draft NIST IR 8547) that provides a structured framework for organizations to seamlessly realize quantum-safe encryption by applying a hybrid migration approach.

Cryptographic Security Management Becomes an Urgent Priority

Beyond post-quantum readiness, the study reveals foundational weaknesses in how organizations inventory, manage, and govern cryptographic assets today. With an intensifying threat landscape and more data, devices, and people to secure, CISOs and their teams are feeling the crunch. Only 43% of respondents indicate that their organizations have a full data inventory that identifies where data resides and flows, who has access, and how it is used, while 25% are in the process of compiling such an inventory. Plus, less than half of respondents (48%) report that their organizations have steps in place to secure confidential data for more than 10 years.

Similarly, just 43% of global respondents say they have complete visibility of their cryptographic estate, ranging from a high of 53% in Canada to a low of 33% in the DACH region. The latter being somewhat surprising given that this region leads in global PQ preparedness according to those surveyed, as mentioned above. Only 43% report having full or complete visibility into certificates across their organization and just 40% have full or complete visibility into keys and secrets.

Over two-thirds of respondents (68%) cite the management of cryptographic assets as either extremely or very difficult. Common concerns include insufficient staff (45%), lack of skilled personnel (42%), isolated and fragmented systems (41%), difficulty building an accurate inventory of keys, secrets, and certificates (37%), and no clear ownership (36%).

While organizations may feel they still have time to address these cryptographic inventory and management gaps, the CA/Browser Forum has removed any such buffer with the passage of Ballot SC081v3. These new rules phase TLS certificate maximum validity from 398 days today to a 47-day limit by 2029, including a staged rollout starting March 15, 2026! This change forces near monthly certificate renewals, making visibility and automation essential now.

Trends in Deployment of PKI and HSMs

Today, PKI is essential to establishing and maintaining trusted identities – user and machine – underpinning a Zero Trust approach.

Private cloud-based apps and mobile device authentications that use PKI credentials declined significantly year-over-year, while this year's top three cited applications using PKI credentials were private networks and VPNs (52%), SSL certificates for public-facing websites and services (50%), and document/message signing (45%).

At the same time, PKI technologies are perennially cited as a significant area of possible change and

Quite simply, you can't migrate what you can't see.

uncertainty. Consistent with last year's study, the top two reported sources of uncertainty are the evolution of PKI technology itself (49%), along with external mandates and standards (43%). Regarding the latter, current regulatory changes and national identity initiatives (eIDAS 2.0, digital identity wallets) are pushing PKI to support interoperable, auditable, and privacy preserving credentialing. The biggest year-over-year change here was budget being a top source of change/uncertainty for 42% of respondents, up 12% from the year before.

The No. 1 reported challenge to deploying PKI-enabled applications is that existing PKI is incapable of supporting new applications – cited by 46% of global respondents, up from 34% a year earlier. Meanwhile at 37%, unclear ownership topped the list again as the main challenge to deploying and managing PKI.

Consistent with ongoing skillset and resourcing shortages, organizational preference to use an internal corporate CA significantly declined year-over-year, from 60% to 46% with increasing reliance on third parties and managed services.

Same as last year, Common Criteria EAL Level 4+ was cited as the most important security certification when deploying PKI infrastructure by 54% of respondents, down marginally from 57% the year prior. FIPS 140-2 was the second most important certification; however, its importance has significantly declined year-over-year from 55% to 32%.

And the HSM party continues, with more organizations using HSMs (60% vs. 55% the year prior) and using HSMs to secure PKI (63% vs. 51% prior). The top two HSM use cases are database encryption and encryption and tokenization solutions, each cited by 49% of respondents. The top areas of HSM deployment to secure PKI are online roots and offline roots.

In general, PKI and HSM deployments are evolving from static on-prem systems to cloud-enabled and PQ-ready platforms that are automated and auditable with data-in-use protections to meet operational and compliance requirements.

Navigating the Year Ahead

With 47-day certificates and Q-Day on the horizon, coupled with an ever-intensifying threat landscape, cyber leaders need to prepare their organizations now. Central to this effort is compiling a full cryptographic inventory, improving crypto-agility, and advancing the organization's PQ journey in accordance with government and standards body guidance. Learn how Entrust can help you navigate the year ahead.

Introduction

Introduction

The purpose of this research is to provide important information about trends in post-quantum, cryptographic security, PKIs, and HSMs. Ponemon Institute surveyed 4,149 IT and IT security practitioners who are familiar with the use of these technologies in their organizations.

The countries in this research are the United States (552 respondents), United Kingdom/Ireland (573 respondents), Canada (396 respondents), DACH (553 respondents), Indonesia (369 respondents), and Singapore (482 respondents).

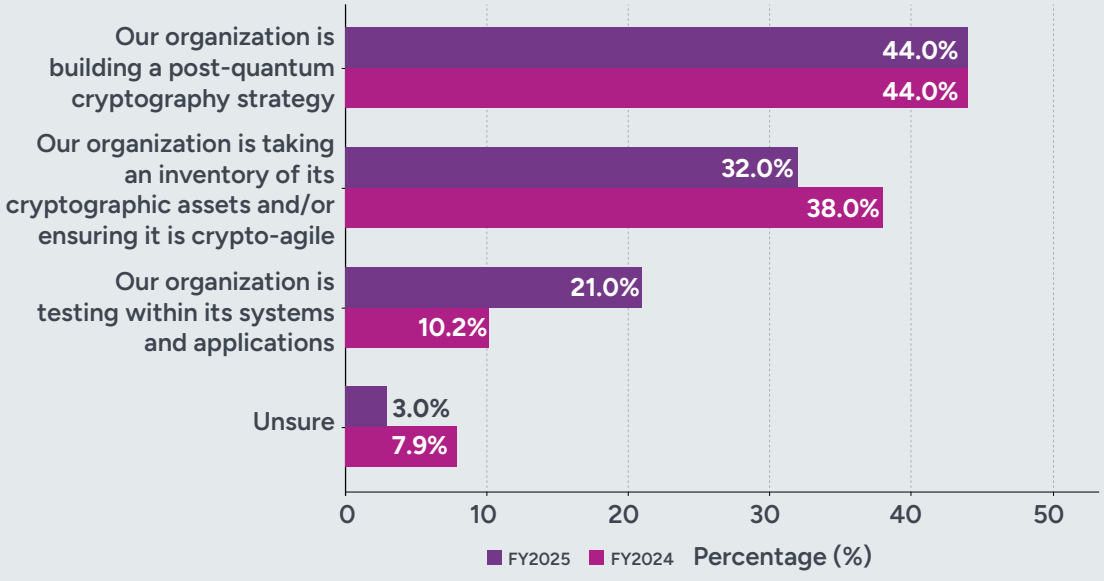
The post-quantum threat is coming quickly, but will organizations be prepared?

Quantum computing is a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers. The quantum threat, sometimes referred to as "post-quantum," is the inevitability that within the decade it will be capable of breaking traditional public cryptography such as RSA and ECC.

Only 38 percent of respondents say their organizations are preparing for the post-quantum threat, a slight decrease from 41 percent in last year's report. As shown in Figure 1, of these respondents, 44 percent from 2024 and 2025 are building a post-quantum cryptography strategy.

Thirty-two percent of respondents say their organizations are taking an inventory of its cryptographic assets and/or ensuring it is crypto-agile. This is a decline from 38 percent of respondents in last year's report. Testing within organizations' systems and applications increased significantly from 10 percent of respondents to 21 percent.

FIGURE 1. At what stage in preparing for the post-quantum threat is your organization?



The following summarizes the most significant research trends in post-quantum and cryptographic trends.

Organizations believe the PQ threat is imminent. Seventy-five percent of respondents agree and say a quantum computer will be capable of breaking traditional public key cryptography within 5 years (51 percent) or in five to 10 years (24 percent). Only 12 percent say it will never happen.

The biggest challenge to reducing the quantum threat and migration to post-quantum cryptography (PQC) continues to be the inability to improve the discovery/inventory of their organizations' cryptographic assets. Forty-one percent of respondents in this year's study vs. 43 percent of respondents in last year's study say the inability to improve visibility into their cryptographic assets is the greatest concern. Two concerns that have increased significantly are the lack of an adequate budget (39 percent in this year's study vs. only 31 percent in last year's study) and lack of in-house expertise (38 percent in this year's study vs. only 28 percent in last year's study).

Fifty percent of respondents say a successful quantum attack would have a serious impact on their organizations and industries. Fifty percent rate the potential impact as serious, but only 36 percent of respondents rate the adequacy of government policy and public-private coordination on quantum readiness as more than adequate. A successful quantum attack against organizations and industries could result in the loss of access to encrypted critical infrastructure (58 percent of respondents) and exposure of long-term sensitive data such as health records and trade secrets (59 percent of respondents).

The lack of visibility into the cryptographic estate, certificates, and keys and secrets puts organizations' cryptographic security at risk. Only 43 percent of respondents say their organizations have full or complete visibility into their organizations' cryptographic estate, only 43 percent of respondents say they have full or complete visibility into certificates across the organization, and only 40 percent say they have full or complete visibility into keys and secrets across the organization.

Private cloud-based applications and mobile device authentication applications that use PKI credentials declined significantly from 2024. Private cloud-based applications using PKI declined the most (56 percent of respondents in 2024 vs. 32 percent of respondents this year). Mobile device authentication decreased from 60 percent of respondents to 41 percent of respondents). The top applications using PKI credentials are private networks (52 percent of respondents), SSL certificates for public-facing websites and services (50 percent of respondents), and document/message signing (45 percent of respondents).

Internal corporate certificate authorities (CAs) are most often used to deploy PKIs but have declined since last year. Forty-six percent of respondents in this year's report use CAs to deploy PKI and 60 percent of respondents in last year's study. Business-partner-provided service increased the most, from 18 percent of respondents in last year's report to 40 percent of respondents in this year's study. Private CAs running within a public cloud increased from 21 percent of respondents last year to 37 percent of respondents this year.

The most important security certification when deploying PKI infrastructure is Common Criteria EAL Level 4+ (54 percent in this year's study vs. 57 percent of respondents in last year's study). The second most important certification is FIPS 140-2 Level 3. However, its importance has declined significantly, from 55 percent of respondents to 32 percent of respondents.

The biggest uncertainty and concern about the evolution of PKI are PKI technologies and external mandates and standards. When asked what the greatest areas of change and uncertainty to PKI will be, 49 percent of respondents say it is PKI technologies, an increase from 43 percent in 2024, and external mandates and standards, an increase from 37 percent of respondents in 2024. Budget and resources increased significantly to 43 percent of respondents vs. 30 percent of respondents.

More organizations use HSMs and use HSMs to secure PKI. Sixty-six percent of respondents in this year's research vs. 55 percent of respondents in last year's research say their organizations use HSMs. Sixty-three percent of respondents in this year's research vs. 51 percent of respondents in last year's research say their organizations use HSMs to secure PKI. Q36

The top areas of deployment to secure PKI are online roots and offline roots. According to last year's research, 47 percent said they are deployed to secure PKI in online roots and 42 percent said they are deployed to secure PKI in offline roots.

Key Findings

Key Findings

In this section we present the research results in detail. The report is organized according to the following topics. Whenever possible, trends in research findings from last year's Entrust study are included.

