2024 PKI and Post-Quantum Trends Study

SPONSORED BY ENTRUST

Independently conducted by Ponemon Institute LLC

Publication Date: October 2024

ENTRUST

SECURING A WORLD IN MOTION

Ponemon INSTITUTE

Contents

Part 1
Introduction

Part 1

INTRODUCTION

Public key infrastructure (PKI) is considered essential to keep people, systems, and things securely connected. According to research, organizations looking to achieve PKI maturity need to address challenges such as clear ownership of the PKI strategy and ensuring sufficient skills.

The 2024 PKI and Post-Quantum Trends Study is part of a larger study published in May involving 4,052 respondents in nine countries.[1] In this report, Ponemon Institute presents the findings based on a survey of 2,176 IT and IT security personnel who are involved in their organizations' enterprise PKI in the following nine countries: United States (409 respondents), Germany (309 respondents), United Kingdom (289 respondents), Canada (245 respondents), Singapore (235 respondents), United Arab Emirates (UAE) (203 respondents), Japan (168 respondents), Saudi Arabia/Middle East (162 respondents), and Australia/NZ (156 respondents).

[1] 2024 State of Zero Trust & Encryption Study (sponsored by Entrust), Ponemon Institute, May 2024.

The following is a summary of the most important takeaways from the research:

PKI and IoT Trends

The orchestration of the PKI software increased from 42% of respondents to 50% of respondents. However, 59% of respondents say orchestration is very or extremely complex, an increase from 43% of respondents in 2023.

Responsibility for the PKI strategy is being assigned to IT security and IT leaders. As PKI becomes increasingly critical to an organization's security posture, the CISO and CIO are most responsible for their organization's PKI strategy. The IT manager being most responsible for the PKI strategy has declined from 26% to 14% of respondents.

Fifty-two percent of respondents say they have PKI specialists on staff who are involved in their organization's enterprise PKI. Of the 48% respondents who say their organizations do not have PKI specialists, many rely on consultants (45%) or service providers (55%).

A certificate authority (CA) provides assurance about the parties identified in a PKI certificate. Each CA maintains its own root CA for use only by the CA. The most popular method for deploying enterprise PKI continues to be through an internal corporate CA or an externally hosted private CA-managed service, according to 60% and 47% of respondents, respectively.

No clear ownership, insufficient skills, and requirements too fragmented or inconsistent are the top three challenges to enabling applications to use PKI. The challenge of no clear ownership continues to be the top challenge to deploying and managing PKI, according to 51% of respondents. Other challenges are insufficient skills (43% of respondents), and requirements are too fragmented or inconsistent (43% of respondents).

Key improvements in PKI adoption are reflected in the decline of critical challenges. Challenges that are declining significantly include the lack of resources (from 64% of respondents to 41% of respondents) and lack of visibility of the applications that will depend on PKI (from 48% to 33% of respondents).

As organizations strive to achieve greater PKI maturity, they anticipate the most change and uncertainty in PKI technologies and in working with vendors. Forty-three percent of respondents say PKI technologies and 41% of respondents say it will be with products and services.

Cloud-based services continue to be the No. 1 trend driving deployment of applications using PKI (46% of respondents). However, respondents who say IoT is the most important trend driving the deployment of applications using PKI has declined from 47% of respondents to 39% of respondents. BYOD and internal mobile device management has increased significantly from 24% of respondents to 34% of respondents.

More organizations are deploying certificate revocation techniques. In addition to verifying the CA's signature on a certificate, the application software must also be sure that the certificate is still trustworthy at the time of use. Certificates that are no longer trustworthy must be revoked by the CA. Those organizations that do not deploy a certificate revocation technique has declined significantly from 32% to 13%.

The certificate revocation technique most often deployed continues to be Online Certificate Status Protocol (OCSP), according to 45% of respondents. For the first time, the manual certificate revocation list is the second technique most often deployed.

Smart cards (for CA/root key protection) to manage the private keys for their root/policy/issuing CAs are used by 41% of respondents. Thirty-one percent of respondents say removable media for CA/root keys cards are used.

Organizations' primary root CA strategies are shifting significantly since 2021. A root certificate is a public key certificate that identifies a root CA. Both offline, self-managed and offline, externally hosted increased to 29% of respondents. Online, self-managed solutions decreased from 31% of respondents to 25% of respondents, while online, externally hosted solutions decreased from 21% to 17% of respondents.

Organizations with internal CAs use an average of 6.5 separate CAs, managing an average of 31,299 internal or externally acquired certificates. An average of 9.5 distinct applications, such as email and network authentication, are managed by an organization's PKI. This indicates that the PKI is at the core of the enterprise IT infrastructure. Not only the number of applications dependent upon the PKI, but the nature of them indicates that PKI is a strategic part of the core IT backbone.

Conflict with other apps using the same PKI is becoming a bigger challenge to enabling applications to use the same PKI. While the No. 1 challenge is not having sufficient skills, it has decreased from 43% to 37% of respondents.

Common Criteria Evaluation Assurance Level (EAL) 4+ and Federal Information Processing Standards (FIPS) 140-2 Level 3 continue to be the most important security certifications when deploying PKI infrastructure and PKI-based applications. Fifty-seven percent of respondents say Common Criteria EAL4+ is the most important security certification when deploying PKI. The evaluation at this level includes a comprehensive security assessment encompassing design testing and code review.

Fifty-five percent say FIPS 140-2 Level 3 is an important certification when deploying PKI. In the U.S., FIPS 140 is the standard called out by NIST in its definition of a "cryptographic module," which is mandatory for most U.S. federal government applications and a best practice in all PKI implementations.

SSL certificates for public-facing websites and services using PKI credentials is still the application most often used but has declined since 2022. Sixty-four percent of respondents say the application most often using PKI credentials is SSL certificates for public-facing websites and services. However, mobile device authentication and private cloud-based applications have increased as apps using PKI credentials (to 60% and 56% of respondents, respectively).

Scalability to millions of managed certificates continues to be the most important PKI capability for IoT deployments. While scalability is the most important, the support for elliptic curve cryptography (ECC) is the No. 2 most important PKI capability. ECC is an alternative technique to RSA and is considered a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

Today and in the next 12 months, the most important IoT security capabilities are delivering patches and updates to devices and monitoring device behavior. Device authentication will become more important in the next 12 months.

Post-Quantum Cryptography

For the first time, this 2024 global study features organizations' approach to achieving migration to post-quantum cryptography (PQC). As defined in the research, quantum computing is a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

Sixty-one percent of respondents plan to migrate to PQC within the next five years. The most popular path to PQC is implementation of pure PQC (36% of respondents) followed by a hybrid approach combining traditional crypto with PQC (31% of respondents), and thirdly test PQC with their organization's systems and applications (26% of respondents).

Many organizations are not prepared to achieve migration because of the lack of visibility and not having the right technologies. Only 45% of respondents say their organizations have full visibility into their cryptographic estate, and 50% of respondents say they have the right technology to support the larger key lengths and computing power required with PQC.

To prepare for migration, organizations need to know what cryptographic assets and algorithms they have and where they reside. It is important to know data flows and where organizations' long-life data resides that is sensitive and must remain confidential. To achieve full visibility, organizations need to ensure they have a full and clear inventory of all the cryptographic assets (keys, certificates, secrets, and algorithms across the environment) and what is being secured.

Organizations are slow to prepare for the quantum threat. The quantum threat, sometimes referred to as "post-quantum," is the inevitability that within the decade a quantum computer will be capable of breaking traditional public key cryptography. Experts surveyed by the Global Risk Institute predict quantum computing will compromise cybersecurity as early as 2027.

Most respondents are not preparing for the quantum threat. Twenty-seven percent of respondents say their organizations have not yet considered the impact of the threat, 23% are aware of the potential impact but haven't started to create a strategy, and 9% are unsure if their organizations are preparing for the quantum threat.

To prepare for the quantum threat, 44% of respondents say their organizations are building a post-quantum cryptography strategy. Although it is recommended as a best practice, only 38% of respondents say their organization is taking an inventory of its cryptographic assets and/or ensuring it is crypto-agile. Crypto-agility is the capacity for an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant change to system infrastructure.

To protect against the quantum threat, organizations need to be able to have an inventory of their cryptographic assets and achieve a fully crypto-agile approach to be able to easily transition from one algorithm to another. Improving the ability to have a complete inventory of cryptographic assets (43% of respondents) and to achieve crypto-agility (40% of respondents) are the top two concerns.

Crypto-agility is critical to the migration to PQC. Crypto-agility is the capacity for an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant change to system infrastructure. Only 28% of respondents say their organizations have a fully implemented crypto-agile approach.

Part 2

Key Findings

Part 2

KEY FINDINGS

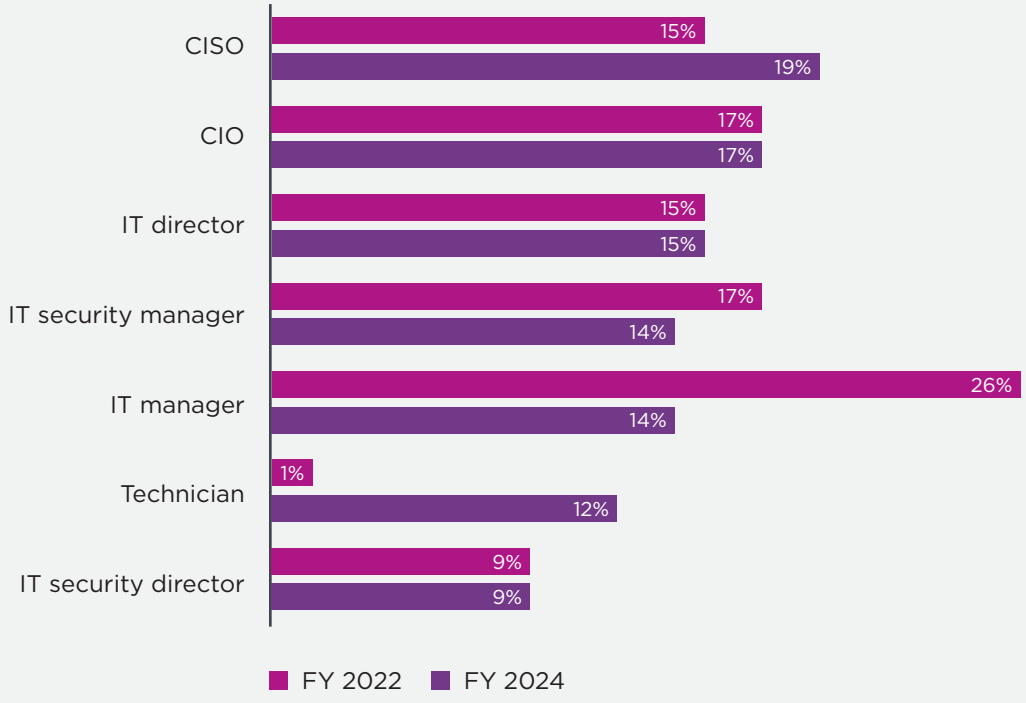
In this section of the report, whenever possible we provide an analysis of the global PKI results over a five-year period from 2019 to 2024.

Trends in achieving PKI maturity and managing IoT keys

Responsibility for the PKI strategy is being assigned to IT security and IT leaders. According to Figure 1, as PKI becomes increasingly critical to an organization's security posture, the CISO and CIO are most responsible for their organization's PKI strategy. The IT manager being most responsible for the PKI strategy has declined from 26% of respondents to 14%.

