2022 GLOBAL PKI AND IoT TRENDS STUDY

Find out how organizations are using PKI and if they're prepared for what's possible.

Ponemon INSTITUTE

TABLE OF CONTENTS

PART 1

Introduction

Ponemon Institute is pleased to present the findings of the *2022 Global PKI and IoT Trends Study*, sponsored by Entrust.

According to the findings, while PKI is considered a strategic part of the core IT backbone, the challenges in achieving PKI maturity continue to be insufficient resources and the shortage of skilled IT and IT security practitioners. Another growing challenge is the lack of visibility of the applications that will depend upon PKI.

The PKI research is part of a larger study published earlier this year involving 6,264 respondents in 17 countries.[1]

In this report, Ponemon Institute presents the findings based on a survey of 2,505 IT and IT security professionals who are involved in their organizations' enterprise PKI in 17 countries including Australia, Brazil, France, Germany, Hong Kong, Japan, Korea, Mexico, Middle East, Netherlands, Southeast Asia, Spain, Sweden, the United Kingdom, and the United States.

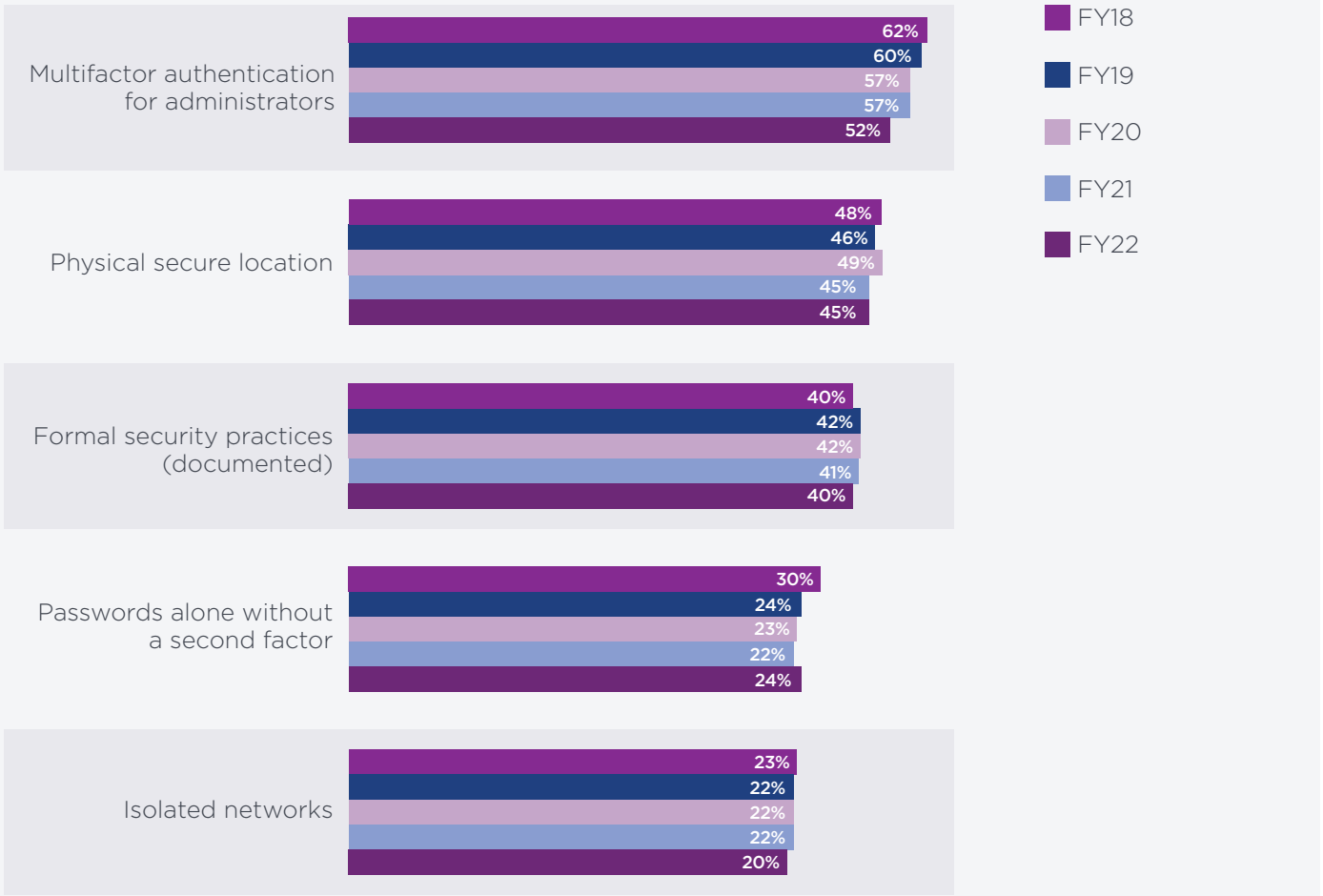
[1] See: **2022 Global Encryption Trends & Key Management Study** (sponsored by Entrust), Ponemon Institute, April 2022.