Post-Quantum: The Threat and the Readiness Journey

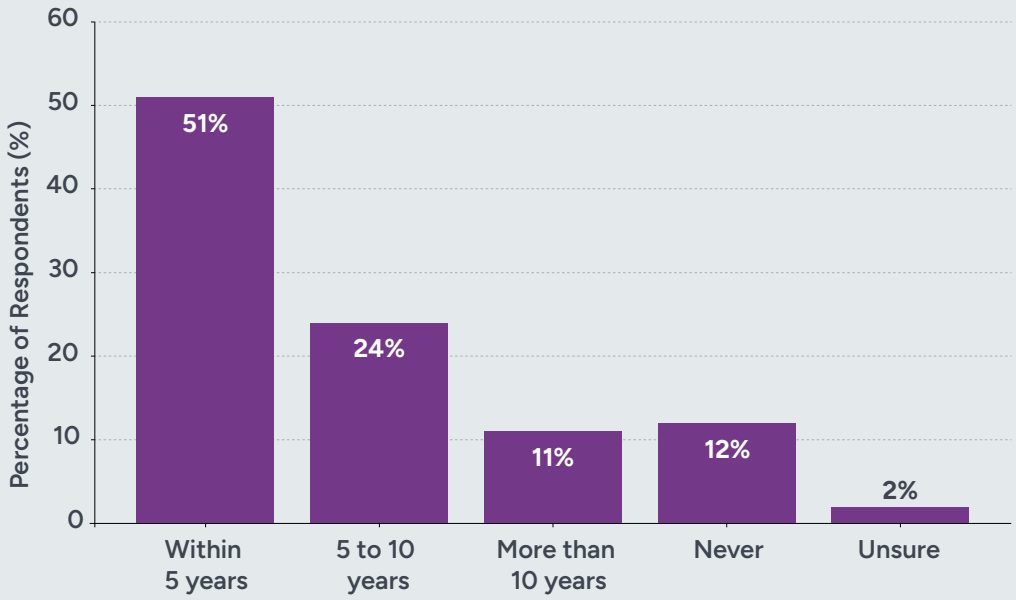
Cryptographic Security and Management

Trends in PKI Security and HSMs

Post-Quantum: The Threat and the Readiness Journey

Organizations believe the post-quantum threat is imminent. As shown in Figure 2, 75 percent of respondents agree and say a quantum computer will be capable of breaking traditional public key cryptography within five years (51 percent) or in five to 10 years (24 percent). Only 12 percent say it will never happen.

FIGURE 2. When do you believe a quantum computer will be capable of breaking traditional public key cryptography, such as RSA and ECC?

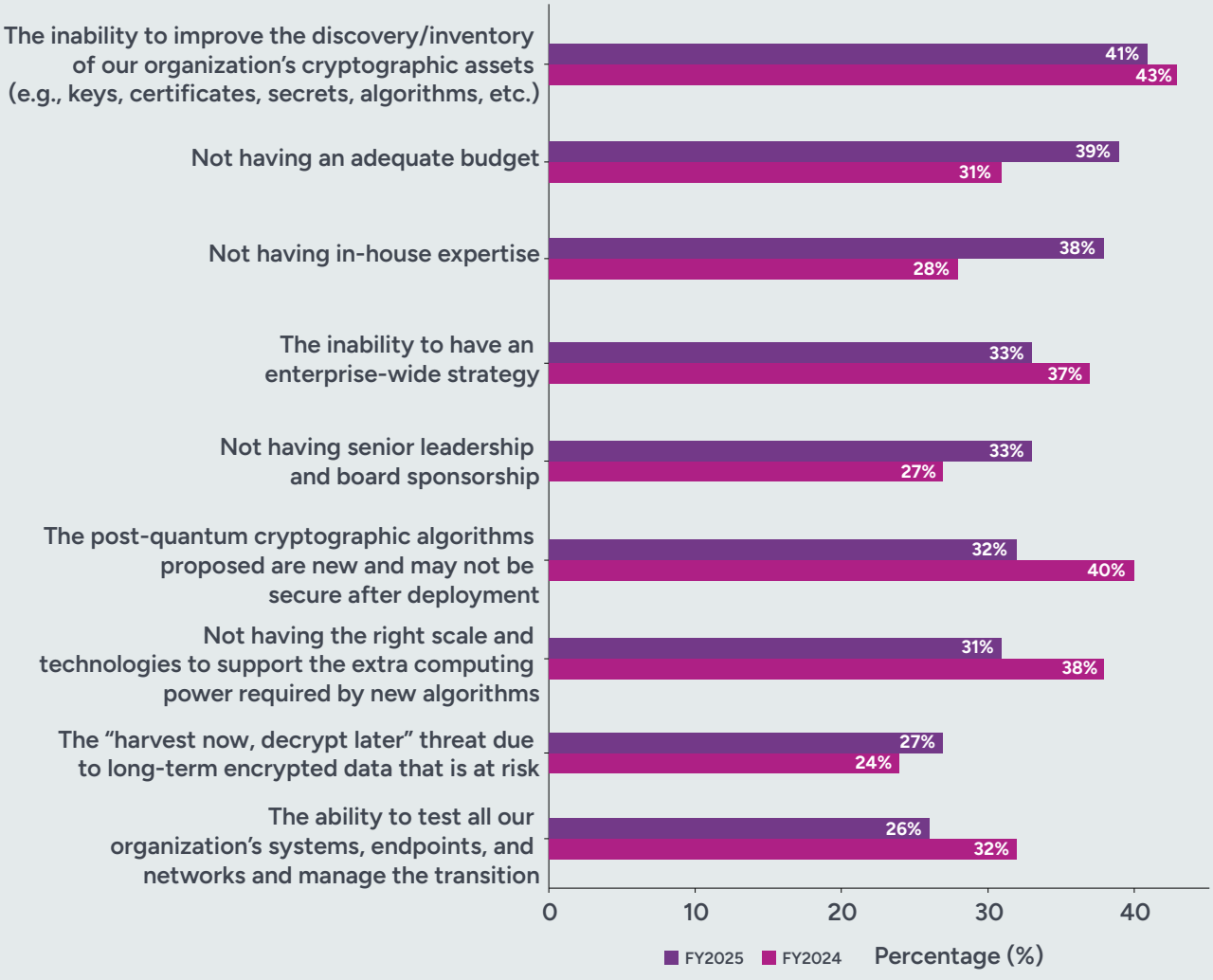


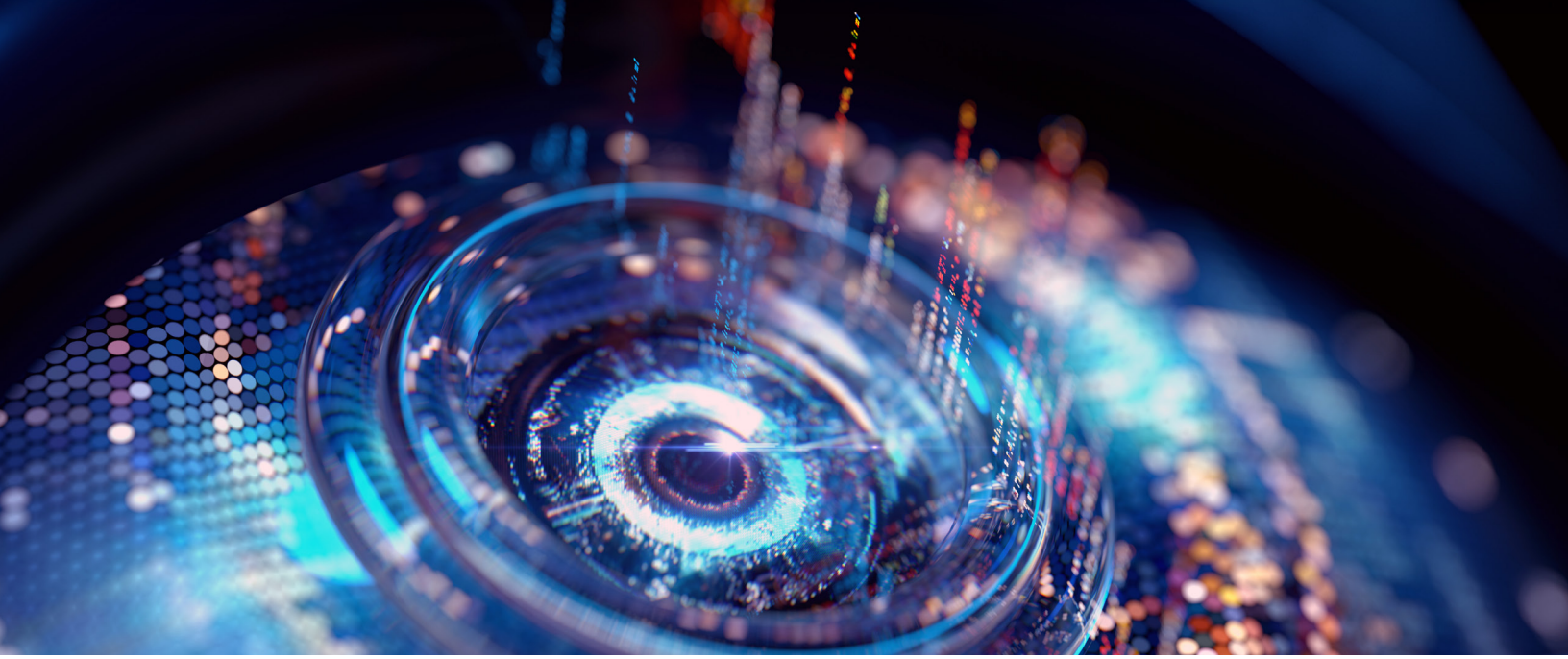
The biggest challenge to reducing the quantum threat and migration to post-quantum cryptography (PQC) continues to be the inability to improve the discovery/inventory of their organizations' cryptographic assets. Post-quantum cryptography consists of encryption algorithms or tools that can withstand attacks from both traditional and quantum computers.

According to Figure 3, 41 percent of respondents in this year's study vs. 43 percent of respondents in last year's study say the inability to improve visibility into their cryptographic assets is the greatest concern. Two concerns that have increased significantly are the lack of an adequate budget (39 percent in this year's study vs. only 31 percent in last year's study) and lack of in-house expertise (38 percent in this year's study vs. only 28 percent in last year's study).

Concerns that have decreased are not having the right scale and technologies to support the extra computing power required by new algorithms (31 percent of respondents in this year's study vs. 38 percent in last year's study) and the post-quantum cryptographic algorithms proposed are new and may not be secure after deployment (32 percent of respondents in this year's study vs. 40 percent of respondents in last year's study).

FIGURE 3. What are your greatest concerns when it comes to the quantum threat and migration to PQC?
Three responses permitted

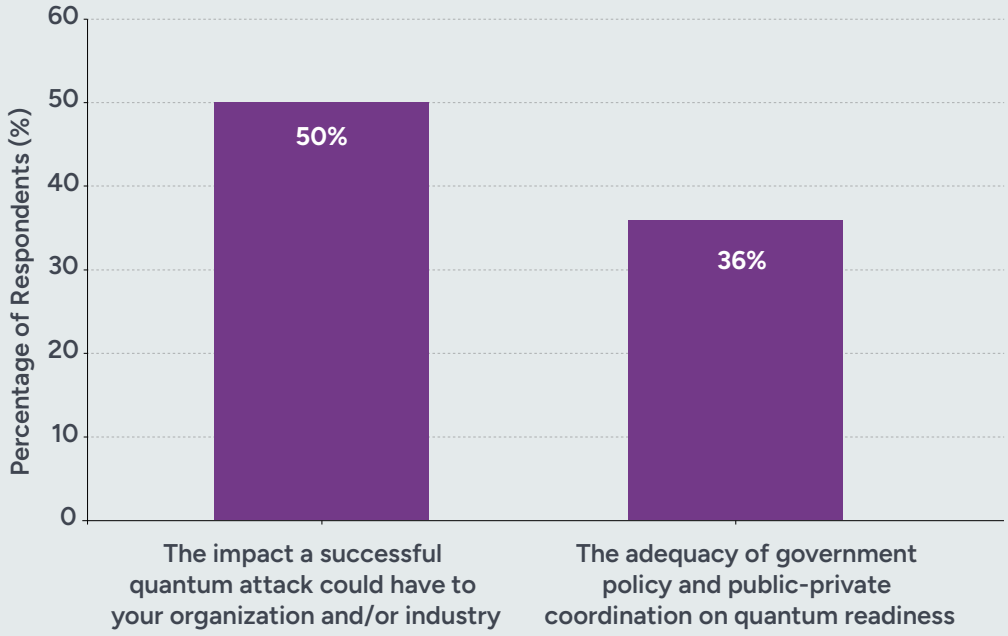




Fifty percent of respondents say a successful quantum attack would have a serious impact on their organizations and industries. Respondents were asked to rate the impact a successful quantum attack would have on their organization and/or industry from 1 = no impact to 10 = serious impact and the adequacy of government policy and public-private coordination on a scale from 1= not adequate to 10 = more than adequate (7+ responses).