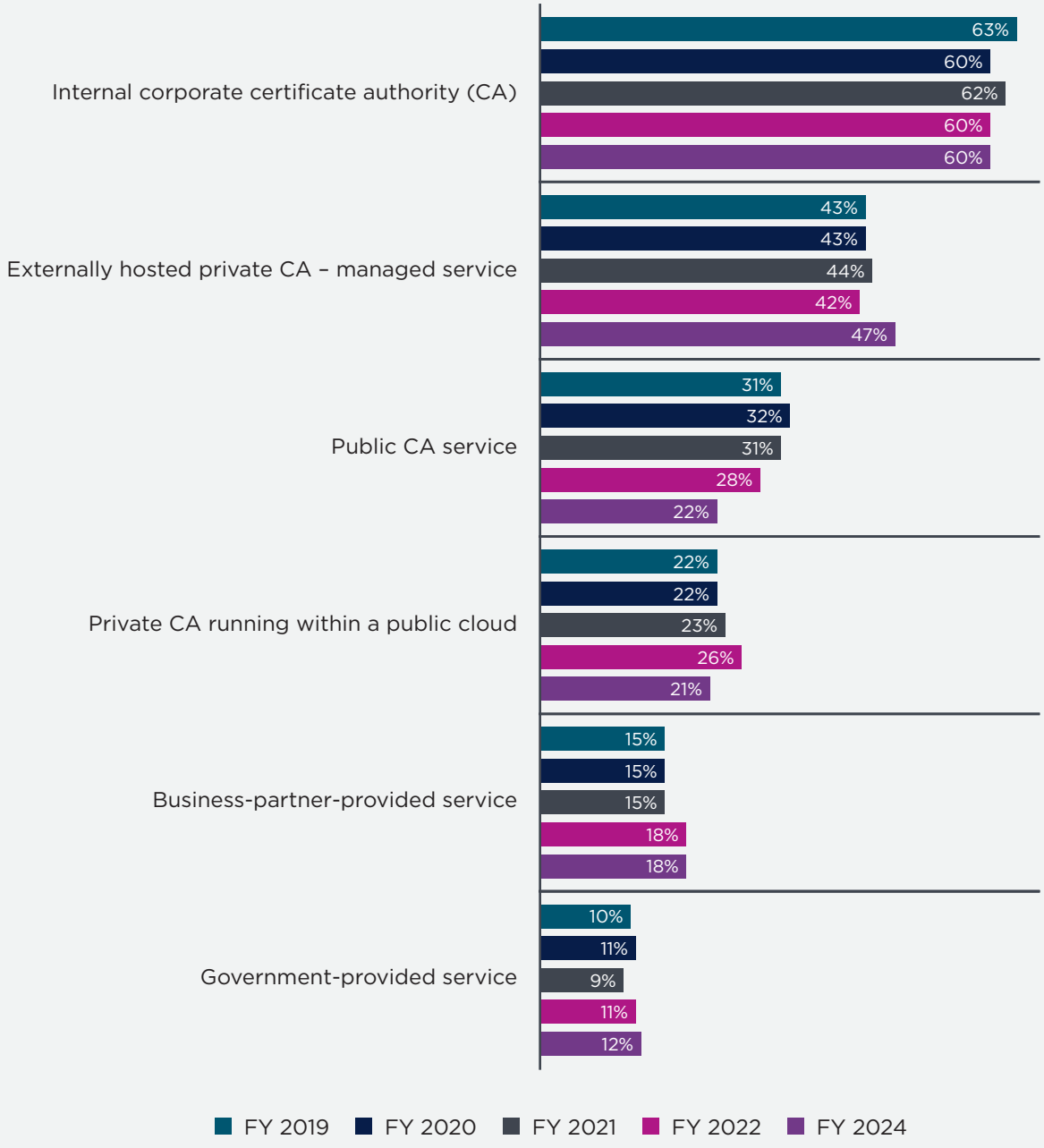
Fifty-two percent of respondents say they have PKI specialists on staff who are involved in their organization's enterprise PKI. Of the 48% respondents who say their organizations do not have PKI specialists, many rely on consultants (45%) or service providers (55%).

Figure 1. **Who is most responsible for your organization's PKI strategy?**



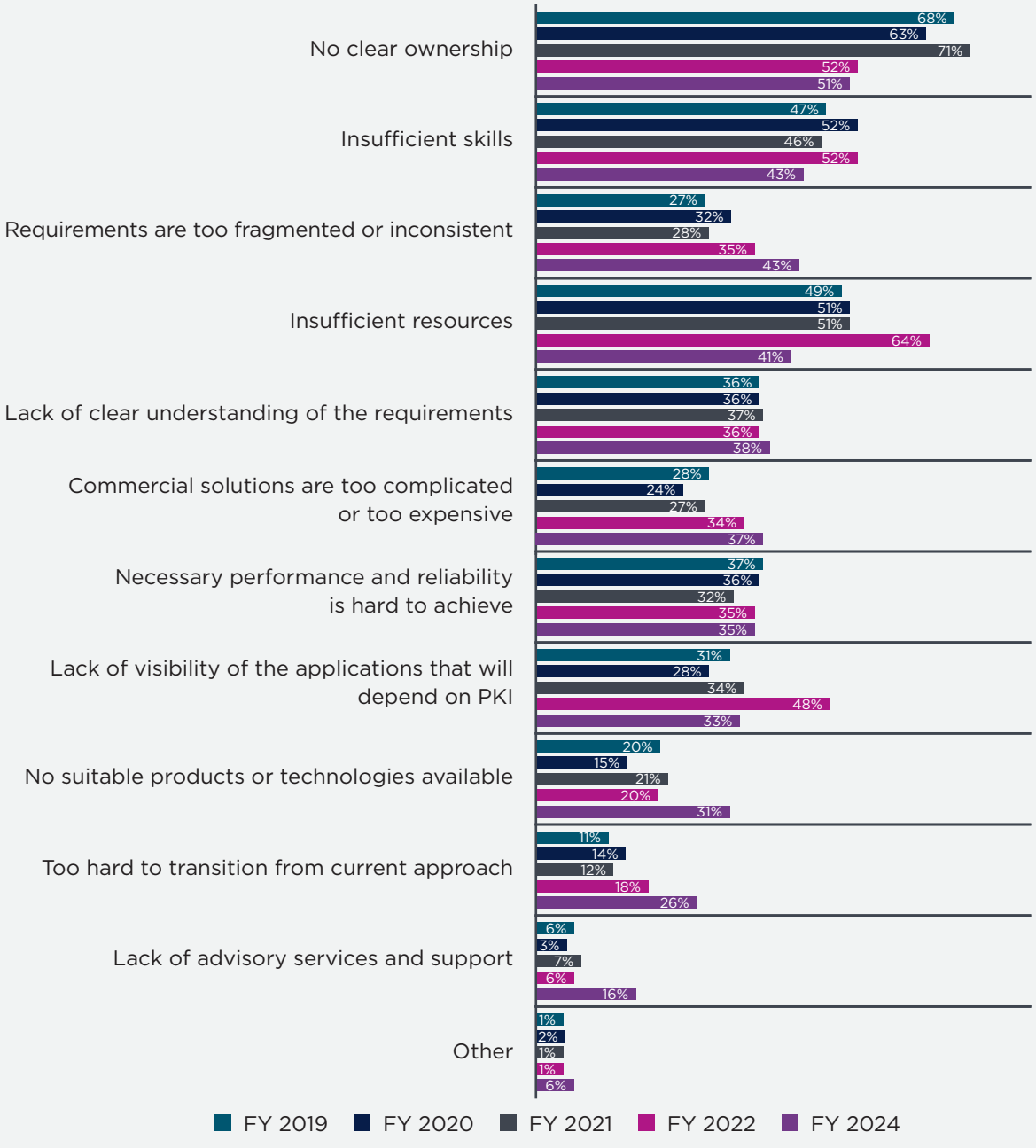
A certificate authority (CA) provides assurance about the parties identified in a PKI certificate. Each CA maintains its own root CA for use only by the CA. As shown in Figure 2, the most popular method for deploying enterprise PKI continues to be through an internal corporate CA or an externally hosted private CA – managed service, according to 60% and 47% of respondents, respectively.

Figure 2. **What describes how your organization's enterprise PKI is deployed?** Please select all that apply.



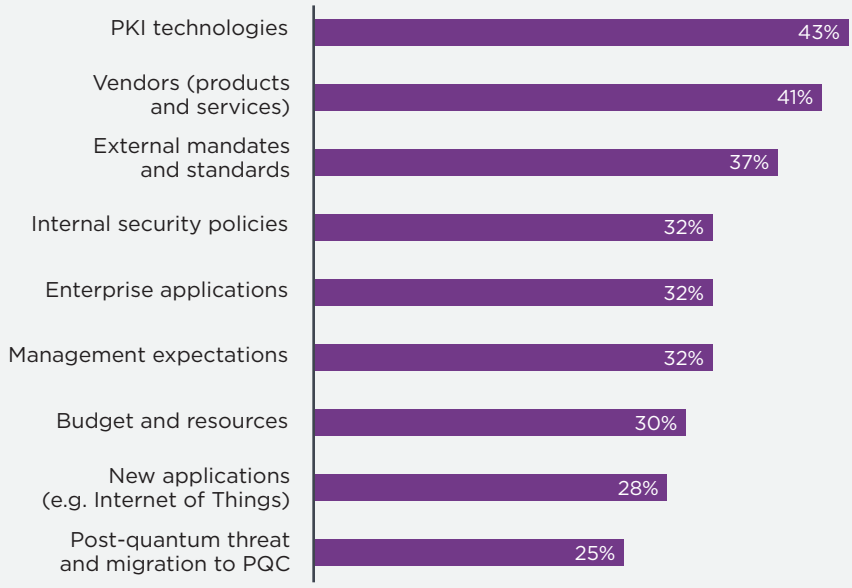
No clear ownership, insufficient skills, and requirements being too fragmented or inconsistent are the top three challenges to enabling applications to use PKI. As shown in Figure 3, the challenge of no clear ownership continues to be the top challenge to deploying and managing PKI, according to 51% of respondents. Other challenges are insufficient skills (43% of respondents), and requirements being too fragmented or inconsistent (43% of respondents). Challenges that are declining significantly include the lack of resources (from 64% to 41% of respondents) and lack of visibility of the applications that will depend on PKI (from 48% of respondents to 33% of respondents).

Figure 3. **The challenges in deploying and managing PKI**
Four responses permitted.



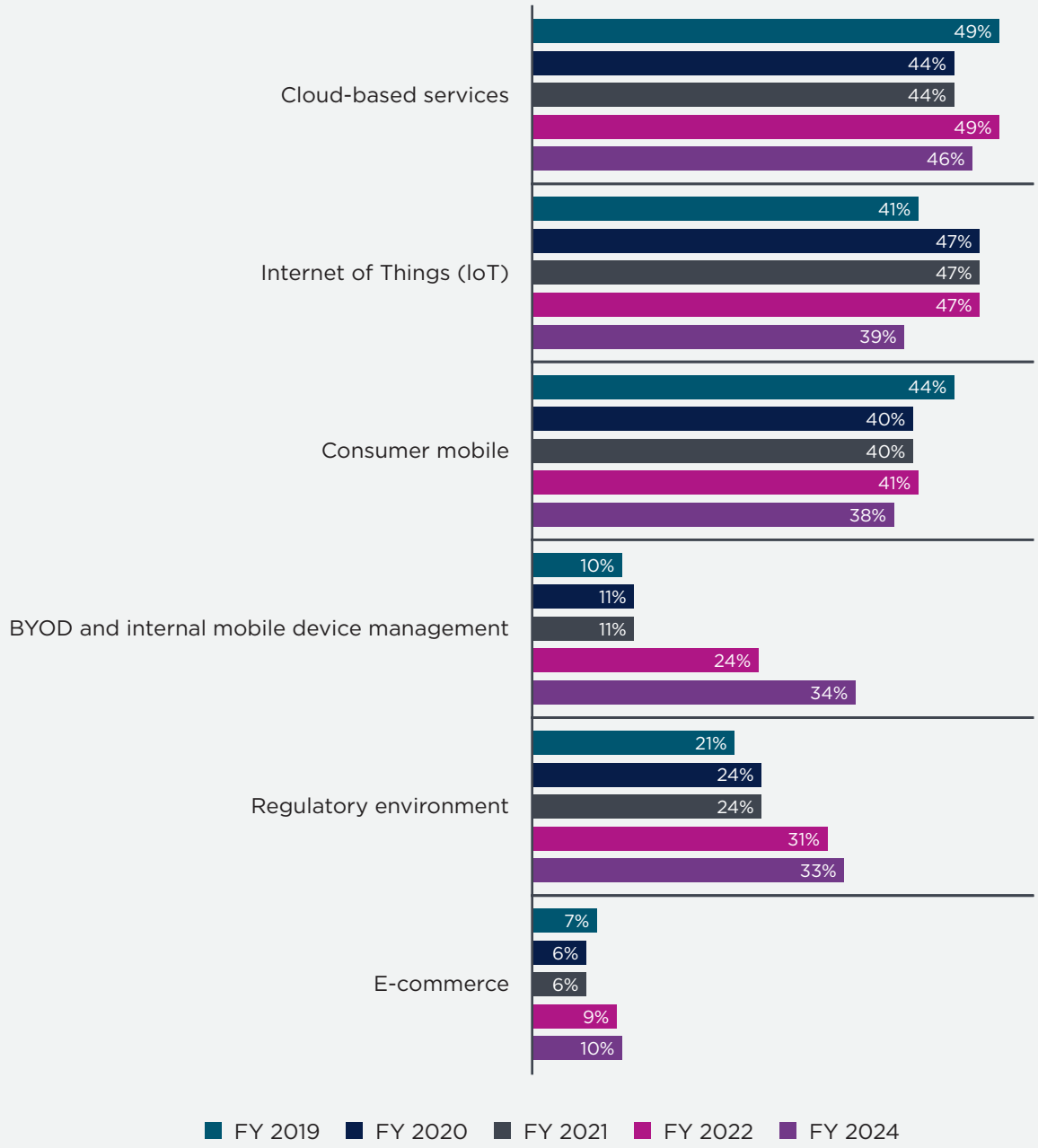
As organizations strive to achieve greater PKI maturity, they anticipate the most change and uncertainty in PKI technologies and with vendors. According to Figure 4, 43% of respondents say PKI technologies and 41% of respondents say it will be with products and services.