Figure 1 shows the primary practices organizations take to secure PKI and certificate authorities (CAs). Most companies represented in this study are using multifactor authentication for administrators (52 percent of respondents). Only 24 percent of respondents say their organizations are dependent upon passwords. Physical security and documented formal security practices have stayed the same at 45 percent and 40 percent of respondents, respectively.

Usage of hardware security modules, most prevalent with offline root CAs and issuing CAs, stayed virtually the same at 37 percent of respondents in 2022 and they remain the most prevalent method of PKI private key protection.

All participants in this research are either involved in the management of their organizations' enterprise PKI or in developing and/or managing applications that depend upon credentials controlled by their organizations' PKI. The IT manager, IT security manager, and CIO are most responsible for their organizations' PKI strategy.

Figure 1. **Practices used to secure PKI and certificate authorities**



PART 2

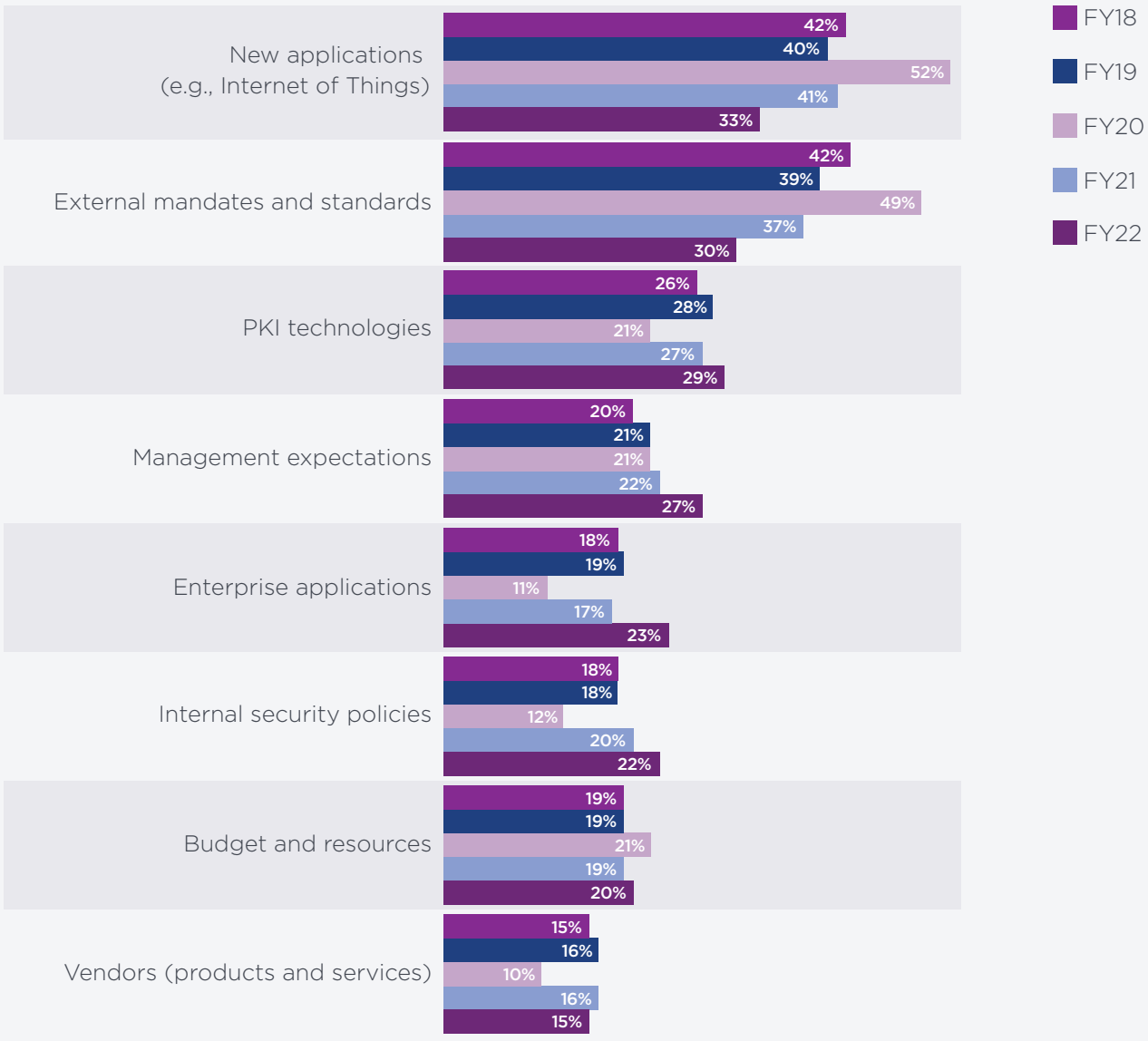
Key Findings

In this section of the report, we provide an analysis of the global PKI results over a five-year period from 2018 to 2022. The complete audited findings are presented in the Appendix of this report.

Trends in managing IoT

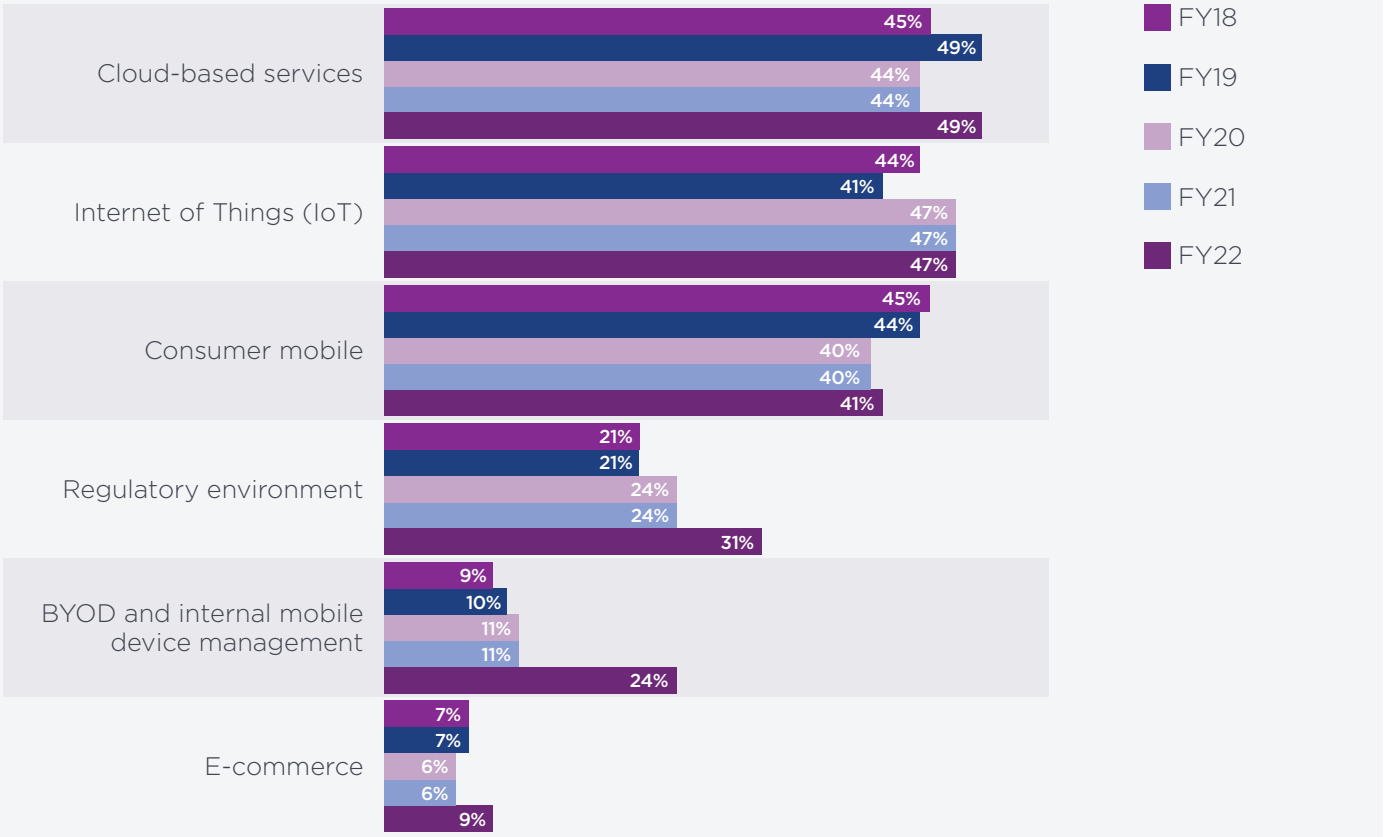
As organizations plan the evolution of their PKI, new applications such as IoT devices and external mandates and standards continue to drive the most change and uncertainty. According to Figure 2, 33 percent of respondents say new applications such as the IoT (a decrease from 41 percent in 2021) and 30 percent of respondents (a decrease from 37 percent in 2021) say external mandates and standards will drive change. Enterprise applications as a change agent for PKI have increased from 17 percent of respondents to 23 percent of respondents.