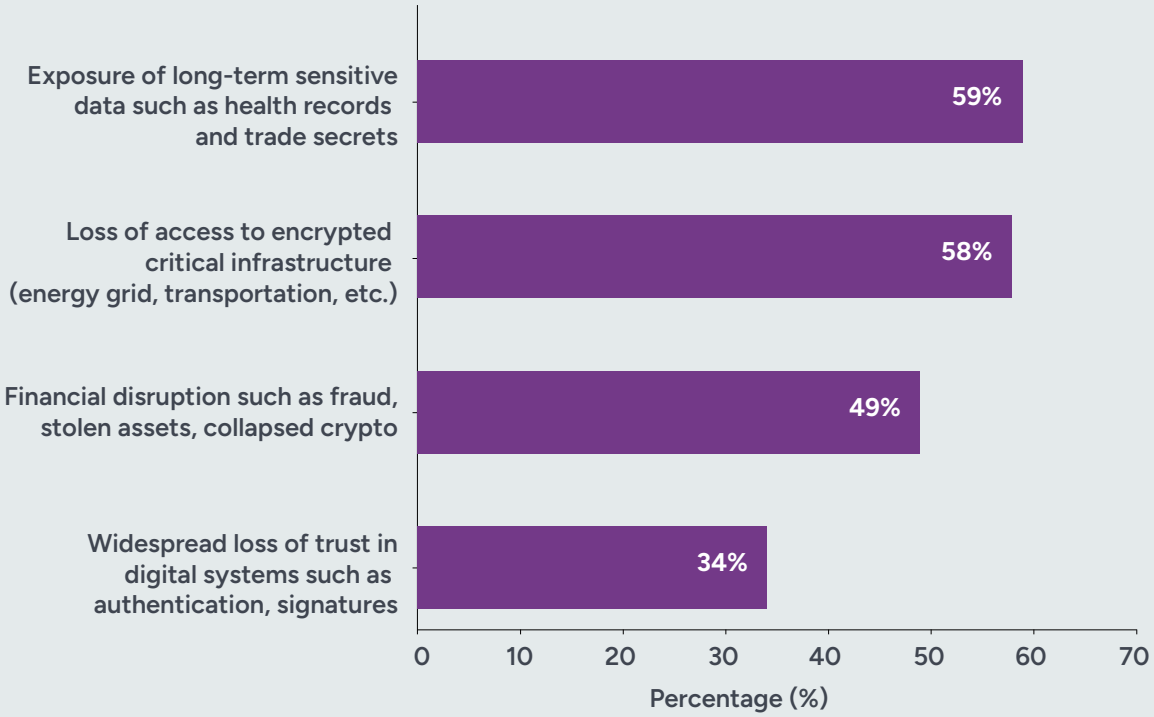
As shown in Figure 4, 50 percent rate the potential impact as serious (7+ on the 10-point scale) but only 36 percent of respondents rate the adequacy of government policy and public-private coordination on quantum readiness as more than adequate (7+ on the 10-point scale). Q7,8,9

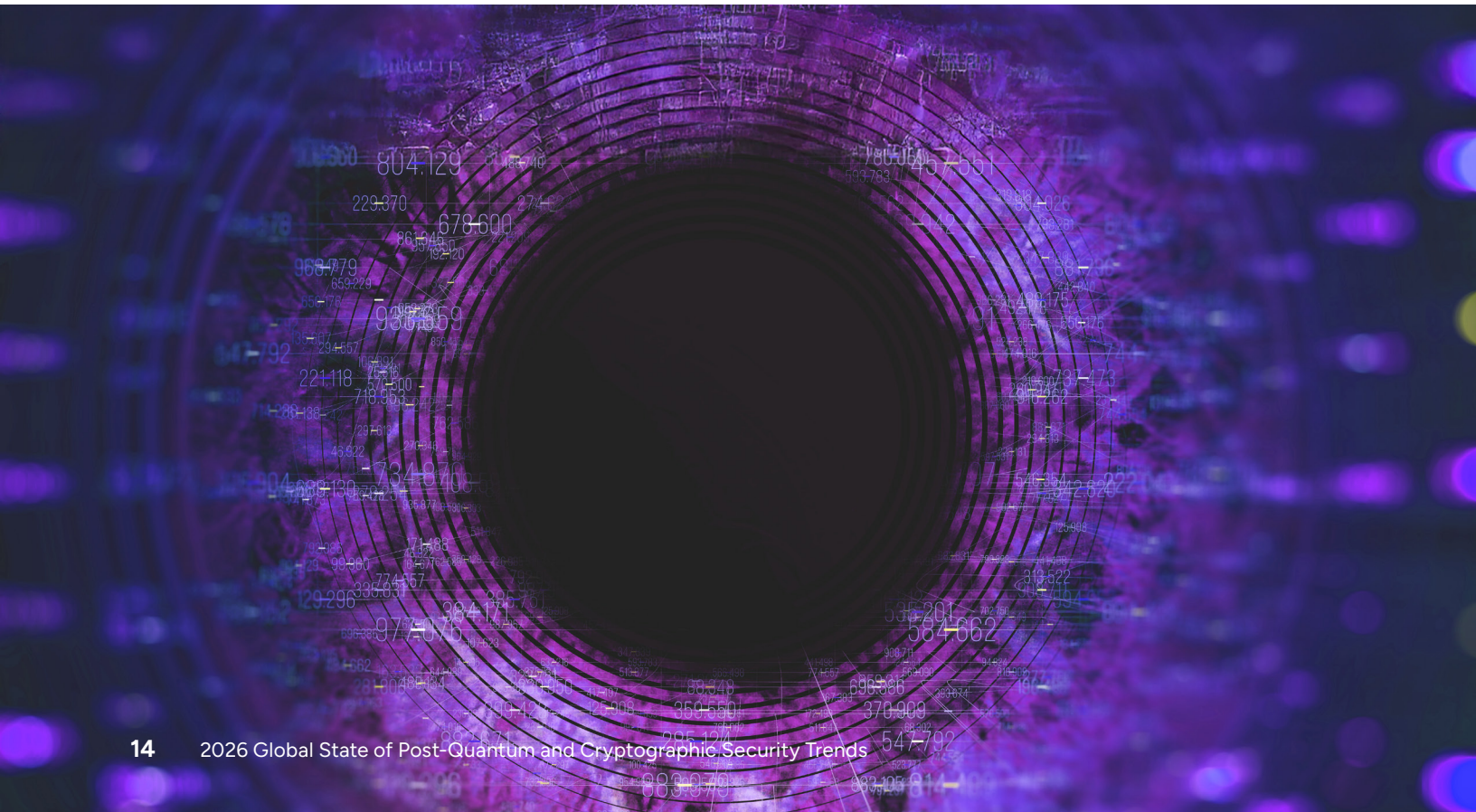
FIGURE 4. A potential quantum attack is considered serious and coordination on quantum readiness between government and the public-private sector is lacking On a scale from 1 = limited impact/not adequate to 10 = serious impact/more than adequate, 7+ responses presented



As shown in Figure 5, a successful quantum attack against organizations and industries could result in the loss of access to encrypted critical infrastructure (58 percent of respondents) and exposure of long-term sensitive data such as health records and trade secrets (59 percent of respondents).

FIGURE 5. The possible consequences if a successful quantum attack occurred
Two responses permitted





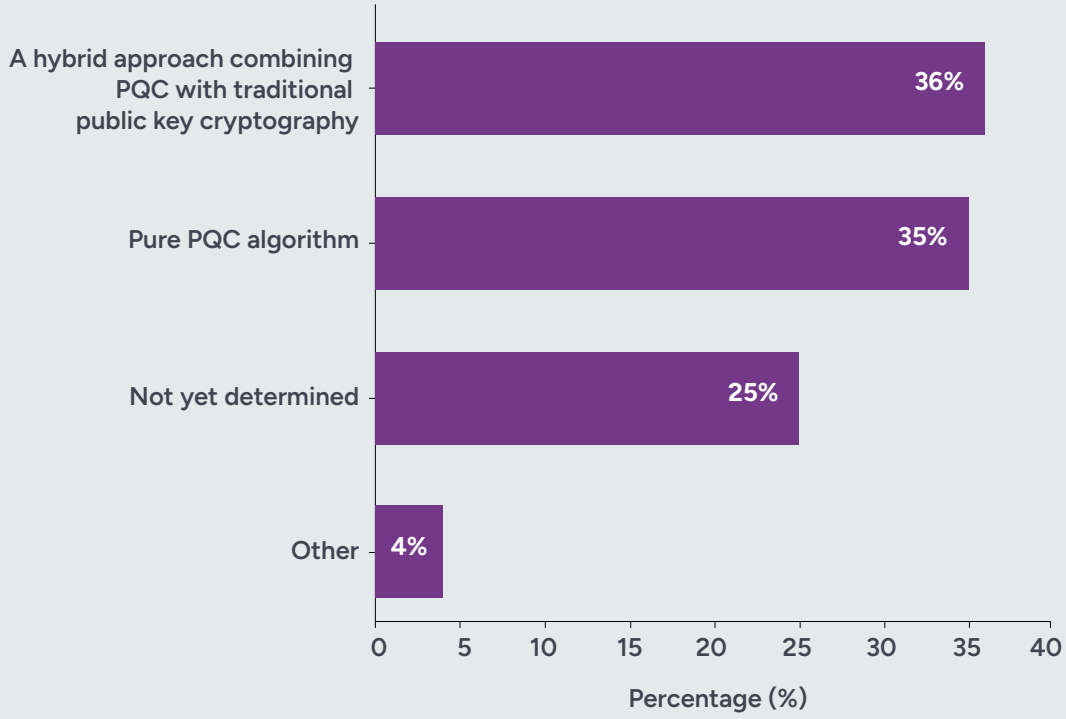
As part of their transition to PQC, 71% of respondents say their organizations are testing PQC (38%) or implementing PQC (33%).

As part of their transition to PQC, 71 percent of respondents say their organizations are testing PQC (38 percent) or implementing PQC (33 percent). Twenty-eight percent of respondents say they are neither testing nor implementing PQC.

According to Figure 6, of the 71 percent that are testing or implementing PQC, 35 percent say their organizations will implement a pure PQC algorithm and 36 percent of respondents say they will adopt a hybrid approach combining PQC with traditional public key cryptography when the transition is completed.

A pure PQC algorithm refers to a post-quantum cryptography (PQC) implementation that uses exclusively quantum-resistant algorithms for all cryptographic functions, with no reliance on traditional (classical) methods like RSA or ECC. This approach aims for complete quantum readiness but can pose compatibility and migration challenges.

FIGURE 6. When the transition to PQC is completed, what will your organization implement?



Cryptographic Security and Management

Senior IT and IT security staff are most responsible for cryptographic security strategies.
As shown in Figure 7, the CIO (24 percent of respondents) and CISO (22 percent of respondents) are most responsible for the strategy.

FIGURE 7. Who is most responsible for your organization's cryptographic security strategy?

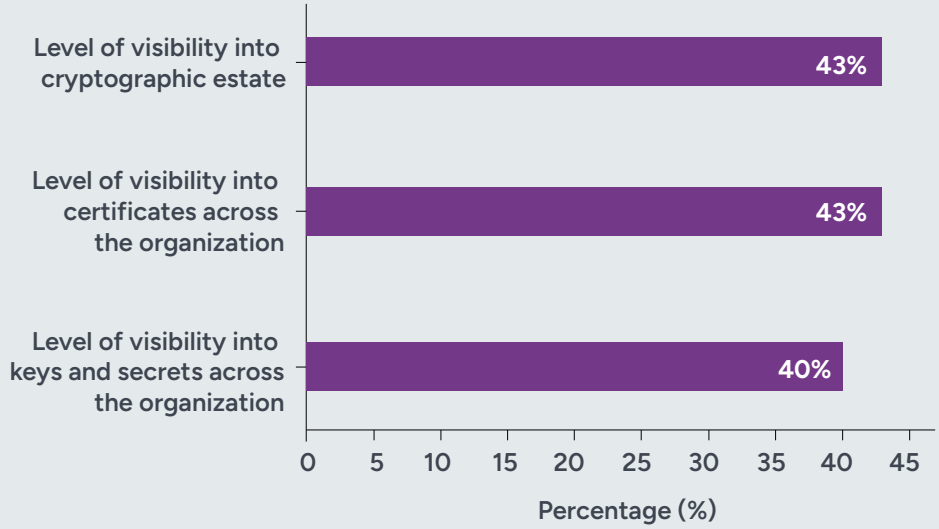
Cryptographic security refers to the technology to safeguard communications with data via encryption and identity from hardware and software (such as HSMs and PKI) to credentials such as keys, certificates, and secrets. Cryptographic security posture management involves continuously monitoring and assessing an organization's cryptographic practices to identify vulnerabilities and ensure compliance with security policies and industry standards.