Figure 4. **As organizations plan the evolution of their PKI, what areas are expected to experience the most change and uncertainty?**
Three responses permitted.



As shown in Figure 5, cloud-based services continue to be the No. 1 trend driving deployment of applications using PKI (46% of respondents). However, respondents who say IoT is the most important trend driving the deployment of applications using PKI has declined from 47% of respondents to 39% of respondents. BYOD and internal mobile device management has increased significantly from 24% of respondents to 34% of respondents.

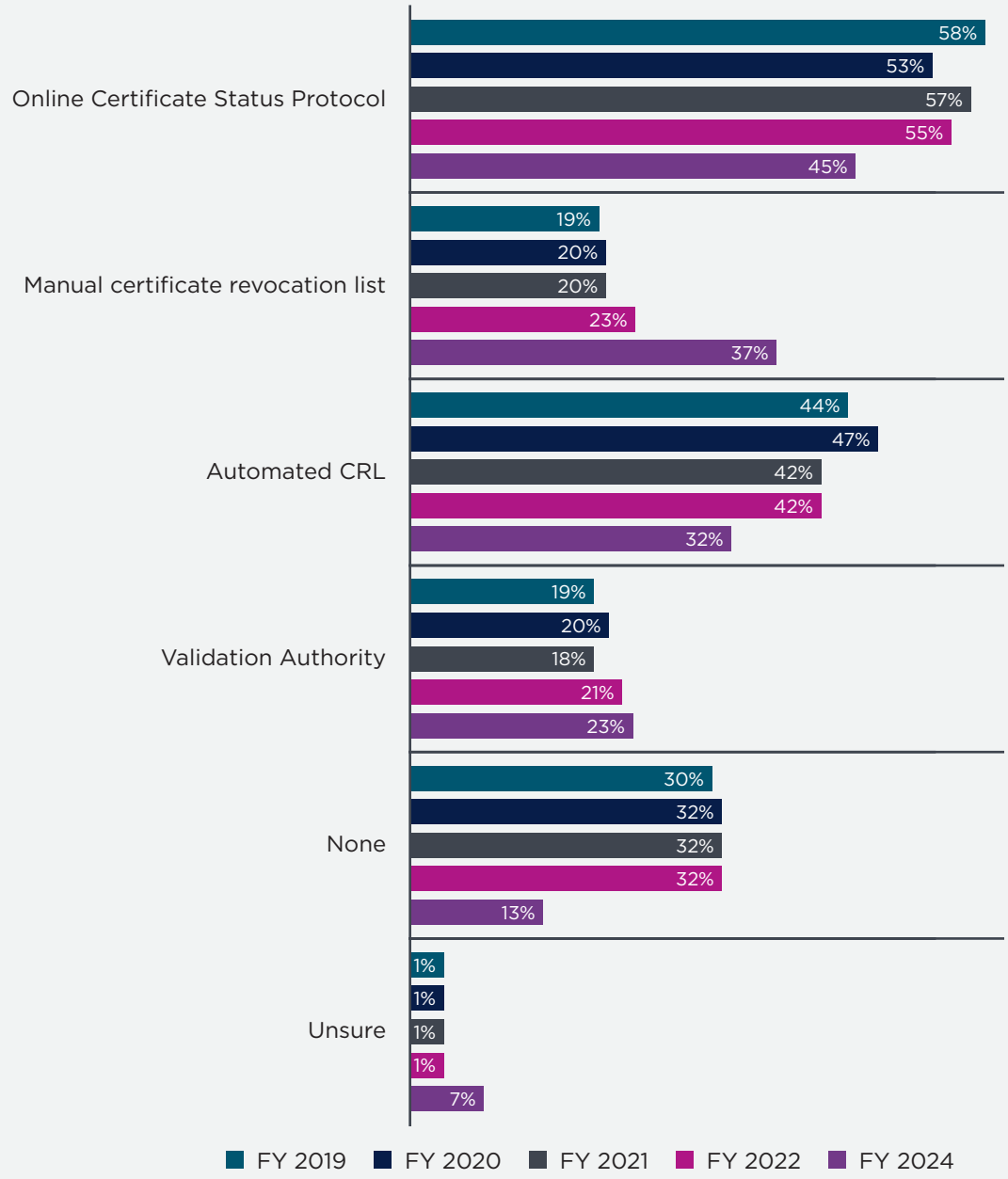
Figure 5. **The most important trends driving the deployment of applications using PKI**
Two responses permitted.



More organizations are deploying certificate revocation techniques. In addition to verifying the CA's signature on a certificate, the application software must also be sure that the certificate is still trustworthy at the time of use. Certificates that are no longer trustworthy must be revoked by the CA.

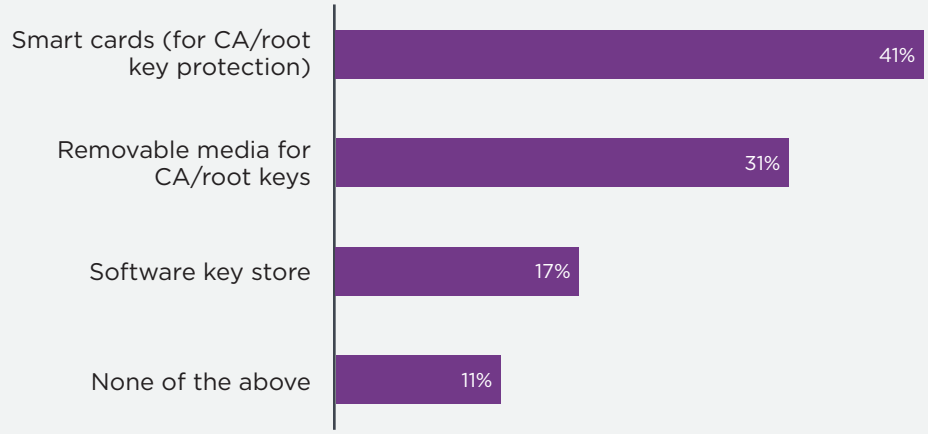
Those organizations that do not deploy a certificate revocation technique has declined significantly from 32% to 13%. The certificate revocation technique most often deployed continues to be Online Certificate Status Protocol (OCSP), according to 45% of respondents. For the first time, the manual certificate revocation list is the second technique most often deployed.

Figure 6. **The certificate revocation techniques used in enterprises**
More than one response permitted.



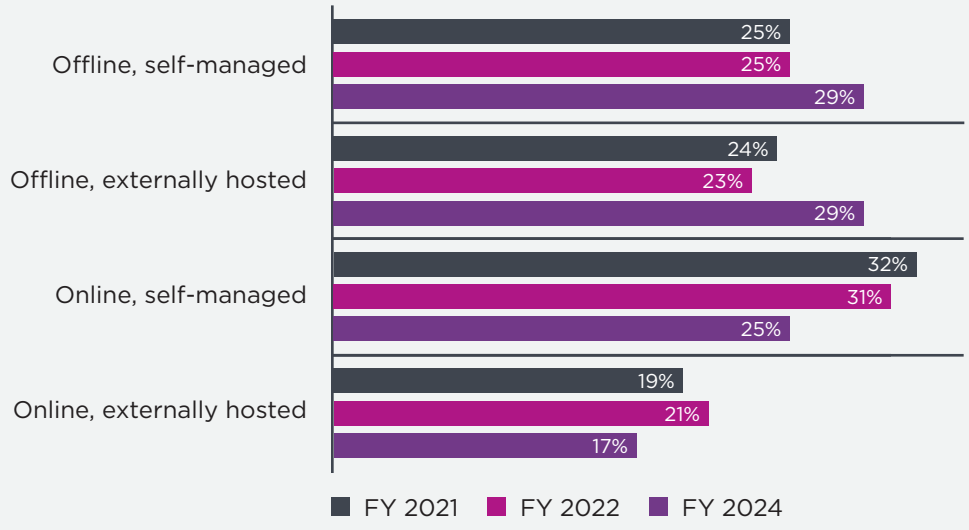
Smart cards (for CA/root key protection) to manage the private keys for their root/policy/issuing CAs are used by 41% of respondents. As shown in Figure 7, 31% of respondents say removable media for CA/root keys are used.

Figure 7. **How do you manage the private keys for your root/policy/issuing CAs?**



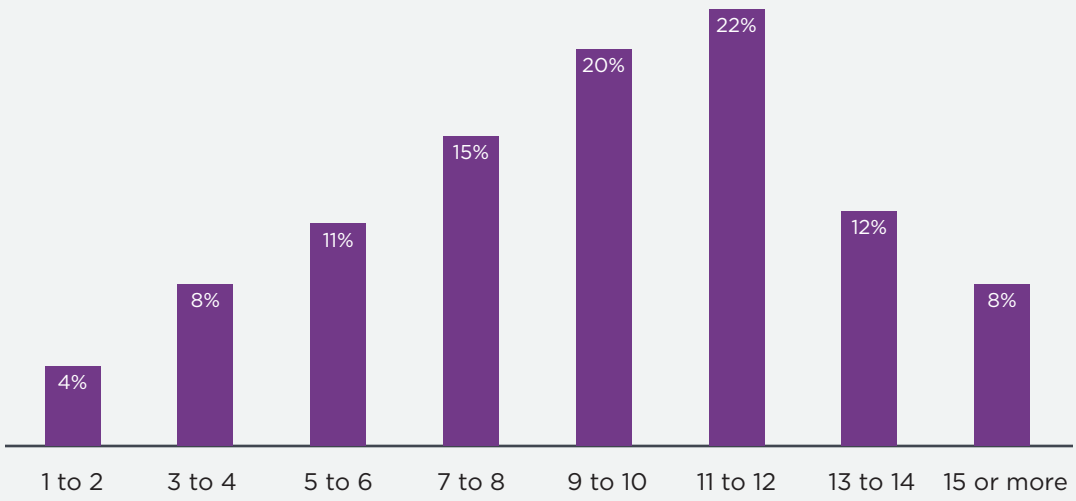
Organizations' primary root CA strategies are shifting significantly since 2021. A root certificate is a public key certificate that identifies a root CA. Figure 8 shows changes in CA root strategies used by organizations. Both offline, self-managed and offline, externally hosted increased to 29% of respondents. Online, self-managed decreased from 31% to 25% of respondents, and online, externally hosted decreased from 21% of respondents to 17% of respondents.

Figure 8. **What is your organization's primary root CA strategy?**
Only one choice permitted.