Figure 2. **As organizations plan the evolution of their PKI, what areas are expected to experience the most change and uncertainty?** (Consolidated view — two responses permitted)



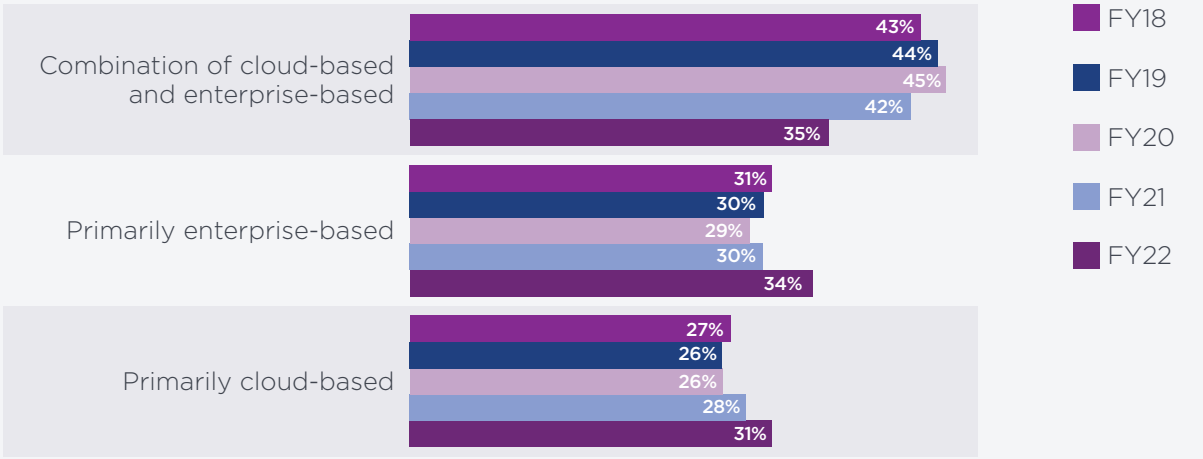
Cloud-based services and IoT continue to be the most important trends driving the deployment of applications using PKI. There is growing recognition that PKI provides important core authentication technology in the IoT. As shown in Figure 3, cloud-based services is the number one trend driving deployment of applications using PKI (49 percent of respondents). Respondents who say IoT is the most important trend driving the deployment of applications using PKI has remained virtually unchanged (47 percent of respondents) since 2020.