Visibility into cryptographic assets is critical to understand and manage risks, ensure compliance, and prepare for future threats. It involves using automated tools for discovery, manual processes like questionnaires, and integrating with other security systems to gain a unified view of all assets and how they are deployed. Organizations often lack a complete picture of their cryptographic assets, which are used everywhere from code to cloud environments. This lack of visibility creates security gaps, such as weak or unmanaged keys, which can lead to breaches.

The lack of visibility into the cryptographic estate, certificates, and keys and secrets puts organizations' cryptographic security at risk. Respondents were asked to rate the level of visibility into their organizations' cryptographic estate, certificates, and keys and secrets on a scale from 1 = no visibility to 10 = complete visibility.

As shown in Figure 8, only 43 percent of respondents say their organizations have full or complete visibility into their organizations' cryptographic estate, only 43 percent of respondents say they have full or complete visibility into certificates across the organization, and only 40 percent say they have full or complete visibility into keys and secrets across the organization.

FIGURE 8. What is the level of visibility into the cryptographic estate, certificates, and keys and secrets? On a scale of 1 = no visibility to 10 = complete visibility, 7+ responses presented



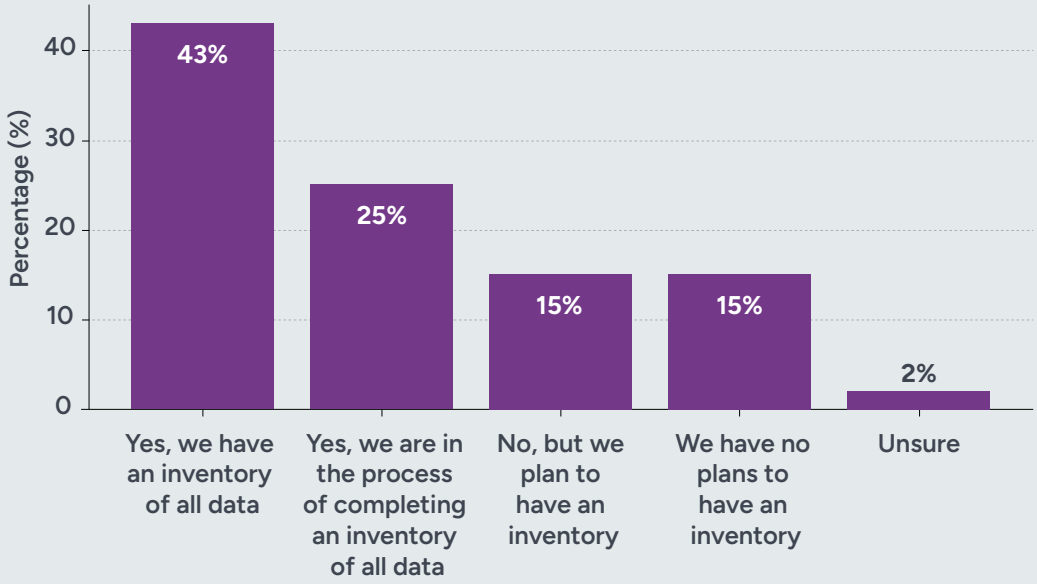
The lack of visibility into the cryptographic estate, certificates, and keys and secrets puts organizations' cryptographic security at risk.

Only 48% say their organizations have steps in place to secure the data in the inventory that needs to remain confidential for more than 10 years.

According to Figure 9, 68 percent of organizations either have an inventory of all their data (43 percent of respondents) or are in the process of completing an inventory of all data (25 percent of respondents) to determine where data resides and understand data flows, who has access, and how data is used.

As discussed previously, 59 percent of respondents say the No. 1 consequence from a successful quantum attack is the exposure of long-term sensitive data such as health records and trade secrets. However, less than half of respondents (48 percent) say their organizations have steps in place to secure the data in the inventory that needs to remain confidential for more than 10 years.

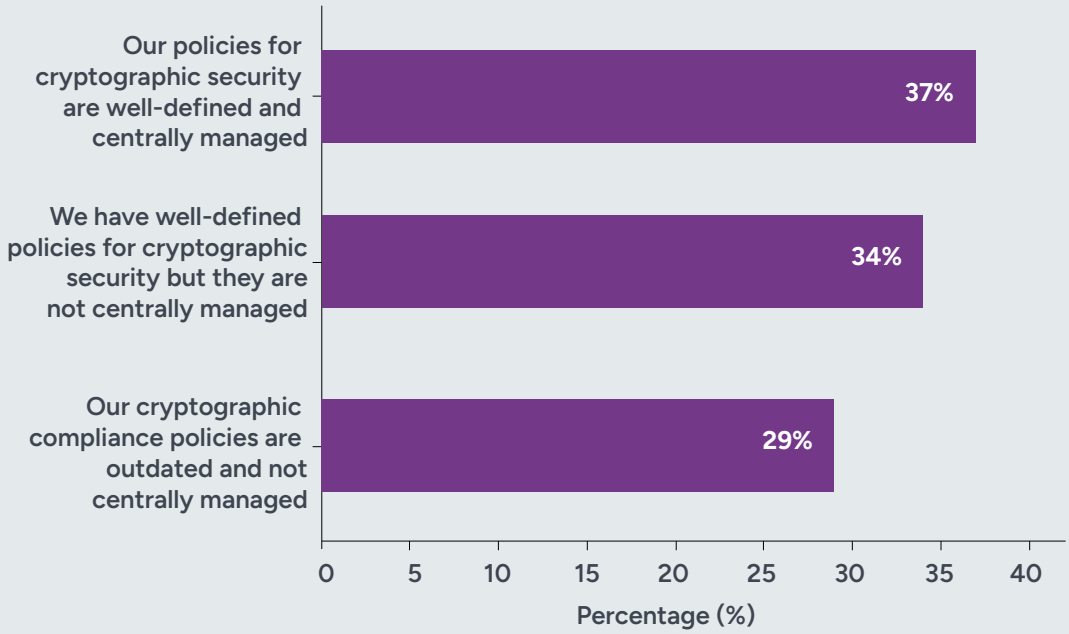
FIGURE 9. Does your organization have an inventory of all its data that enables knowing where data resides, understanding data flows, who has access and how data is used?



Few organizations have well-defined and centralized compliance programs for cryptographic security.

Few organizations have well-defined and centralized compliance programs for cryptographic security. According to Figure 10, only 37 percent of respondents say their policies for cryptographic security are well-defined and centrally managed. Only 34 percent of respondents say their organizations have well-defined policies for cryptographic security but they are not centrally managed, and 29 percent of respondents say their cryptographic compliance policies are outdated and not centrally managed.

FIGURE 10. What best describes your organization's compliance program for cryptographic security?



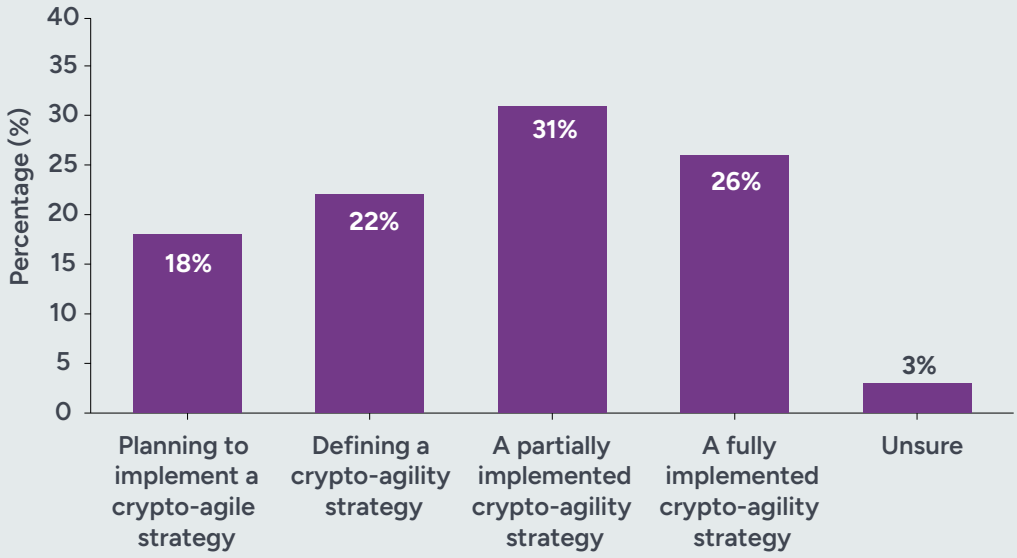
More staff and expertise are needed to improve the management of cryptographic assets. Sixty-eight percent of respondents say the management of cryptographic assets such as keys, certificates, and secrets is extremely difficult (39 percent) or very difficult (29 percent). As shown in Figure 11, insufficient personnel (45 percent of respondents), lack of skilled personnel (42 percent of respondents), systems are isolated and fragmented (41 percent of respondents), and trying to get an accurate inventory of keys, secrets, and certificates (37 percent of respondents) are the biggest challenges. Less than half (47 percent) of respondents say their organizations have PKI specialists on staff. If they don't have specialists on staff, 26 percent of respondents rely on consultants, 37 percent rely on service providers, and 37 percent rely on both consultants and service providers.

FIGURE 11. What makes the management of credentials difficult?

Crypto-agility is an attribute of a system that allows it to transition from one cryptographic system to another by configuration or policy without impacting all the infrastructure around it.

According to Figure 12, 57 percent of respondents say their organizations have a fully implemented crypto-agility strategy (26 percent) or a partially implemented crypto-agility strategy (31 percent). Forty percent of respondents say their organizations plan to implement a crypto-agility strategy (18 percent) or are defining its strategy (22 percent).

FIGURE 12. What best describes the maturity of your organization's crypto-agility strategy involving people, process, and technology?



Trends in the deployment of PKI and HSMs

Private cloud-based applications and mobile device authentication applications that use PKI credentials declined significantly from 2024. PKI credentials are digital certificates issued by a CA that bind a public key to an identity, enabling secure authentication encryption and digital signatures.

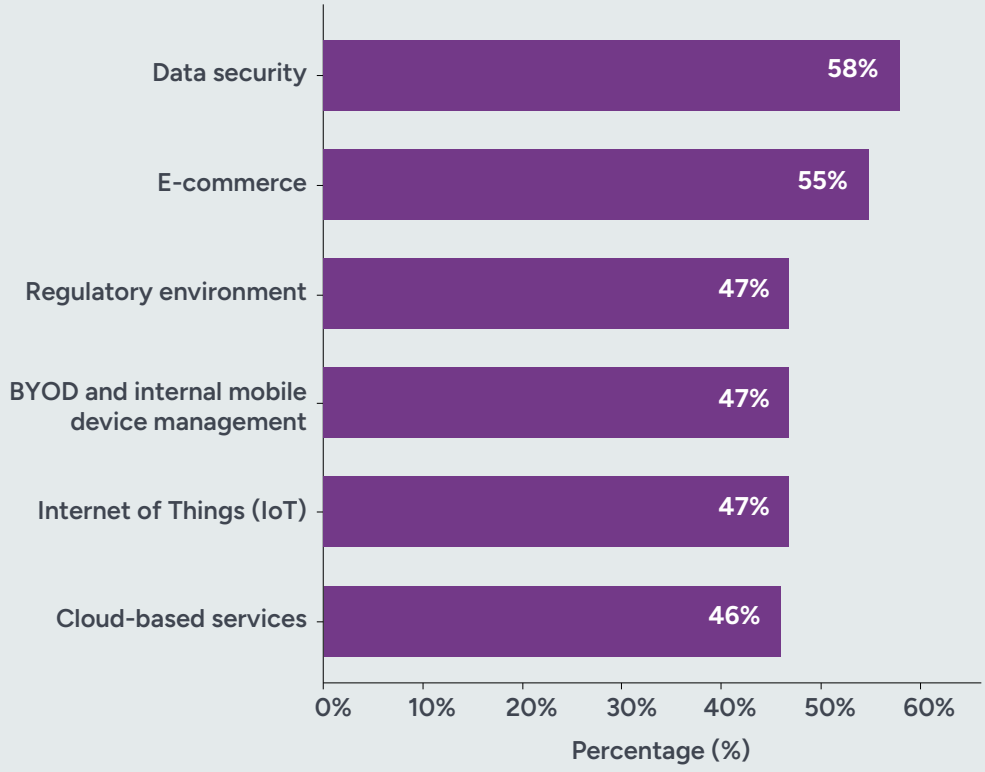
An internal corporate certificate authority (CA) is a private system used by an organization to issue and manage its own digital certificates, which are crucial for securing internal resources like intranet sites, VPNs, and devices. Unlike public CAs that verify identities for the public internet, an internal CA provides the organization with control, flexibility, and automation to manage the entire certificate lifecycle for its private network.