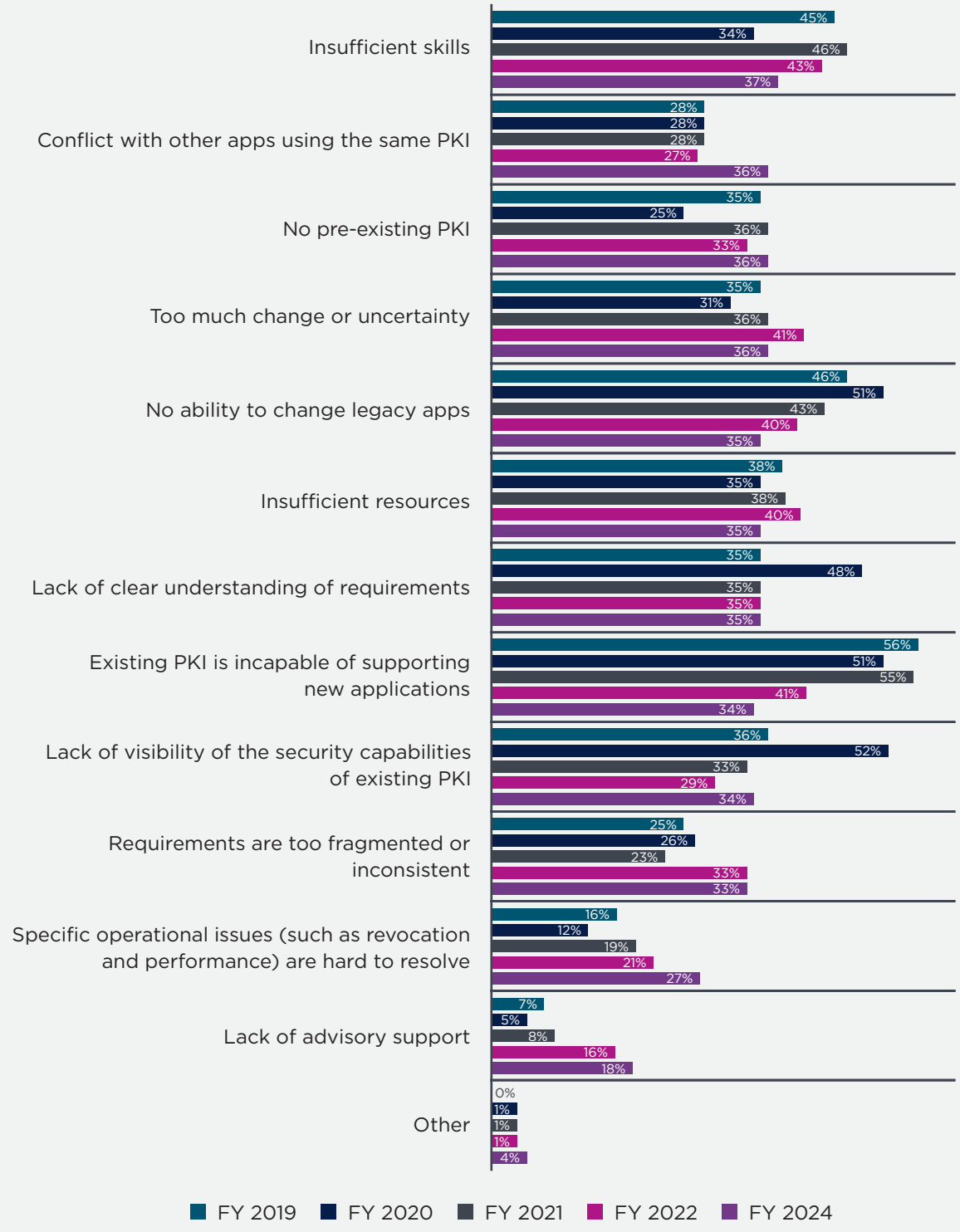
Organizations with internal CAs use an average of 6.5 separate CAs, managing an average of 31,299 internal or externally acquired certificates. As shown in Figure 9, an average of 9.5 distinct applications, such as email and network authentication, are managed by an organization's PKI. This indicates that the PKI is at the core of the enterprise IT infrastructure. Not only the number of applications dependent upon the PKI but the nature of them indicates that PKI is a strategic part of the core IT backbone.

Figure 9. **How many distinct applications does your PKI manage certificates on behalf of?** Extrapolated value is 9.5 distinct applications.



Conflict with other apps using the same PKI is becoming a bigger challenge to enabling applications to use the same PKI. As shown in Figure 10, while the No. 1 challenge is not having sufficient skills, it has decreased from 43% of respondents to 37% of respondents.

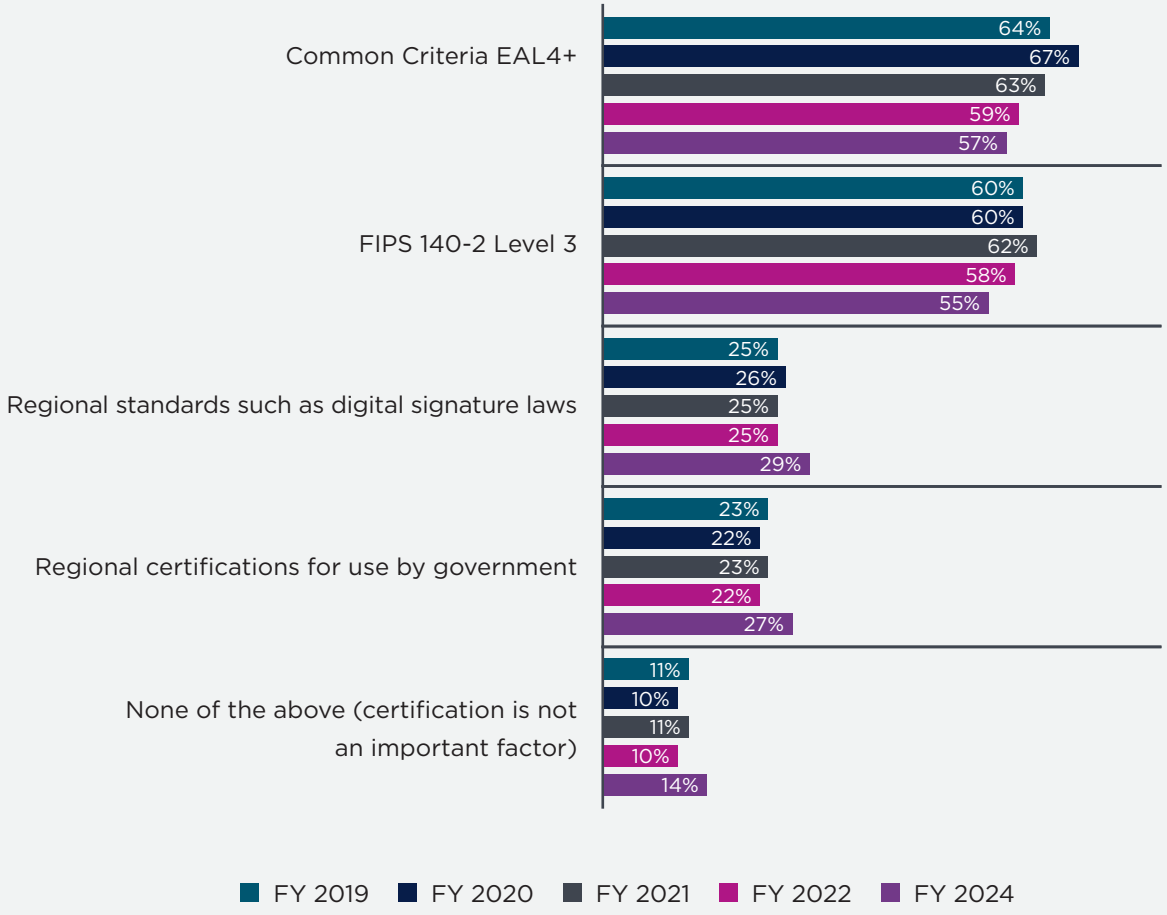
Figure 10. **What are the challenges to enable applications to utilize PKI?**
Four responses permitted.



Common Criteria Evaluation Assurance Level (EAL) 4+ and Federal Information Processing Standards (FIPS) 140-2 Level 3 continue to be the most important security certifications when deploying PKI infrastructure and PKI-based applications. As shown in Figure 11, 57% of respondents say Common Criteria EAL4+ is the most important security certification. The evaluation at this level includes a comprehensive security assessment encompassing design testing and code review.

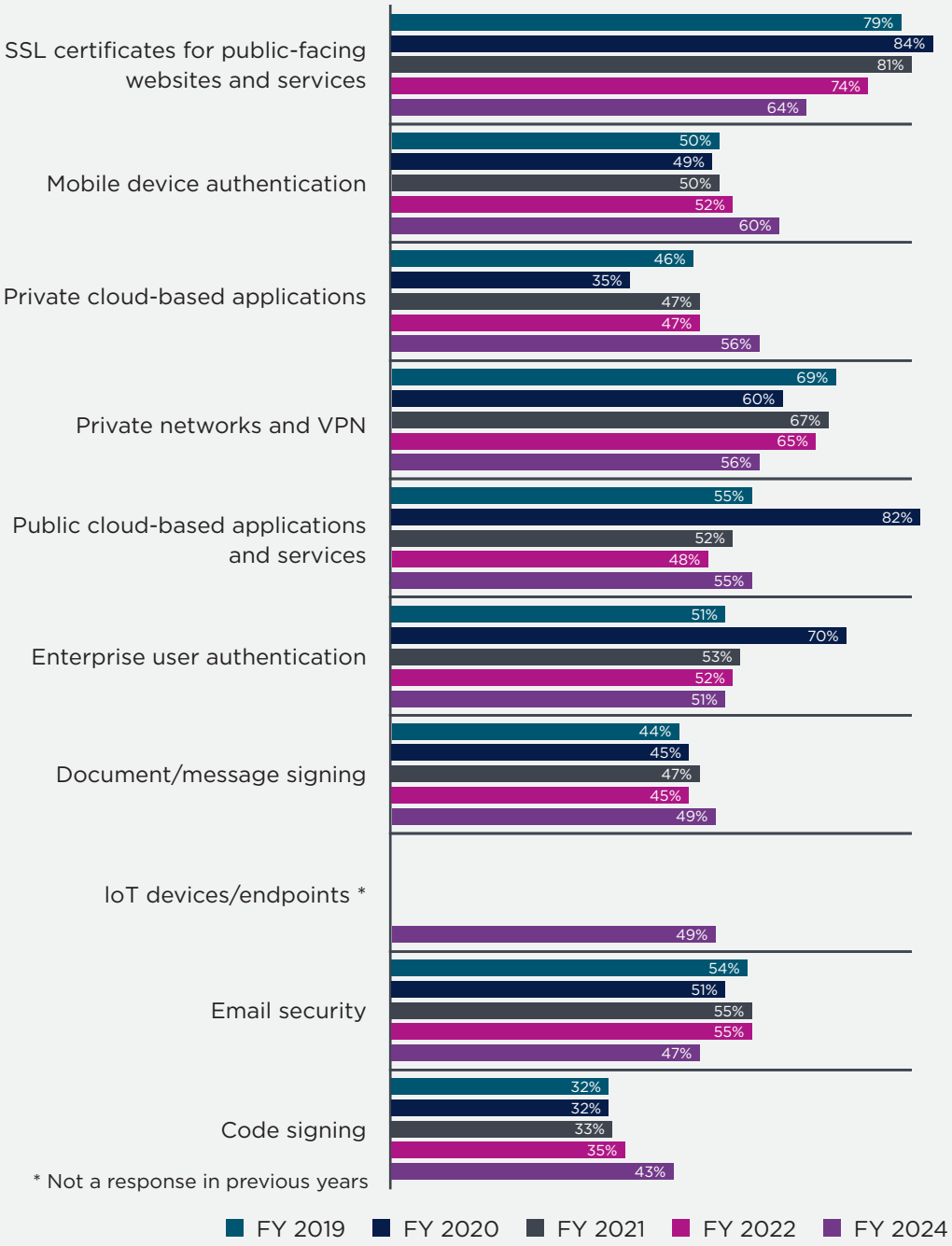
Fifty-five percent say FIPS 140-2 Level 3 is an important certification when deploying PKI. In the U.S., FIPS 140 is the standard called out by NIST in its definition of a "cryptographic module," which is mandatory for most U.S. federal government applications and a best practice in all PKI implementations.