Figure 3. **The most important trends driving the deployment of applications using PKI**
(Consolidated view — two responses permitted)



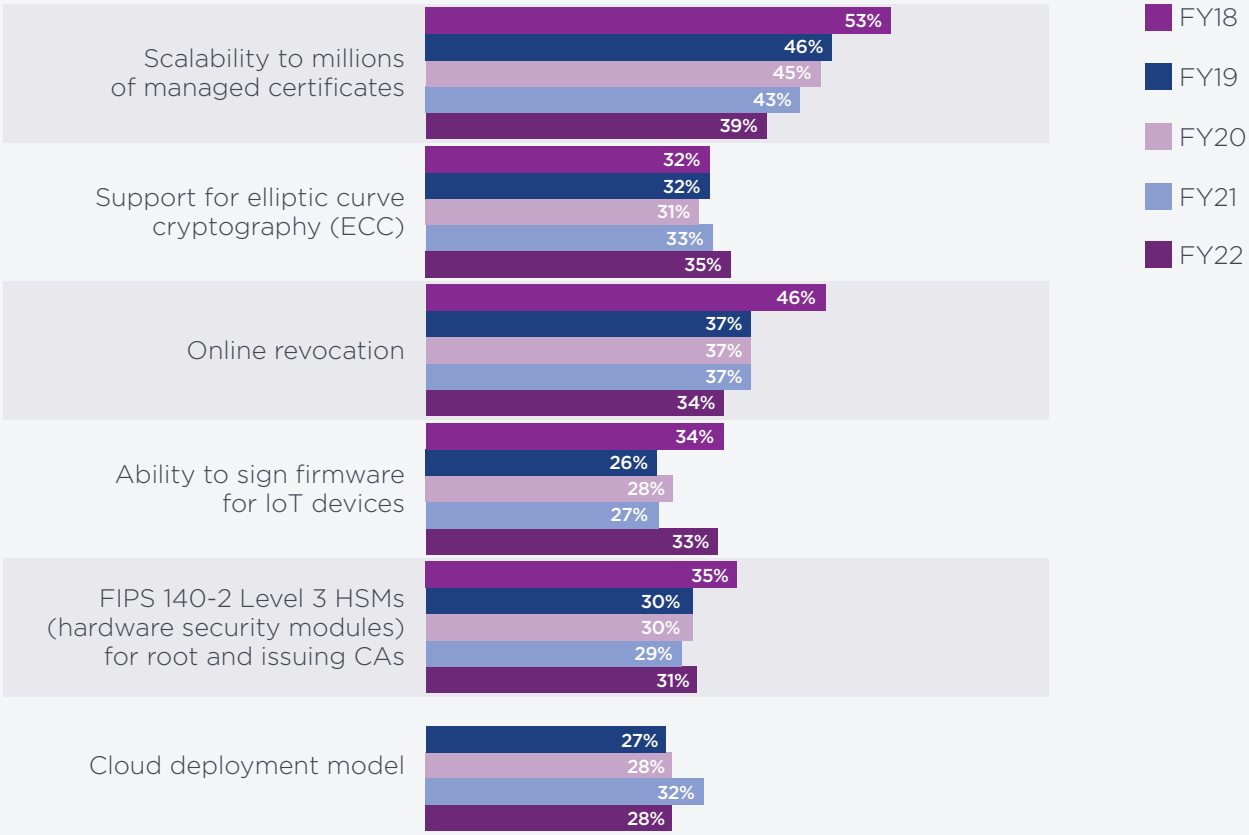
In the next two years, an average of 44 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication. As shown in Figure 4, 35 percent of respondents believe that as the IoT continues to grow supporting PKI deployments for IoT device credentialing will be a combination of cloud-based and enterprise-based. However, this has decreased from 42 percent of respondents in 2021.

Figure 4. **As IoT continues to grow, what PKI deployments will support IoT device credentialing?**



Scalability to millions of managed certificates continues to be the most important PKI capability for IoT employments. Figure 5 lists the most important PKI capabilities for IoT deployments. While scalability is the most important, it has decreased in importance from 53 percent of respondents in 2018 to 39 percent of respondents in 2022. The ability to sign firmware for IoT devices has increased from 27 percent of respondents in 2021 to 33 percent of respondents in 2022.