As shown in Figure 13, private cloud-based applications using PKI declined the most (56 percent of respondents in 2024 vs. 32 percent of respondents this year). Mobile device authentication decreased from 60 percent of respondents to 41 percent of respondents). The top applications using PKI credentials are private networks (52 percent of respondents), SSL certificates for public-facing websites and services (50 percent of respondents), and document/message signing (45 percent of respondents).

FIGURE 13. What applications use PKI credentials in your organization?
More than one response permitted

As shown in Figure 14, the most important trends driving the deployment of applications that make use of PKI are data security (58 percent of respondents), e-commerce (55 percent of respondents), and BYOD and internal mobile device management, Internet of Things, and the regulatory environment (all 47 percent of respondents).

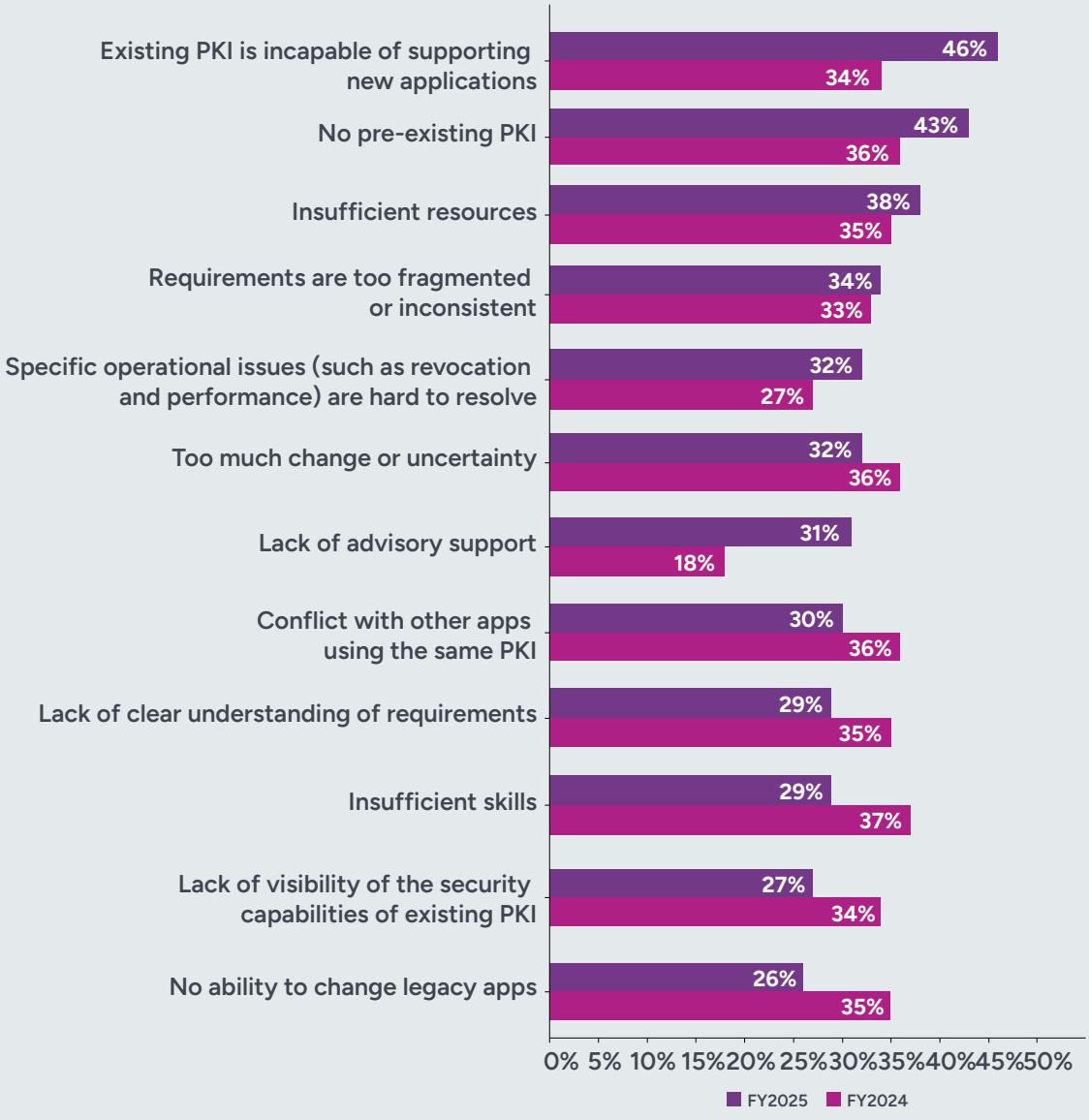
FIGURE 14. What are the most important trends that are driving the deployment of applications that make use of PKI? Three responses permitted



More organizations believe the biggest challenge to deploying PKI-enabled applications is that existing PKI is incapable of supporting new applications. As shown in Figure 15, in this year's research, 46 percent of respondents say the No. 1 challenge is that existing PKI is incapable of supporting new applications, an increase from 34 percent of respondents in last year's study. Lack of advisory support increased from 18 percent of respondents to 31 percent of respondents in this year's research, and no pre-existing PKI as a challenge increased from 36 percent of respondents to 43 percent in this year's research.

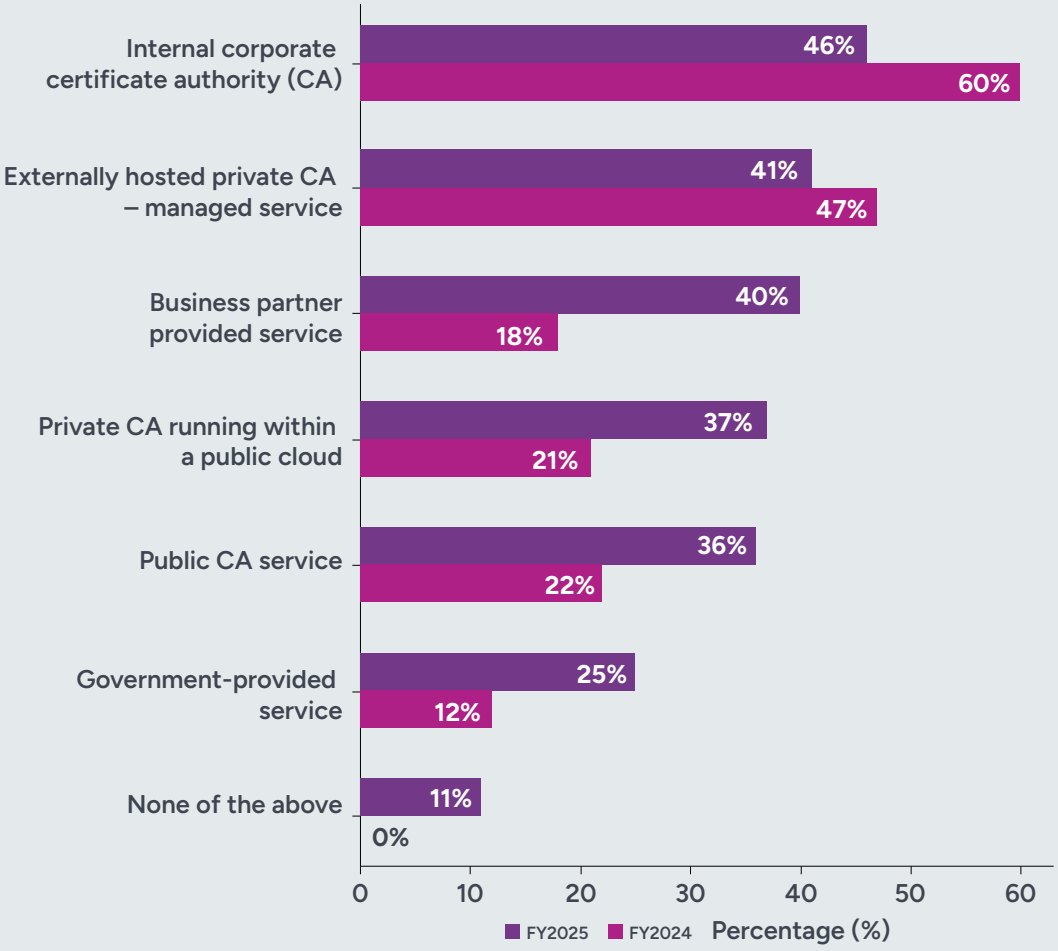
Challenges that decreased from last year are no ability to change legacy apps (26 percent of respondents in this year's research vs. 35 percent of respondents in last year's research) and insufficient skills (decreased from 37 percent of respondents vs. 29 percent of respondents in last year's research).

FIGURE 15. What are the challenges to deploying PKI-enabled applications?
Four responses permitted



The use of internal corporate certificate authorities (CAs) to deploy PKIs has declined since last year. According to Figure 16, 46 percent of respondents in this year's report use CAs to deploy PKI and 60 percent of respondents in last year's study. Business-partner-provided service increased the most, from 18 percent of respondents in last year's report to 40 percent of respondents in this year's study. Private CAs running within a public cloud increased from 21 percent of respondents last year to 37 percent of respondents this year.

FIGURE 16. What best describes how your organization's enterprise PKI is deployed?
More than one response permitted



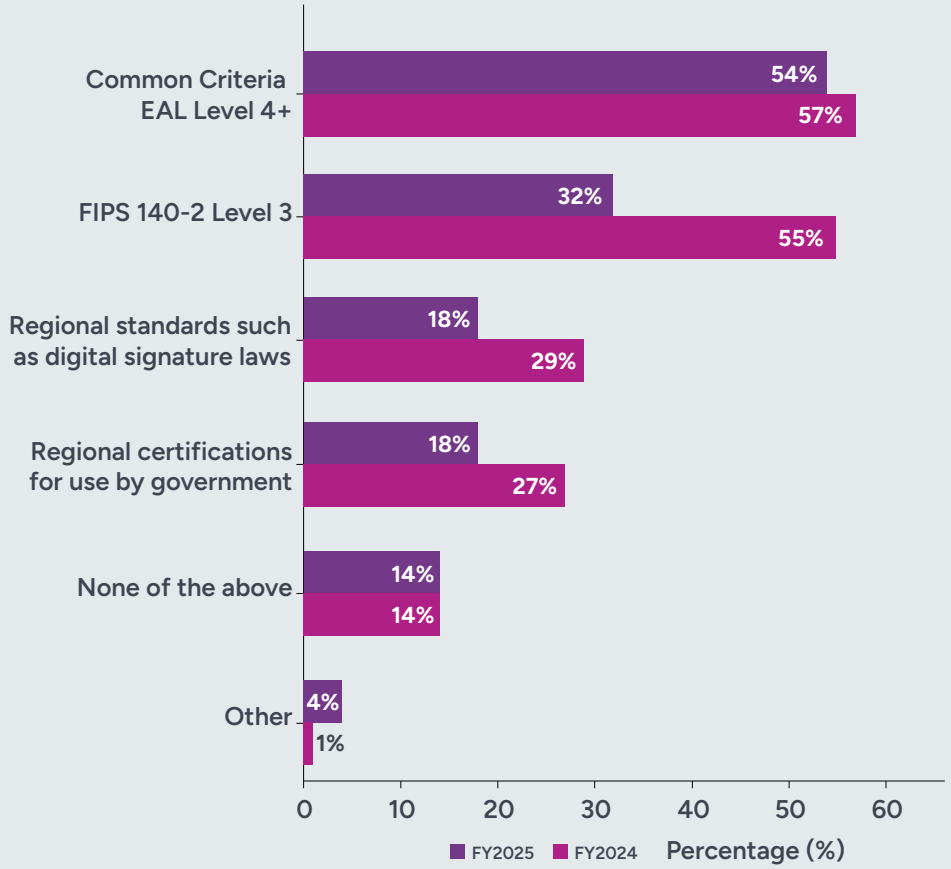
The use of internal corporate certificate authorities (CAs) to deploy PKIs has declined since last year.

Common Criteria (CC) EAL4+ is a high-level security certification for IT products that signifies a thorough and rigorously tested design, implementation, and deployment process. It represents a strong level of independently assured security suitable for organizations with significant security concerns, such as government agencies and financial institutions, ensuring the product is built and tested to withstand sophisticated attacks. EAL4+ means the product has been enhanced beyond the standard EAL4 requirements through "augmentations," which often include advanced vulnerability analysis and a more robust flaw remediation process.