Figure 11. **Security certifications important when deploying PKI infrastructure**
Consolidated view; more than one response permitted.



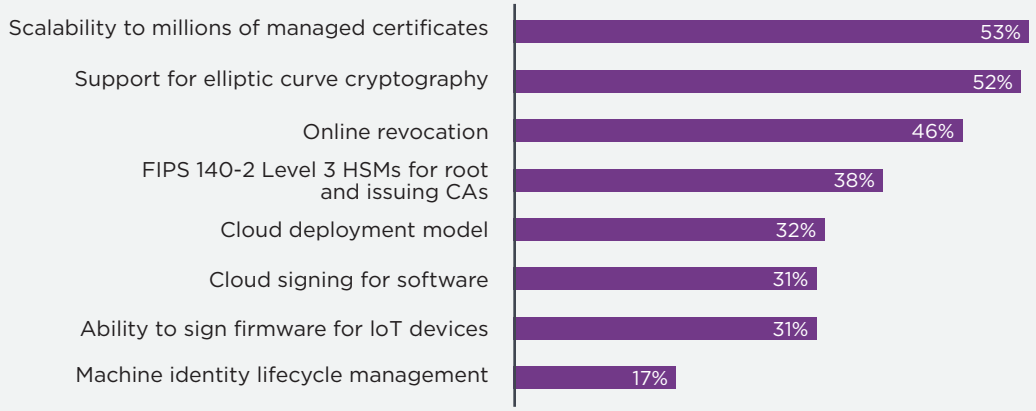
SSL certificates for public-facing websites and services using PKI credentials is still the application most often used but has declined since 2022. According to Figure 12, 64% of respondents say the application most often using PKI credentials is SSL certificates for public-facing websites and services. However, mobile device authentication and private cloud-based applications have increased as a result of apps using PKI credentials (to 60% and 56% of respondents, respectively).

Figure 12. **What applications use PKI credentials in organizations?**
More than one response permitted.



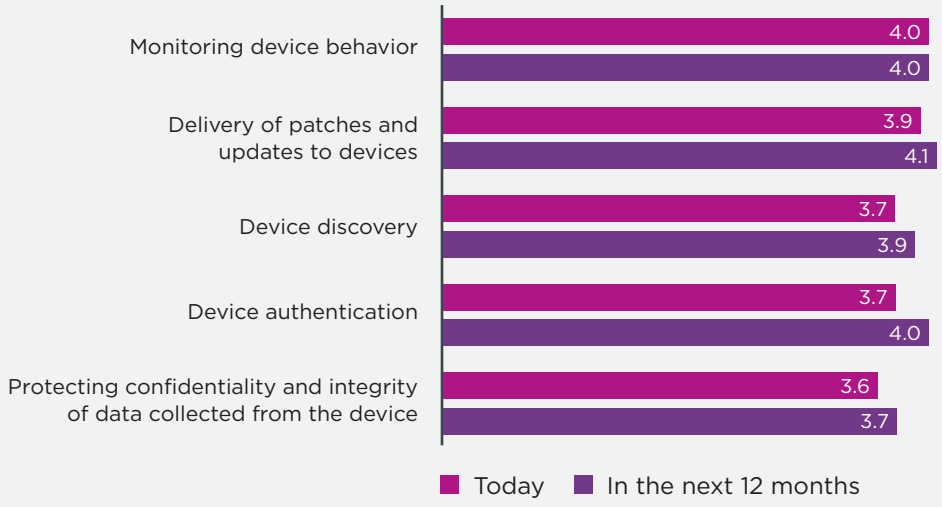
Scalability to millions of managed certificates continues to be the most important PKI capability for IoT deployments. Figure 13 lists the most important PKI capabilities for IoT deployments. While scalability is the most important, the support for elliptic curve cryptography (ECC) is the No. 2 most important PKI capability. ECC is an alternative technique to RSA and is considered a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

Figure 13. **What are the most important PKI capabilities for IoT deployments?**
Three responses permitted.



Today and in the next 12 months, the most important IoT security capabilities are delivering patches and updates to devices and monitoring device behavior. As shown in Figure 14, device authentication will become more important in the next 12 months.

Figure 14. **How important are the following IoT security capabilities to your organization today and in the next 12 months?**
On a scale from 1 = not important to 5 = very important

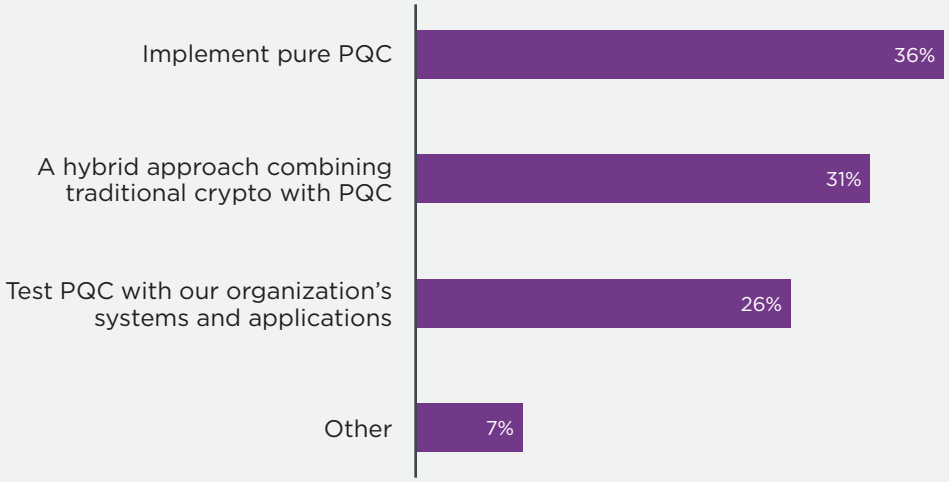


Post-Quantum Cryptography

For the first time, this 2024 global study features organizations' approach to achieving migration to post-quantum cryptography (PQC). As defined in the research, quantum computing is a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

Sixty-one percent of respondents plan to migrate to PQC within the next five years. Figure 15 presents three options to achieve migration. The most popular is implementation of pure PQC (36% of respondents) followed by a hybrid approach combining traditional crypto with PQC (31% of respondents), and test PQC with their organization's system and applications (26% of respondents).

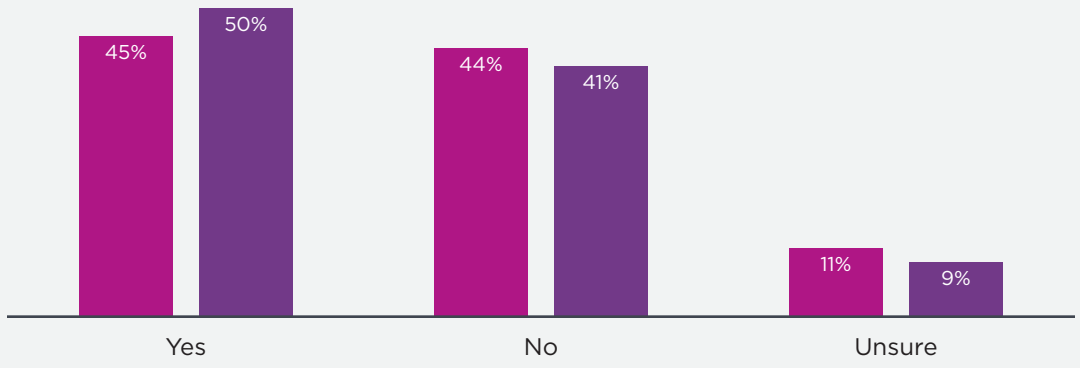
Figure 15. **How will your organization achieve migration to PQC?**
One choice permitted.



Many organizations are not prepared to achieve migration because of the lack of visibility and not having the right technologies. As shown in Figure 16, only 45% of respondents say their organizations have full visibility into their cryptographic estate and 50% of respondents say they have the right technology to support the larger key lengths and computing power required with PQC.

To prepare for migration, organizations need to know what cryptographic assets and algorithms they have and where they reside. It is important to know data flows and where organizations' long-life data resides that is sensitive and must remain confidential. To achieve full visibility, organizations need to ensure they have a full and clear inventory of all the cryptographic assets (keys, certificates, secrets, and algorithms across the environment) and what is being secured.

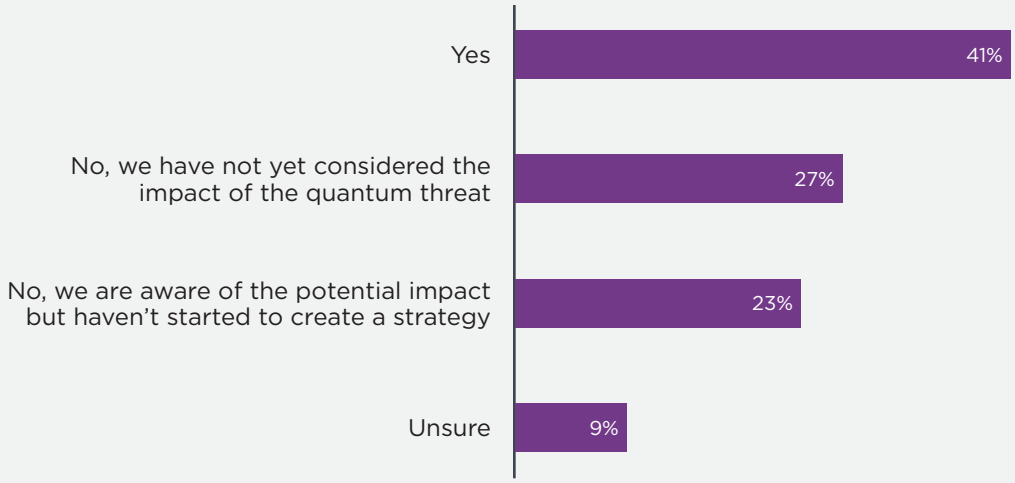
Figure 16. **Does your organization have full visibility into its entire cryptographic estate and the right technology to support the larger key lengths and computing power required with PQC?**



Organizations are slow to prepare for the quantum threat. The quantum threat, sometimes referred to as "post-quantum," is the inevitability that within the decade, a quantum computer will be capable of breaking traditional public key cryptography. Experts surveyed by the Global Risk Institute predict quantum computing will compromise cybersecurity as early as 2027.

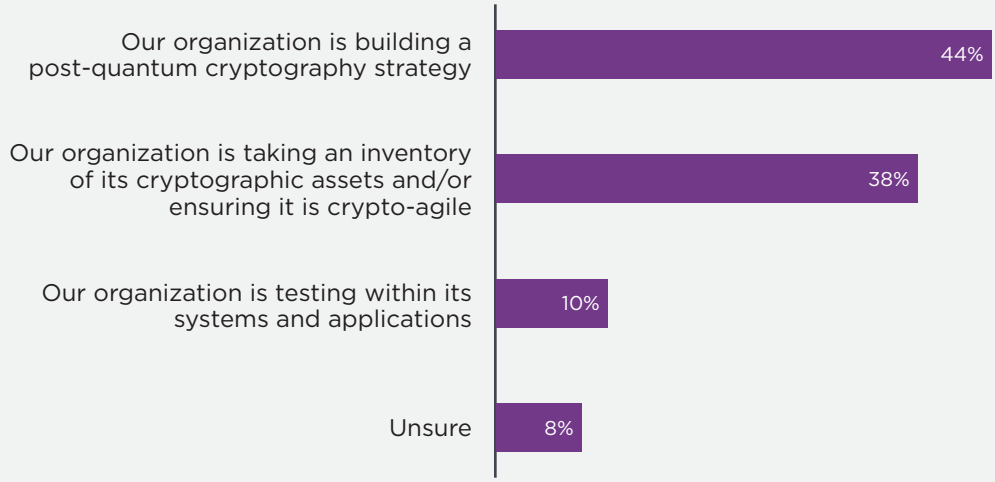
As shown in Figure 17, most respondents are not preparing for the quantum threat. Twenty-seven percent of respondents say their organizations have not yet considered the impact of the threat, 23% say they are aware of the potential impact but haven't started to create a strategy, and 9% are unsure.