Figure 5. **What are the most important PKI capabilities for IoT deployments?**
(Two responses permitted)

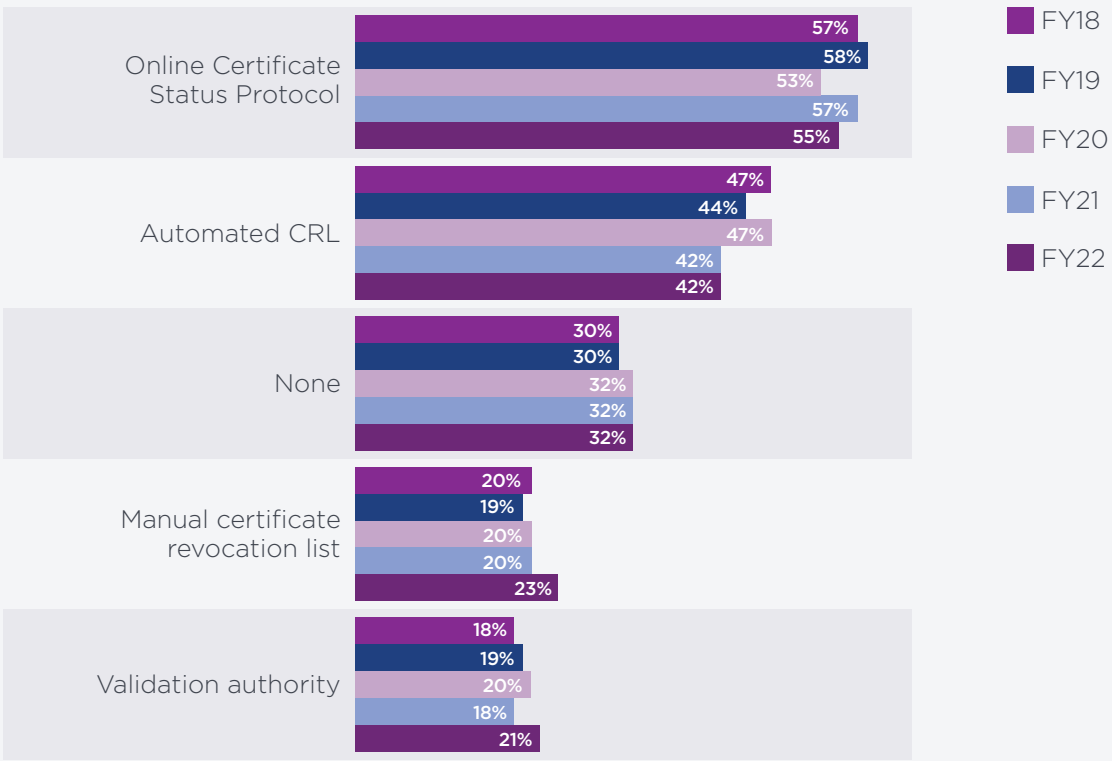


Challenges in achieving PKI maturity

According to Figure 6, the certificate revocation technique most often deployed continues to be online certificate status protocol (OCSP), according to 55 percent of respondents. The next most popular technique is the use of automated certificate revocation list (CRL), according to 42 percent of respondents, a decrease from 47 percent of respondents in 2020.