FIPS 140-2 Level 3 is a security standard that requires cryptographic modules to have both strong physical tamper-resistance and identity-based authentication. Key features include tamper-response circuitry that erases sensitive data if tampering is detected and the need for individual users to have unique login credentials. It is considered a significant leap from lower levels and is often required for handling high-value or regulated data.

According to Figure 17, the most important security certification when deploying PKI infrastructure is Common Criteria EAL Level 4+ (54 percent in this year's study vs. 57 percent of respondents in last year's study). The second most important certification is FIPS 140-2 Level 3. However, its importance has declined significantly from 55 percent of respondents to 32 percent of respondents.

FIGURE 17. Which security certifications are important when deploying PKI infrastructure?
More than one response permitted

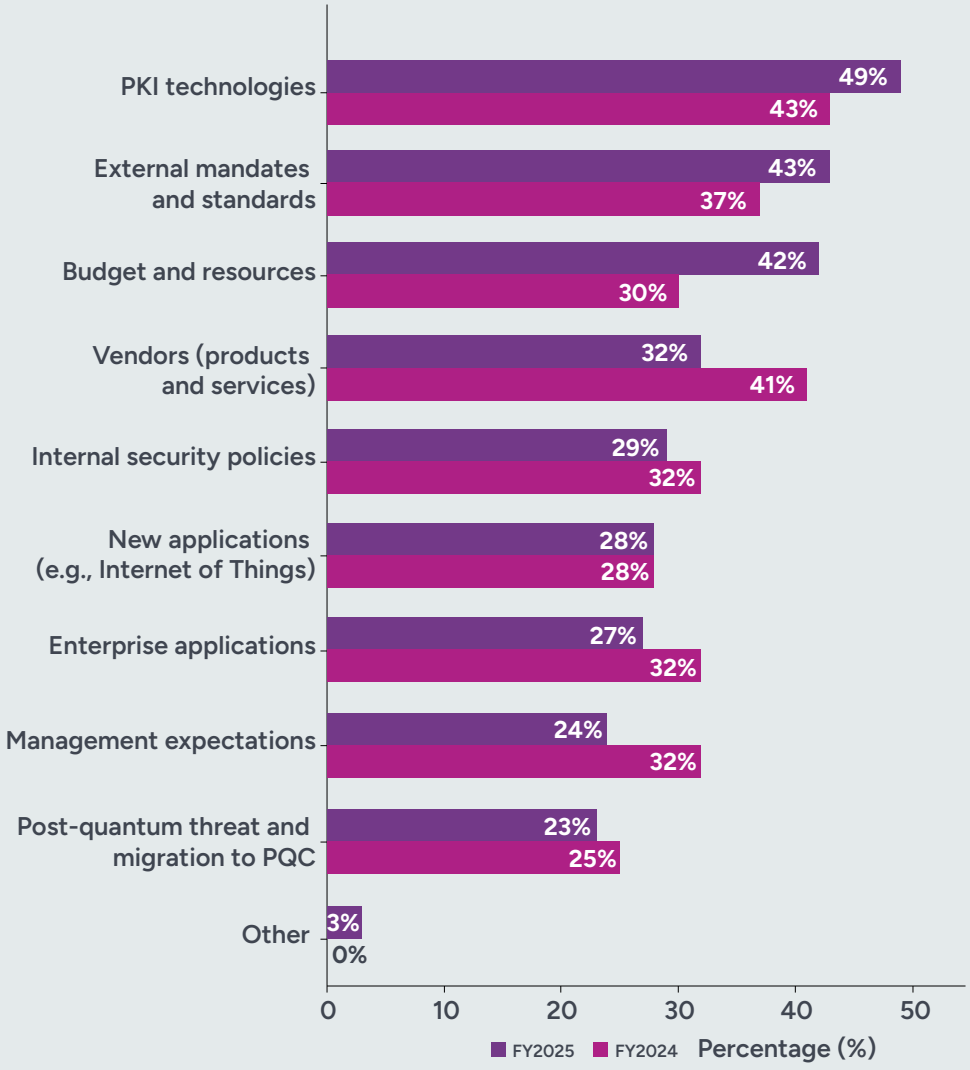


According to Figure 18, 37 percent of respondents say no clear ownership for PKI deployment and management is the No. 1 challenge. This is followed by no suitable products or technologies available (30 percent of respondents), necessary performance and reliability is hard to achieve (30 percent of respondents), and commercial solutions are too complicated or too expensive (30 percent of respondents).

FIGURE 18. What are the main challenges in deploying and managing PKI?
Three responses permitted

The biggest uncertainty and concern about the evolution of PKI are PKI technologies and external mandates and standards. As shown in Figure 19, when asked what the greatest areas of change and uncertainty to PKI will be, 49 percent of respondents say it is PKI technologies, an increase from 43 percent in 2024 and external mandates and standards, an increase from 37 percent of respondents in 2024 to 43 percent of respondents in 2025. Budget and resources increased significantly to 42 percent of respondents from 30 percent of respondents.

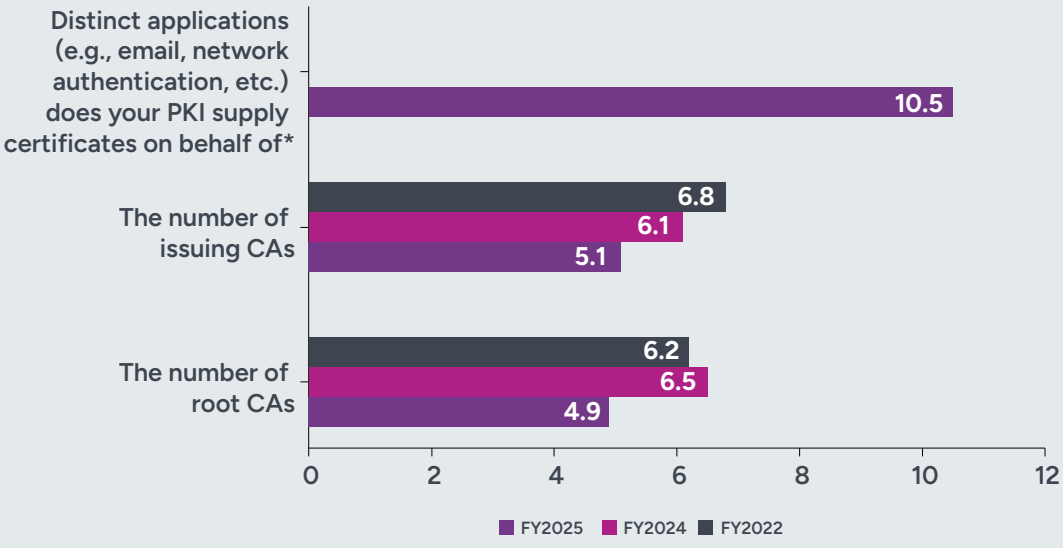
FIGURE 19. What are the greatest areas of possible change and uncertainty with PKI?
Three responses permitted



The number of issuing CAs and root CAs has decreased significantly.

The number of issuing CAs and root CAs has decreased significantly. In cryptography and computer security, a root certificate is a public key certificate that identifies a root certificate authority (CA). As shown in Figure 20, organizations have an average of five root CAs, an average of five issuing CAs, an average of 30,616 certificates issued or acquired from an external service, and an average of 11 distinct applications (such as email and network authentication) PKI supplies certificates on behalf of.

FIGURE 20. The average number of root CAs, issuing CAs, and distinct applications PKI supplies certificates on behalf of



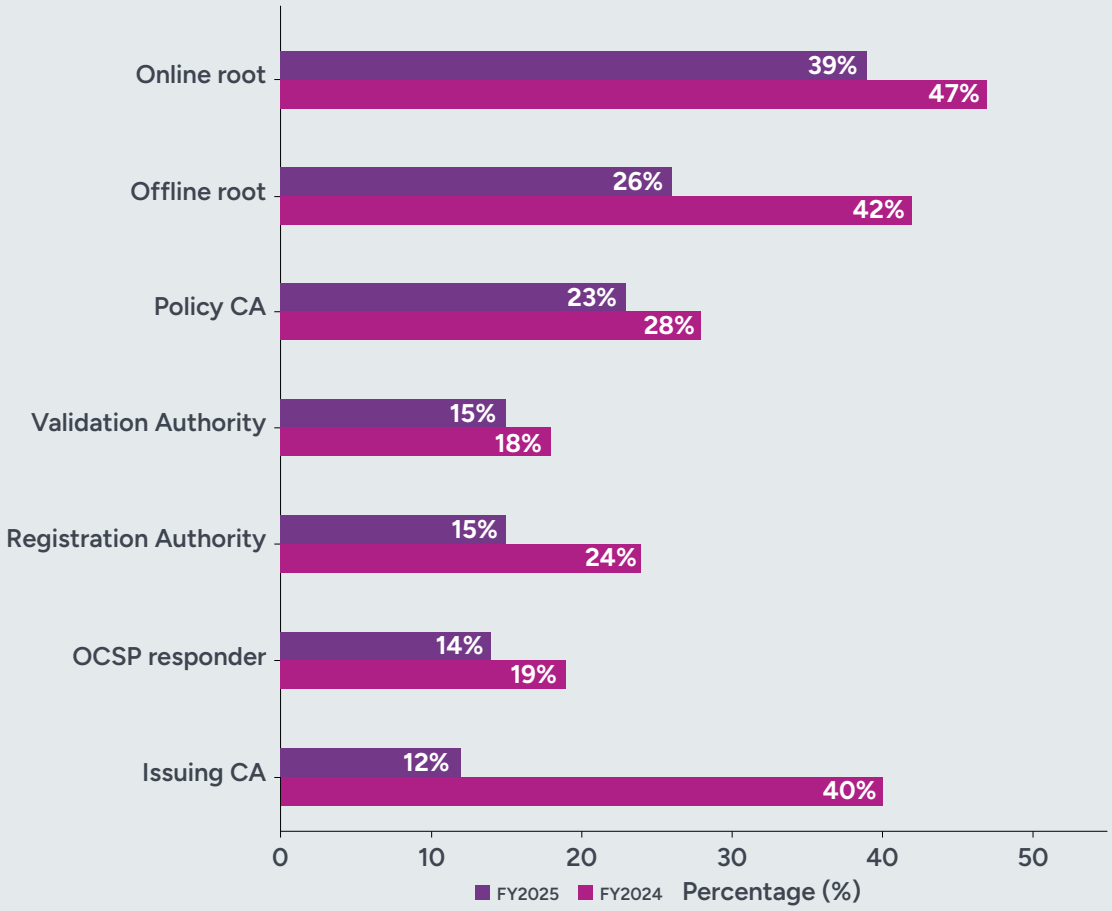
*Not a response in previous years

Hardware security modules (HSMs) are physical computing devices that securely manage cryptographic keys and perform cryptographic operations like encryption, decryption, and authentication. They are tamper-resistant and provide a secure, isolated environment for sensitive data, ensuring that keys are generated, stored, and used within the device, never leaving its protected boundary. HSMs are used to add a layer of security to applications, especially in sensitive areas like financial transactions and cloud environments.

More organizations use HSMs to secure PKI. Sixty-six percent of respondents in this year's research vs. 55 percent of respondents in last year's research say their organizations use HSMs. Sixty-three percent of respondents in this year's research vs. 51 percent of respondents in last year's research say their organizations use HSMs to secure PKI.

According to Figure 21, the top areas of deployment to secure PKI are online roots and offline roots. According to last year's research, 47 percent said they are deployed to secure PKI in online roots and 42 percent said they are deployed to secure PKI in offline roots.

FIGURE 21. Where are HSMs deployed? More than one response permitted



As shown in Figure 22, the top HSM use cases are for database encryption and encryption and tokenization solutions (both 49 percent of respondents). These are followed by privileged access management (PAM) solutions to protect administrative access (48 percent of respondents), Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) for cloud environments (44 percent of respondents), and PKI.