Figure 17. **Is your organization preparing for the quantum threat?**



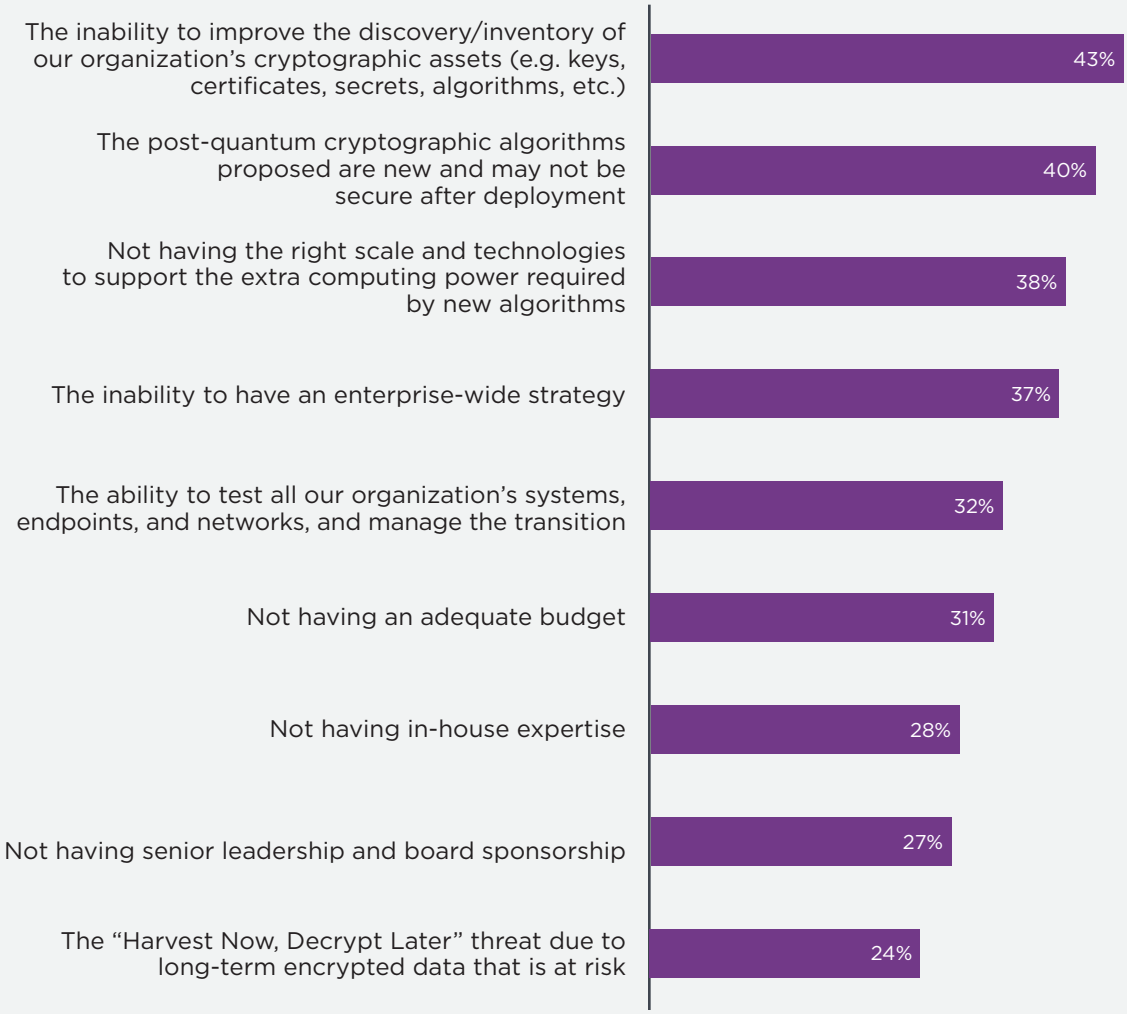
To prepare for the quantum threat, 44% of respondents say their organizations are building a post-quantum cryptography strategy, as shown in Figure 18. Although it is recommended as a best practice, only 38% of respondents say their organization is taking an inventory of its cryptographic assets and/or ensuring it is crypto-agile. Crypto-agility is the capacity for an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant change to system infrastructure.

Figure 18. **If yes, at what stage in preparing for the quantum threat is your organization?**
One choice permitted.



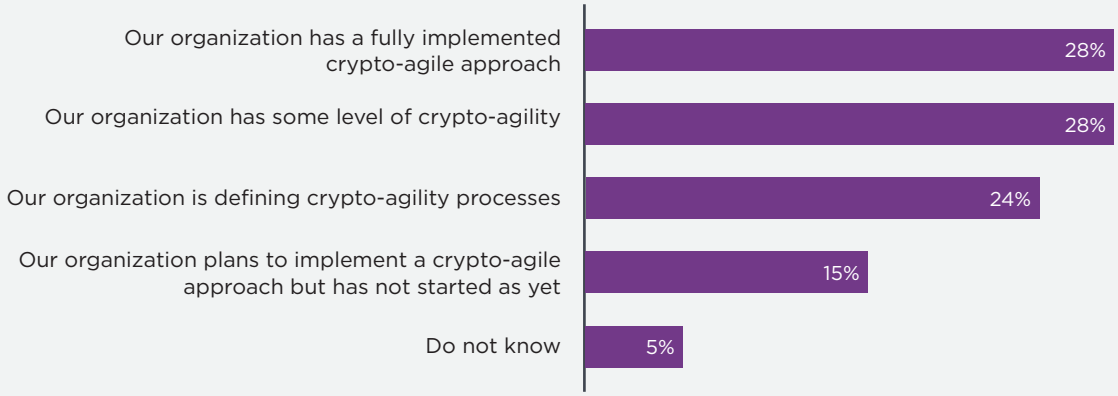
To protect against the quantum threat, organizations need to be able to have an inventory of their cryptographic assets and achieve a fully crypto-agile approach to be able to easily transition from one algorithm to another. Figure 19 presents a list of concerns organizations have that will impede the successful transition to PQC and minimize the quantum threat. Improving the ability to have a complete inventory of cryptographic assets (43% of respondents) and to achieve crypto-agility (40% of respondents) are the top two concerns.

Figure 19. **What are your greatest concerns when it comes to the quantum threat and migration to PQC?**
Three responses permitted.



Crypto-agility is critical to the migration to PQC. Crypto-agility is the capacity for an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant change to system infrastructure. As shown in Figure 20, only 28% of respondents say their organizations have a fully implemented crypto-agile approach.

Figure 20. **What is the current state of your organization's crypto-agility?**
One choice permitted.

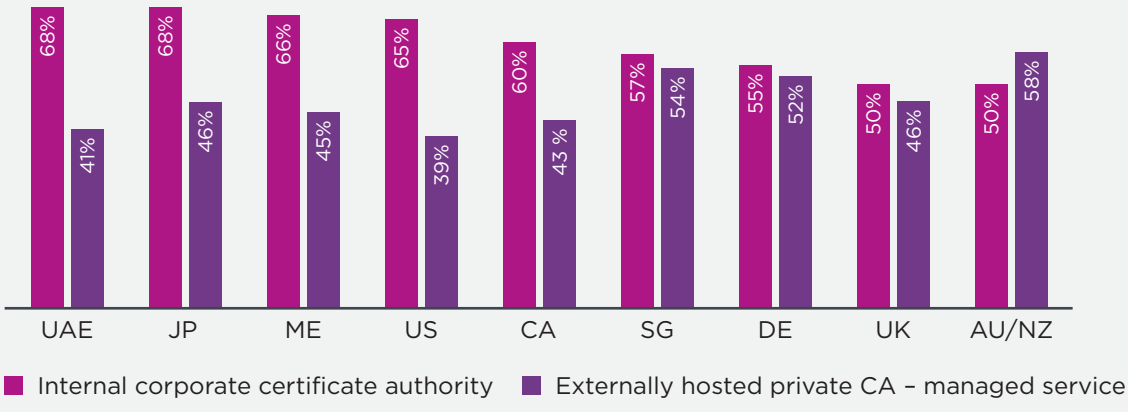


Global Analysis

In this section, we provide the most salient differences among the nine countries and regions represented in this study: Australia/NZ (AU/NZ), Canada (CA), Germany (DE), Japan (JP), Saudi Arabia/Middle East (ME), Singapore (SG), United Arab Emirates (UAE), United Kingdom (UK), and the United States.

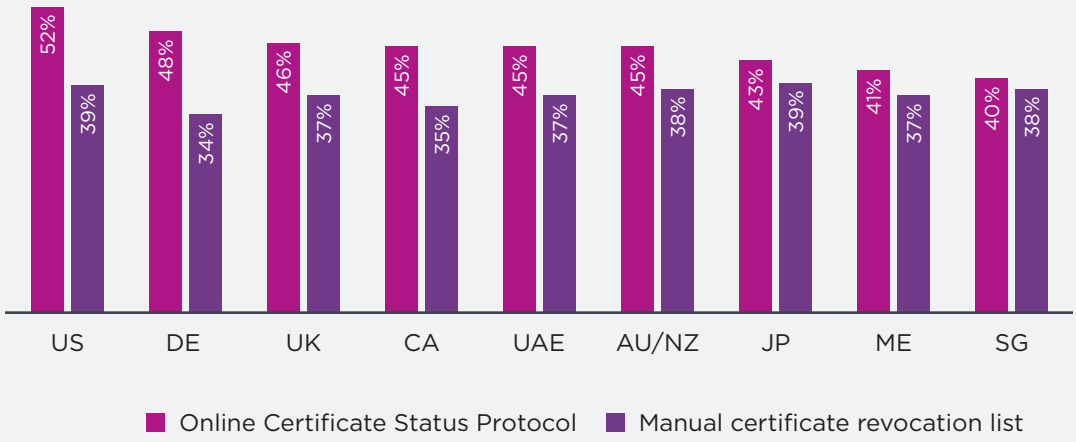
With the exception of Australia/New Zealand, organizations are deploying enterprise PKI through internal corporate certificate authorities, as shown in Figure 21.

Figure 21. **How would you describe how your organization's enterprise PKI is deployed?**
Top 2 choices



Only 13% of respondents say their organizations do not use a certificate revocation technique. As shown in Figure 22, of those respondents who say their organizations use a certificate revocation technique, the United States (52% of respondents), Germany (48% of respondents), and the United Kingdom (46% of respondents) are most likely to use the Online Certificate Status Protocol (OCSP). The least likely to use OCSP are Singapore (40% of respondents) and the Middle East (41% of respondents).

Figure 22. **Which certificate revocation technique does your organization deploy?**
Top 2 choices = OCSP and Manual CRL



According to Figure 23, Singapore and Japan have the most individual CAs deployed within their organizations (6.5 and 6.3, respectively).

Figure 23. **What best describes the number of issuing CAs in your organization?**
Extrapolated average values

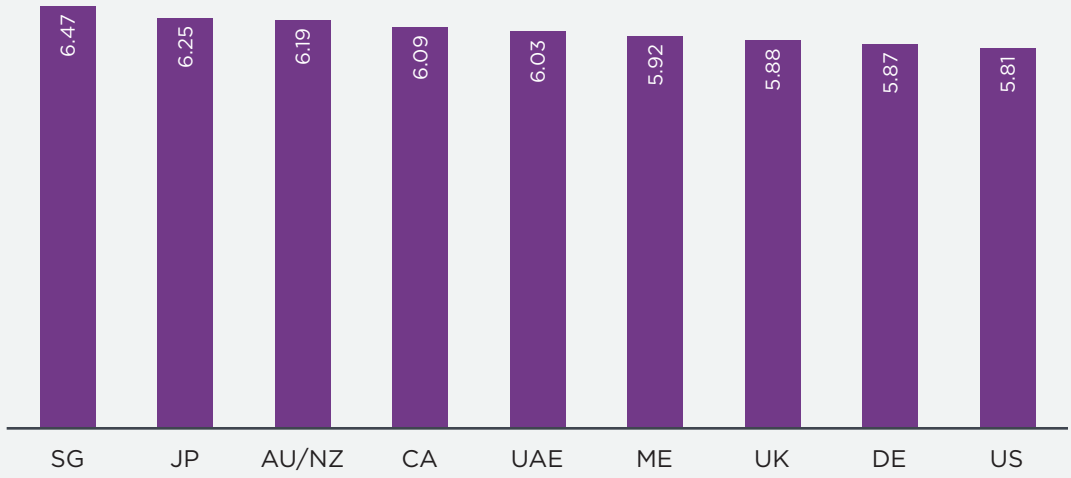


Figure 24 is the number of distinct applications (e.g. email, network authentication, etc.) for which PKI manages certificates. The U.S. at 11.2 has the largest number of distinct applications. Taiwan (6.9) and Russia (6.5) have the least number of distinct applications.

Figure 24. **How many distinct applications does your PKI manage certificates on behalf of?**
Extrapolated average values

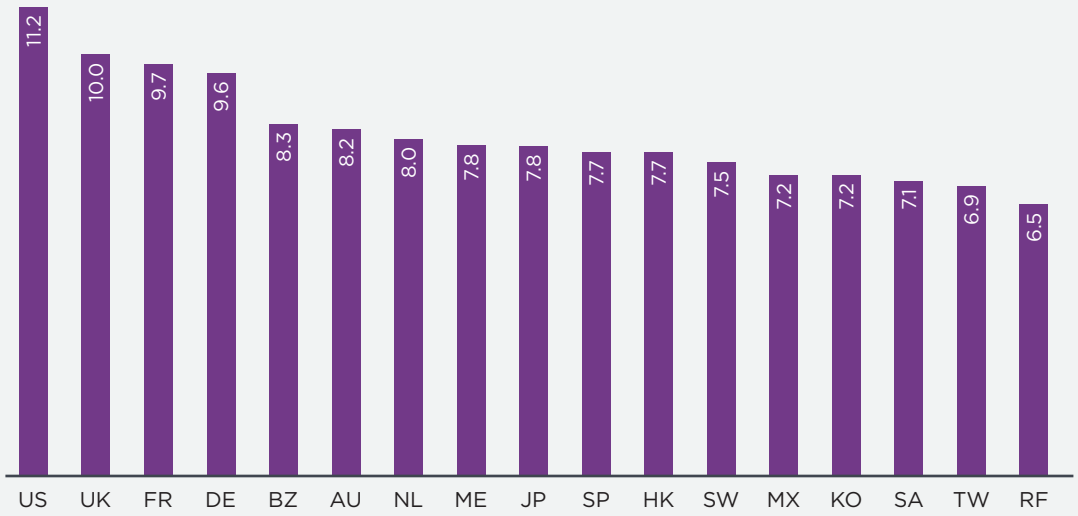
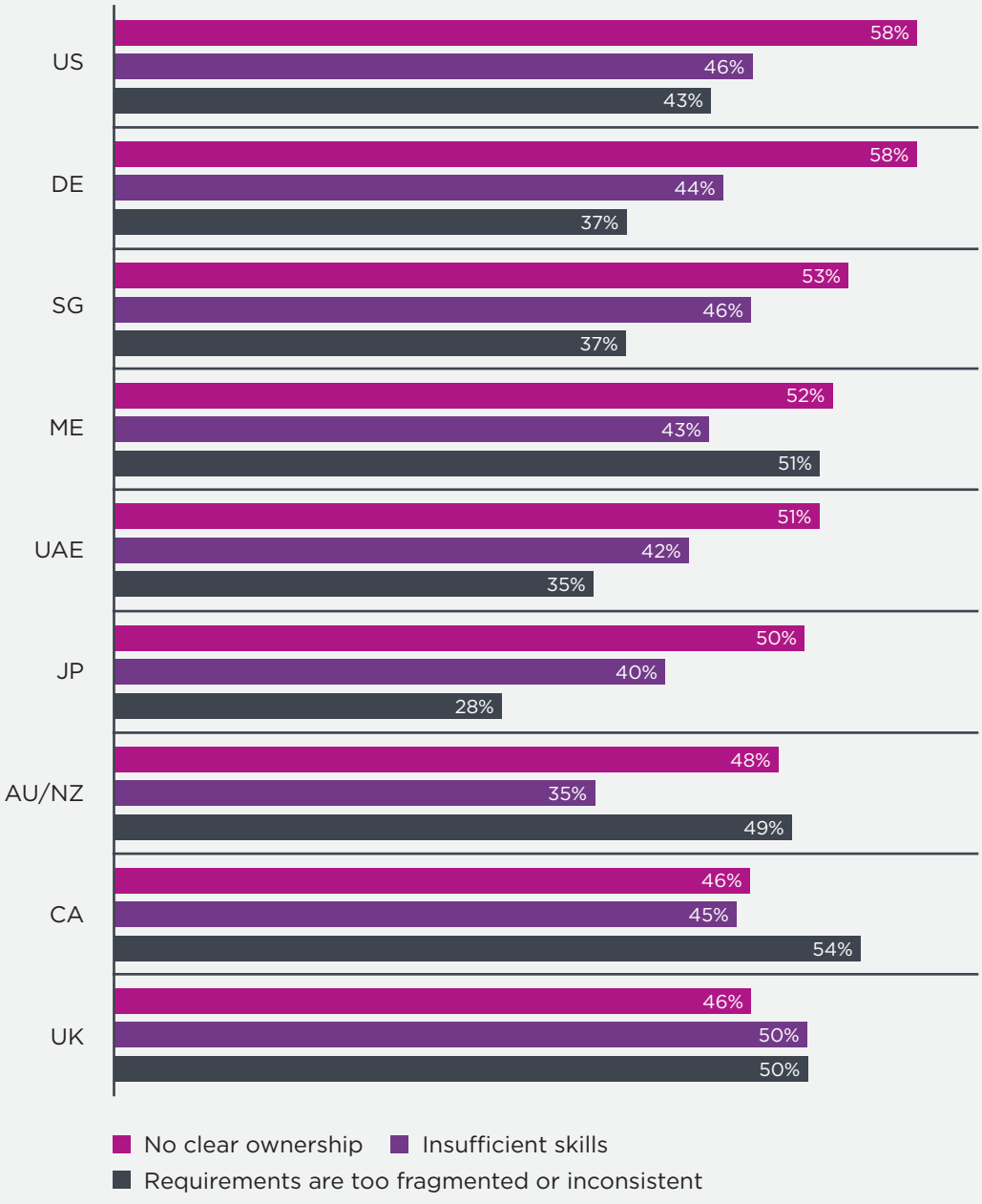


Figure 25 reports the three most salient challenges in deploying and managing PKI. As shown, the United States (58% of respondents), Germany (58% of respondents), Singapore (53% of respondents), the Middle East (52% of respondents), the UAE (51% of respondents), and Japan (50% of respondents) say the biggest challenge is no clear ownership.

There is a consistent theme in these responses. We can see the importance of PKI growing and its integration with core IT applications. Also, PKI's near-term future is being buffeted by trends toward the cloud, mobility, and IoT. However, globally there is the problem of no clear ownership.

Figure 25. **What are the main challenges in deploying and managing PKI?**
Top 3 choices



As organizations plan the evolution of their PKI, where are the greatest areas of possible change and uncertainty? Figure 26 provides the top two choices. Accordingly, in the United States (50% of respondents), Japan (46% of respondents), the Middle East (42% of respondents), Singapore (42% of respondents), and the United Kingdom (42% of respondents) say PKI technologies are the greatest areas of change. In Australia/New Zealand, 47% of respondents say vendors are most likely to be an area of great change and uncertainty.

Figure 26. **Where are the greatest areas of change and uncertainty in the evolution of your PKI?**
Top 2 choices

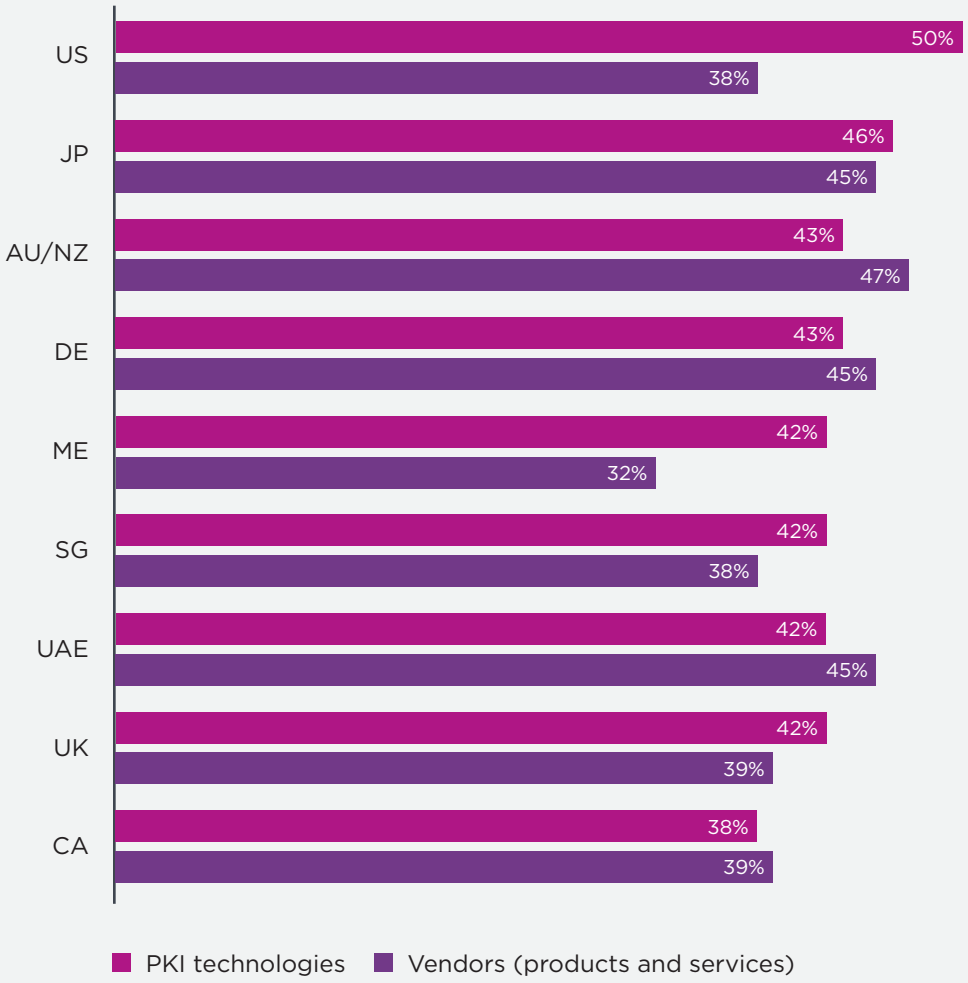
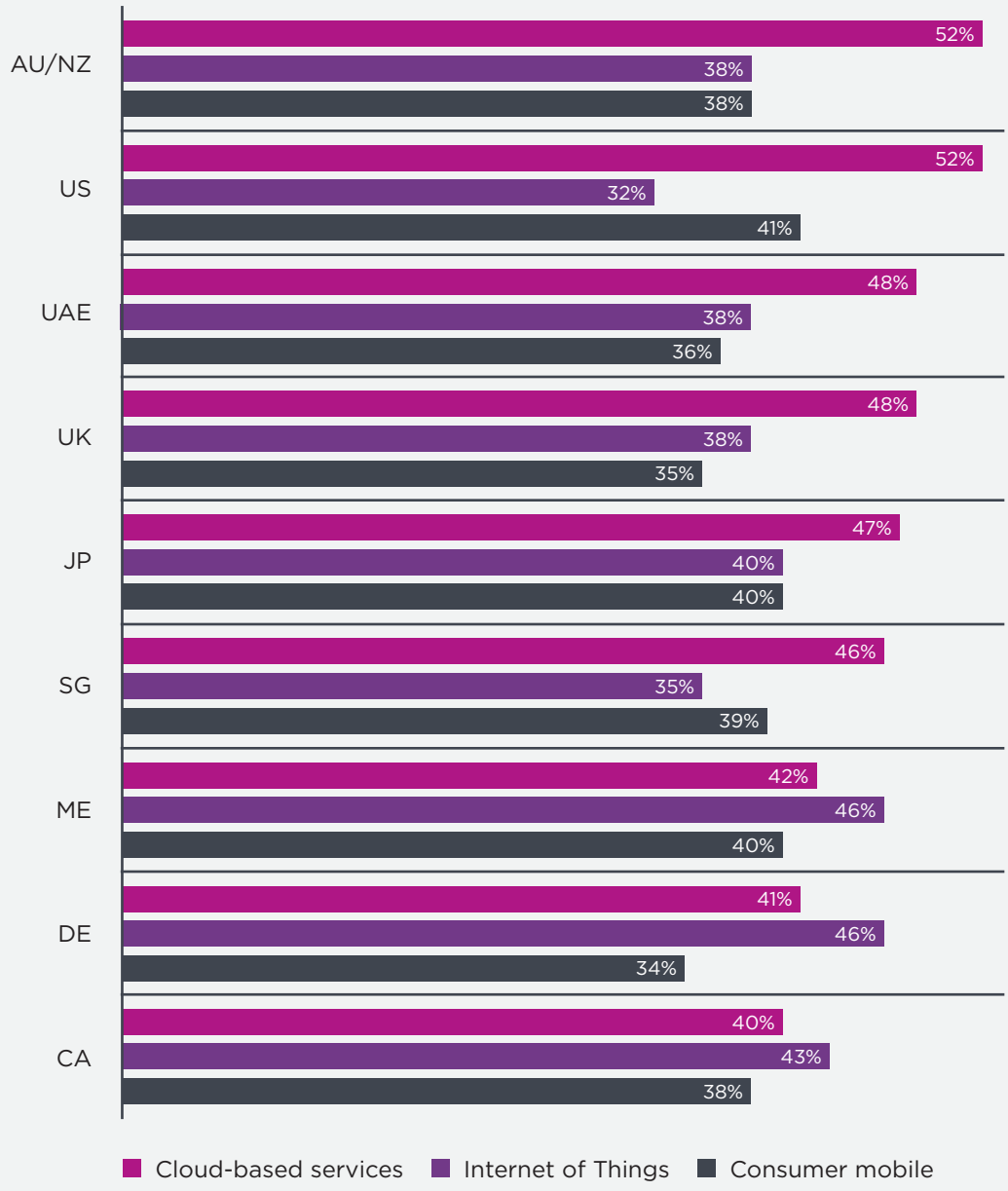