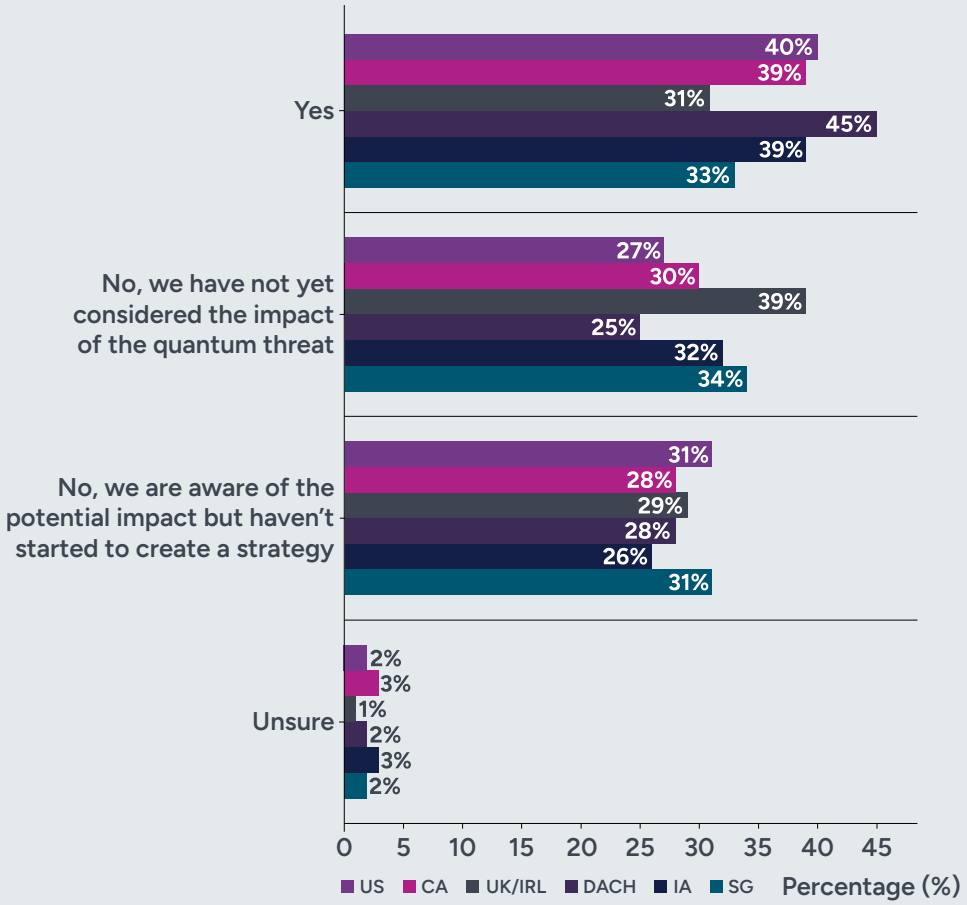
FIGURE 22. What are top HSM use cases? Five responses permitted

Regional Differences

In this section of the report, we present some of the most interesting differences among the countries represented in this research: United States (552 respondents), United Kingdom/Ireland (573 respondents), Canada (396 respondents), DACH (553 respondents), Indonesia (369 respondents), and Singapore (485 respondents).

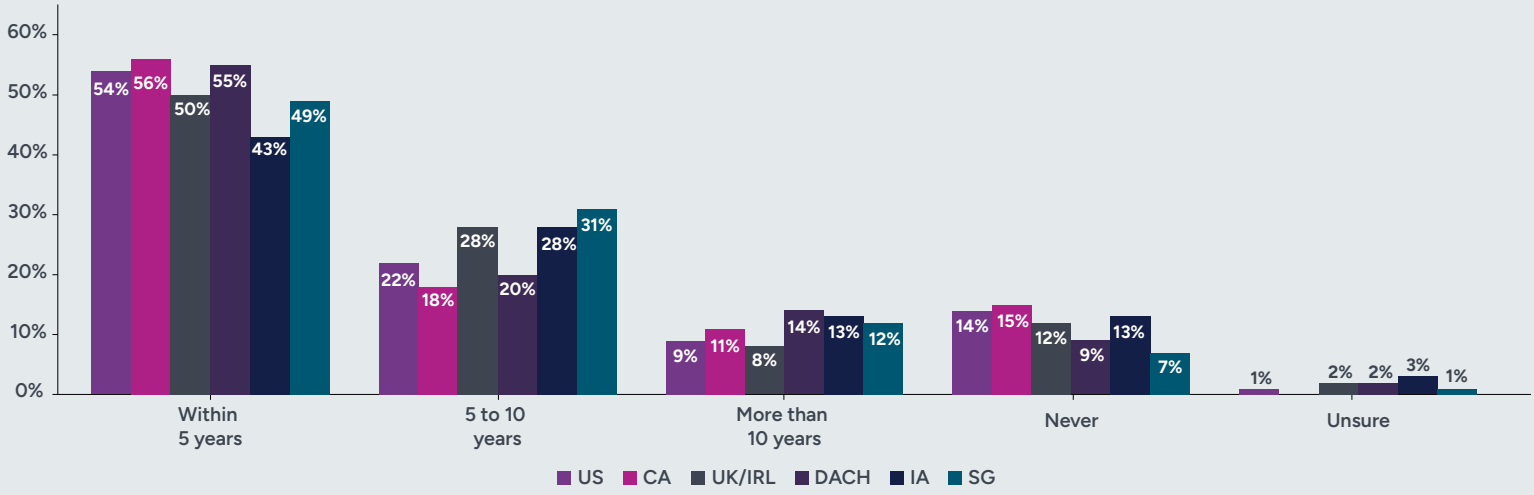
More organizations in DACH have started to prepare for the post-quantum threat. According to Figure 23, 45 percent of respondents say their organizations are preparing. Forty percent of U.S. respondents say their organizations are preparing. Only 33 percent of respondents in Singapore say their organizations are preparing. Organizations in the UK and Ireland have the most respondents who say their organizations have not considered the impact of the quantum threat (39 percent of respondents).

FIGURE 23. Is your organization preparing for the post-quantum threat?



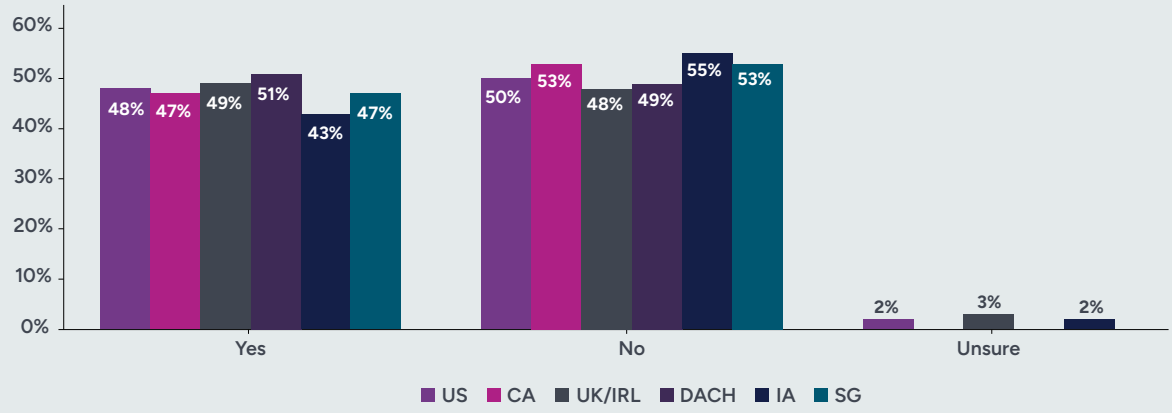
All respondents in the countries represented say the quantum threat is imminent. As shown in Figure 24, 56 percent of respondents in Canada and 55 percent of respondents in DACH predict that within five years the quantum computer will be capable of breaking traditional public key cryptography such as RSA and ECC.

FIGURE 24. When will a quantum computer be capable of breaking traditional public key cryptography such as RSA and ECC?



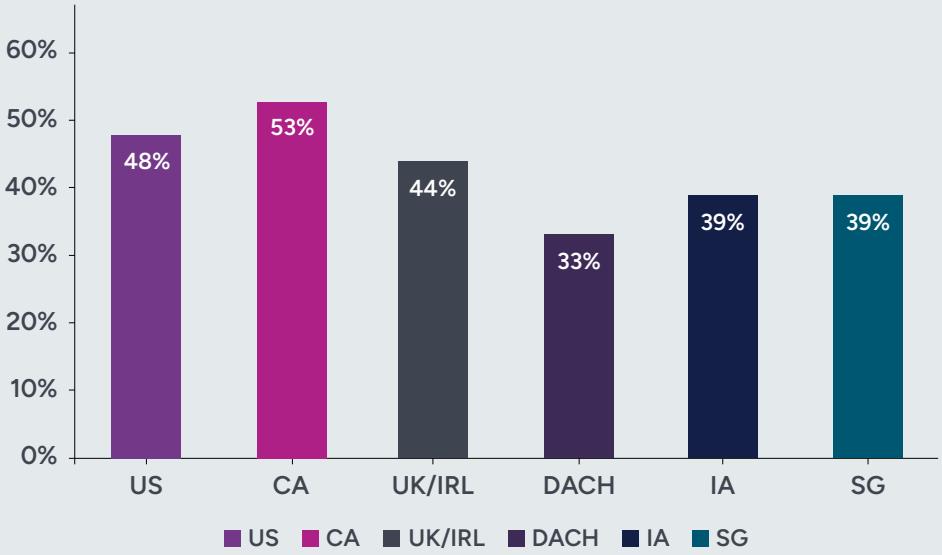
European privacy laws are stricter than in other countries and may be the reason that DACH and the UK and Ireland are most likely to have steps in place to secure data that needs to remain confidential for more than 10 years, 51 percent and 49 percent of respondents, respectively. Indonesia is least likely to have a plan to secure data for more than 10 years (43 percent of respondents).

FIGURE 25. Does your organization have steps in place to secure data that needs to remain confidential for more than 10 years?



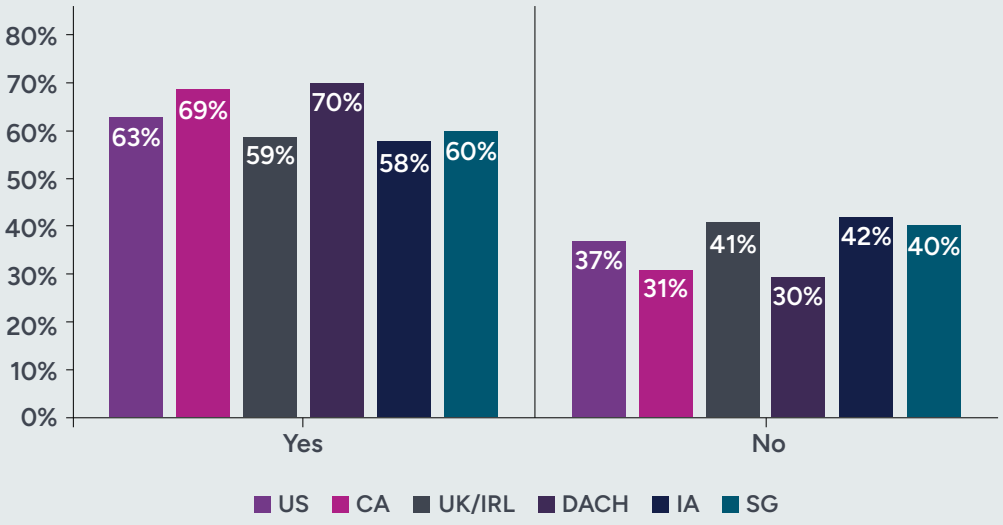
Visibility into organizations' cryptographic estate is critical to managing risks. According to Figure 26, organizations in Canada and the U.S. are most likely to have complete visibility into their cryptographic estate, 53 percent of respondents and 48 percent of respondents, respectively. DACH organizations are least likely to have complete visibility (33 percent of respondents).

FIGURE 26. What is the level of visibility into your organization's cryptographic estate?
On a scale of 1 = no visibility to 10 = complete visibility, 7+ responses presented



HSMs are physical computing devices that securely manage cryptographic keys and perform cryptographic operations like encryption, decryption, and authentication. As shown in Figure 27, 70 percent of respondents in DACH say their organizations use HSMs to secure PKI. Indonesia and the UK and Ireland are more likely not to use HSMs, 42 percent of respondents and 41 percent of respondents, respectively.

FIGURE 27. Does your organization use HSMs to secure PKI?