Figure 27 reports what respondents believe are the most important trends that are driving the deployment of applications that make use of PKI. As shown, Australia/New Zealand (52% of respondents), the United States (52% of respondents), the UAE (48% of respondents), the United Kingdom (48% of respondents), and Japan (47% of respondents) are most likely to cite cloud-based services as driving the deployment of applications that make use of PKI. Respondents in the Middle East (46% of respondents), Germany (46% of respondents), and Canada (43% of respondents) are most likely to say IoT is an important trend.

Figure 27. **What are the most important trends that are driving the deployment of applications that make use of PKI?**
Top 3 choices



Part 3
Methods

Part 3

METHODS

Table 1 reports the consolidated sample response for nine separate country samples. Data collection was started in November 2023 and completed in December 2023. Since the report is published in 2024, we label the data captured in 2023 as FY2024.

Table 1. Sample response	Frequency
Sampling frame	80,307
Total returns	4,377
Rejected or screened surveys	325
Overall sample (encryption trends)	4,052
PKI subsample	2,176
Ratio subsample to overall sample	54%

Figure 28 reports the respondent's organizational level within participating organizations. By design, 69% of respondents are at or above the supervisory levels, and 33% of respondents reported their position as manager/supervisor. Respondents have an average of 12 years of security experience and approximately 6.2 years of experience in their current position.

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

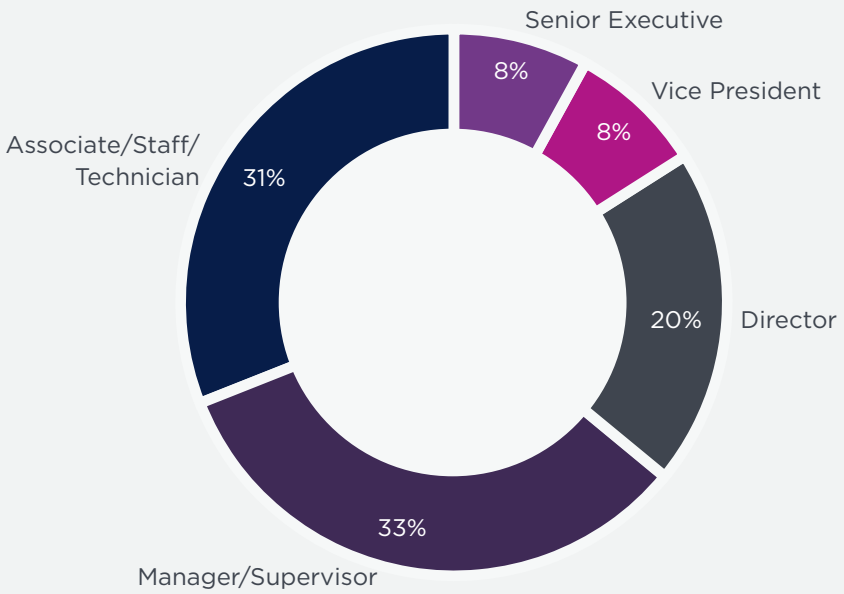


Figure 29 identifies the organizational location of respondents in our study. Almost half (40%) of respondents are located within IT operations. This is followed by security at 16% of respondents, and lines of business at 16% of respondents.

Figure 29. **Distribution of respondents according to organizational location**

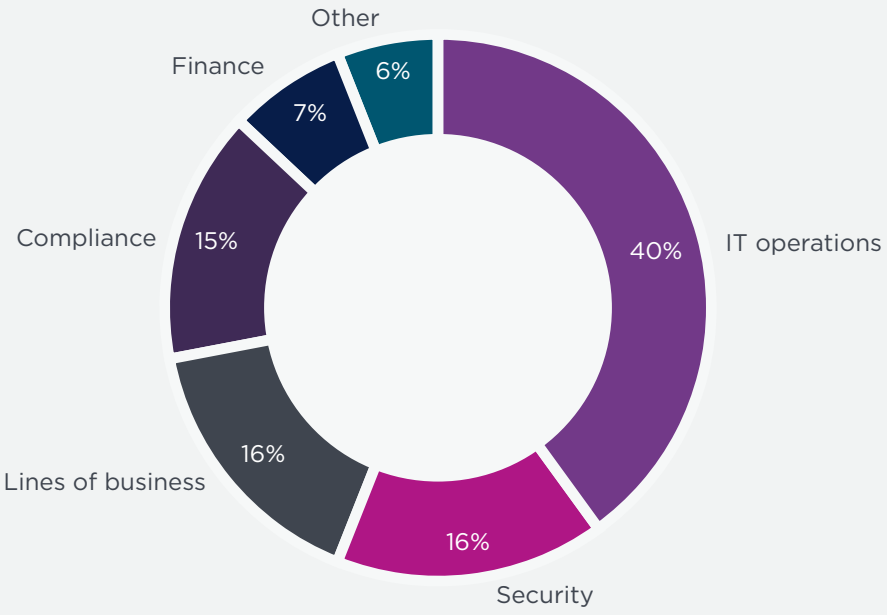
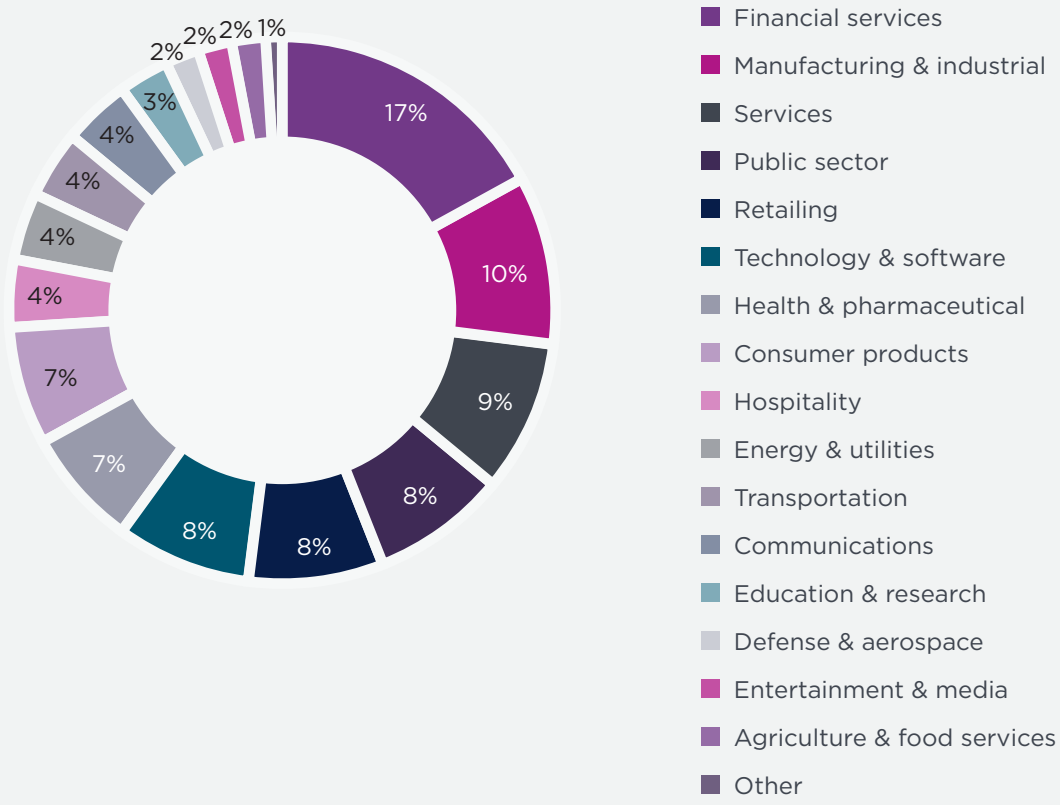


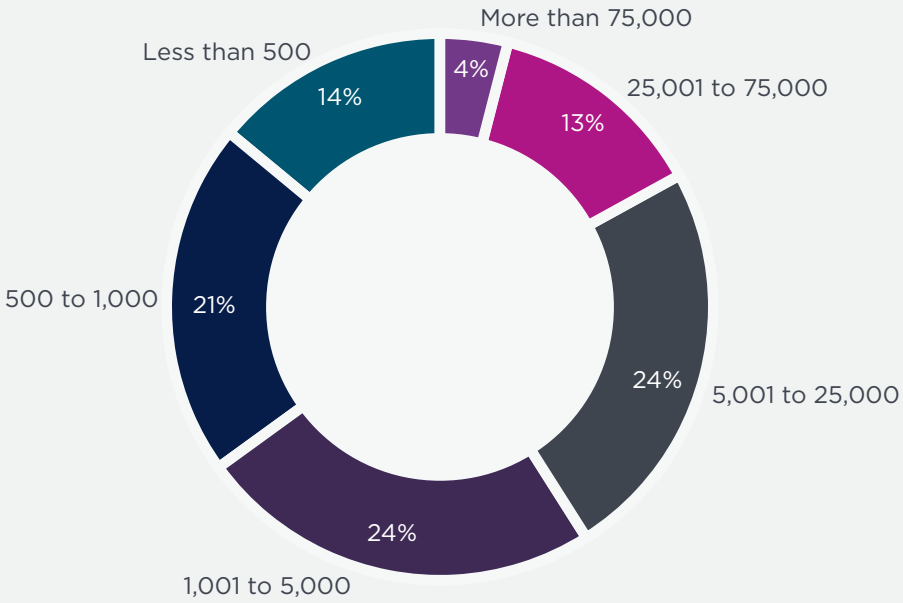
Figure 30 reports the industry classification of respondents' organizations. Seventeen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments, and credit cards. Ten percent of respondents are located in manufacturing and industrial organizations, and 9% of respondents are in services. This is followed by public sector, retailing, and technology and software (each at 8% of respondents).

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



According to Figure 31, more than half (65%) 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.



Part 4
Limitations

Part 4

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 relevant 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 nine countries, 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 is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network.

ENTRUST

SECURING A WORLD IN MOTION

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