Methods

Methods

Table 1 shows a sampling frame of 3,374 IT and IT security practitioners who are familiar with the use of post-quantum, cryptographic security, PKIs, and HSMs. Screening and reliability checks required the removal of 449 surveys. Our final sample consisted of 2,925 surveys from the United States (552), Canada (396), United Kingdom/ Ireland (573), DACH (553), Indonesia (369), and Singapore (482). This represents a 2.2 percent response rate.

Table 1. Sample response	Frequency
Sampling frame	133,760
Total returns	3,374
Rejected or screened surveys	449
Overall sample (encryption trends)	2,925
PKI subsample	1,161
Ratio subsample to overall sample	40%

Figure 28 reports the respondent's organizational level within participating organizations. By design, 67 percent of respondents are at or above the supervisory levels and 31 percent of respondents reported their position as associate/staff/technician. Respondents have on average 8.5 years of security experience with approximately 4.3 years of experience in their current position.

FIGURE 28. Distribution of respondents according to position level
Country samples are consolidated

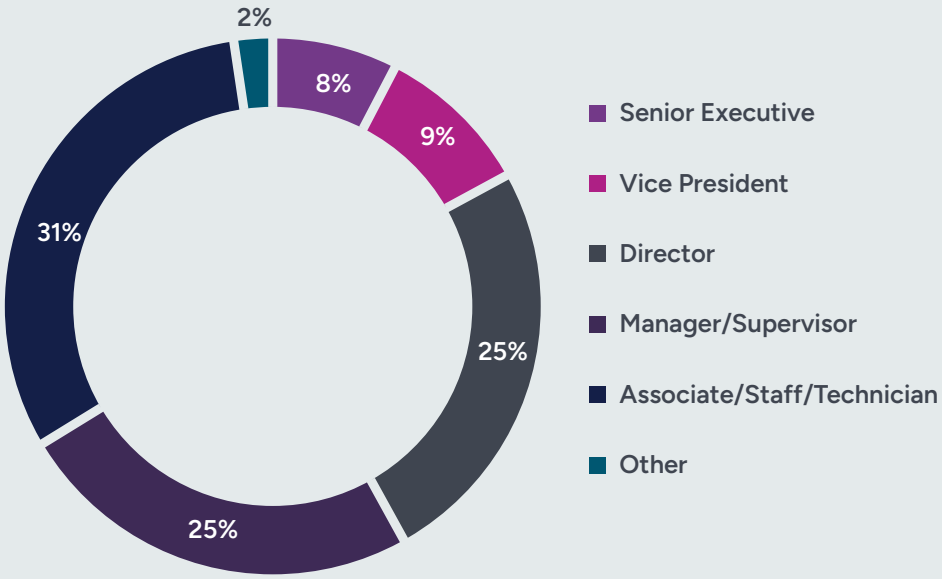


Figure 29 identifies the organizational location of respondents in our study. Approximately half (51 percent) of respondents are located within security and IT operations. This is followed by lines of business at 20 percent and compliance (17%).

FIGURE 29. Distribution of respondents according to organizational location

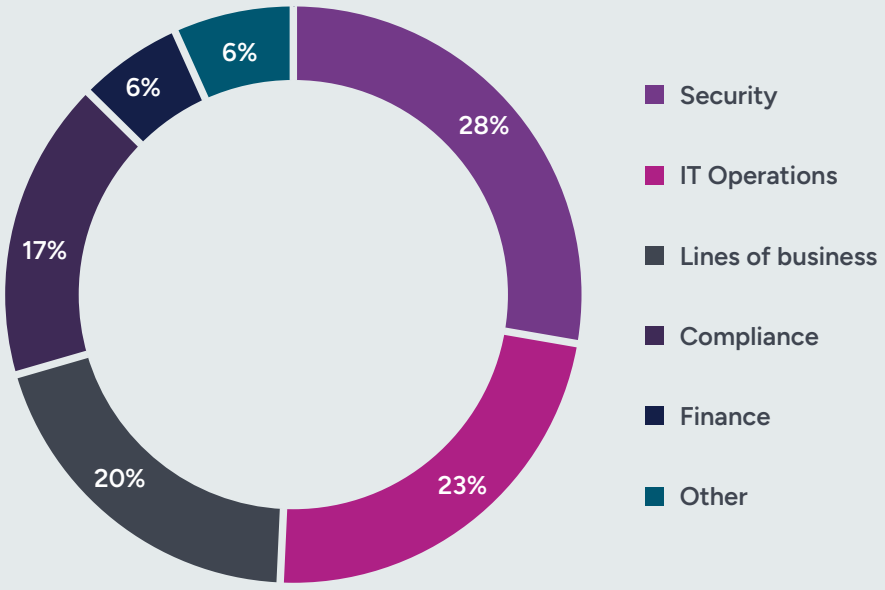
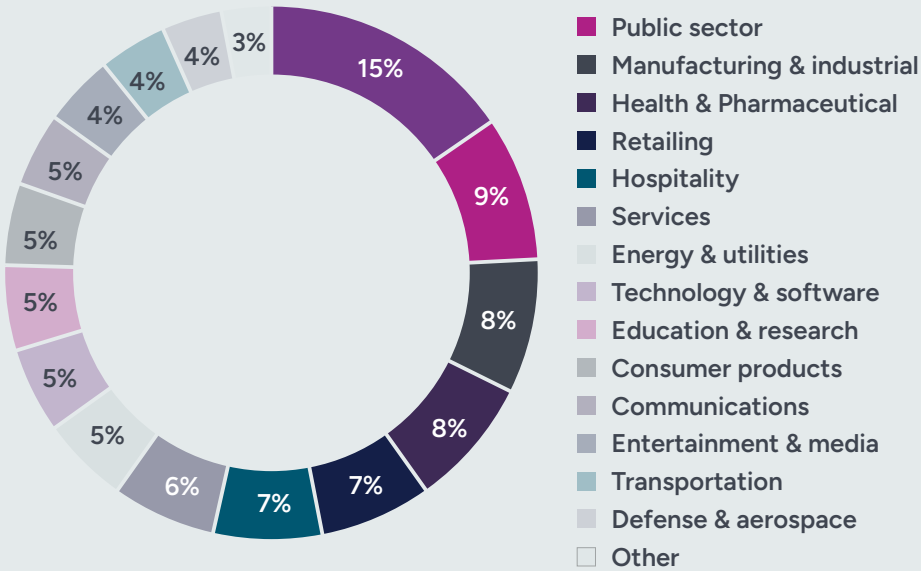
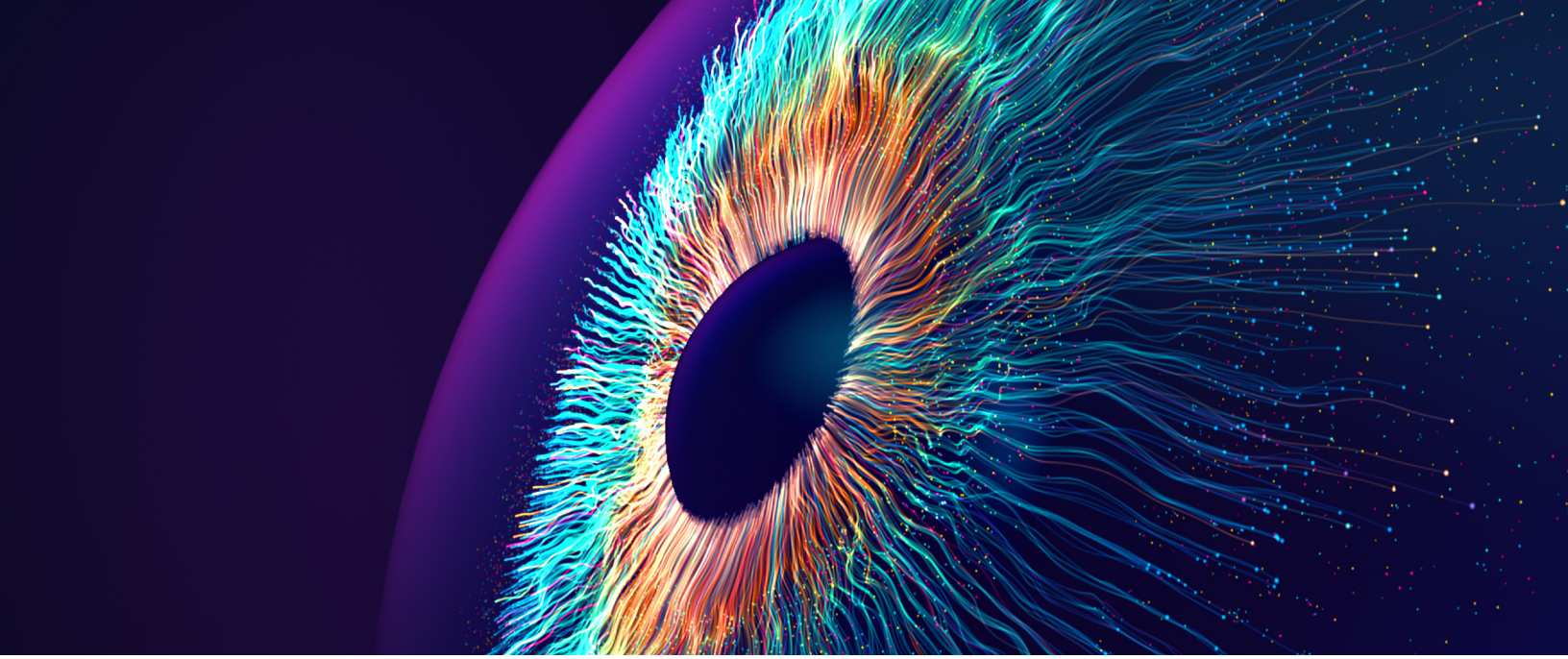


Figure 30 reports the industry classification of respondents' organizations. Fifteen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments, and credit cards. Nine percent of respondents are located in n the public sector. This is followed by manufacturing and industrial, healthcare, and pharmaceutical (each at 8 percent of respondents).

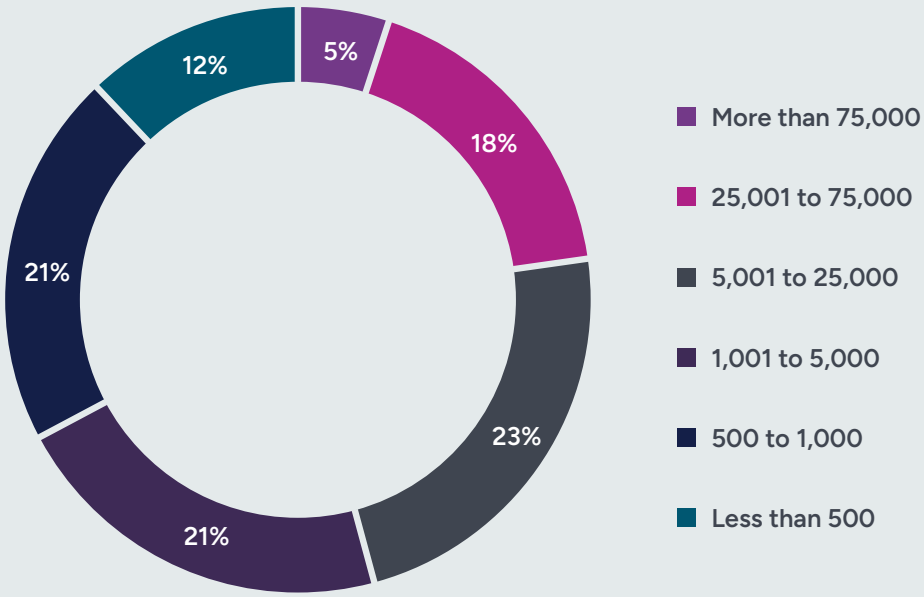
FIGURE 30. Distribution of respondents according to primary industry classification
Country samples are consolidated





According to Figure 31, more than half (67 percent) of respondents are located in larger-sized organizations with a global headcount of more than 1,000 employees.

FIGURE 31. Distribution of respondents according to organizational headcount
Country samples are consolidated



Limitations

Limitations

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from the presented findings. The following items are specific limitations that are germane to most survey-based research studies.

Non-response bias:
The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners in six countries/regions, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.

Sampling-frame bias:
The accuracy of survey results is dependent upon the degree to which our sampling frames are representative of individuals who are IT or IT security practitioners within global companies represented in this study.

Self-reported results:
The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, including sanity checks, there is always the possibility that some respondents did not provide truthful responses.

ABOUT PONEMON INSTITUTE

Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

ENTRUST
SECURING A WORLD IN MOTION

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com