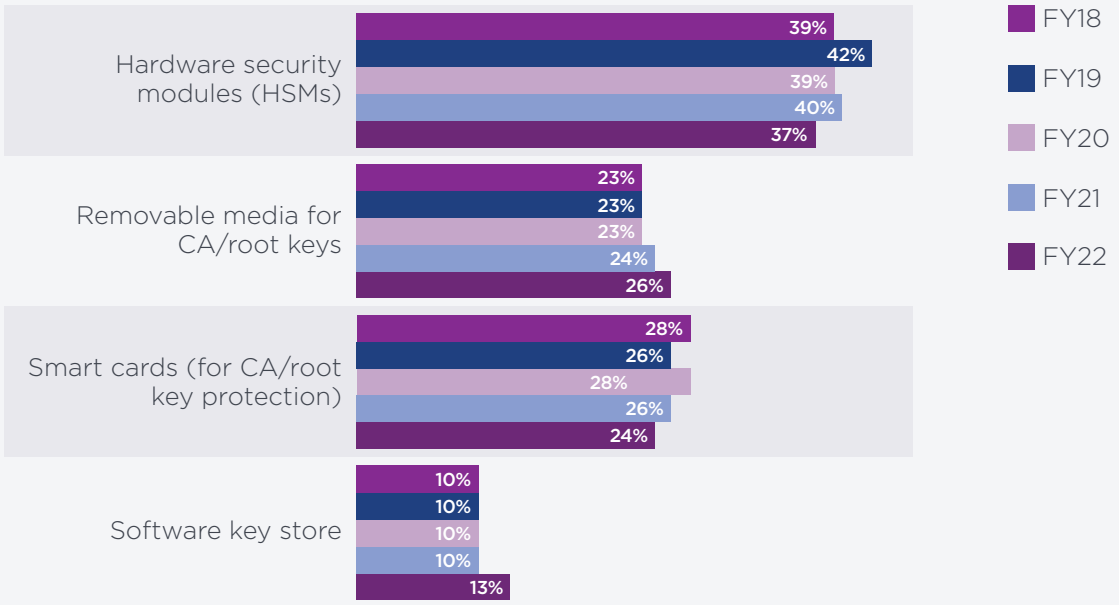
Similar to last year, 32 percent of respondents say they do not deploy a certificate revocation technique. There are many possible explanations for this high percentage — use of alternate means to remove users/devices, use of short lifespan certificates, closed systems, etc.

Figure 6. **The certificate revocation techniques used in enterprises**
(Consolidated view — more than one response permitted)



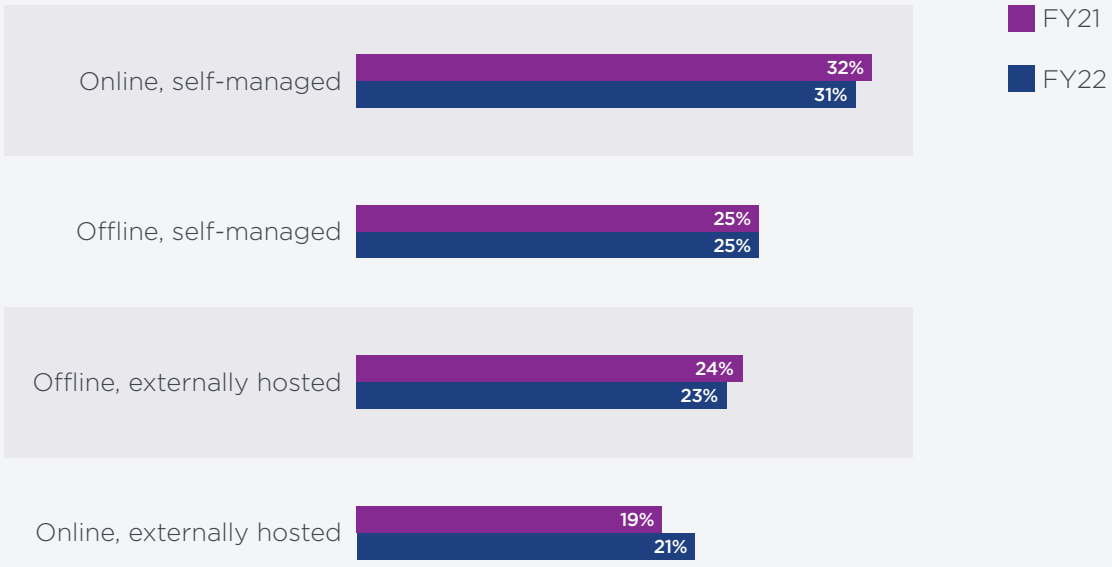
Hardware security modules (HSMs) continue to be most often used to manage the private keys for their root/policy/issuing CAs (37 percent of respondents), as shown in Figure 7. Twenty-six percent of respondents say removable media for CA/root keys and 24 percent of respondents say smart cards are used.

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



Most organizations' primary root CA strategy is online, self-managed. A root certificate is a public key certificate that identifies a root certificate authority (CA). Figure 8 lists the primary root CA strategies used by organizations. Thirty-one percent of respondents say it is online, self-managed followed by offline, self-managed at 25 percent of respondents.

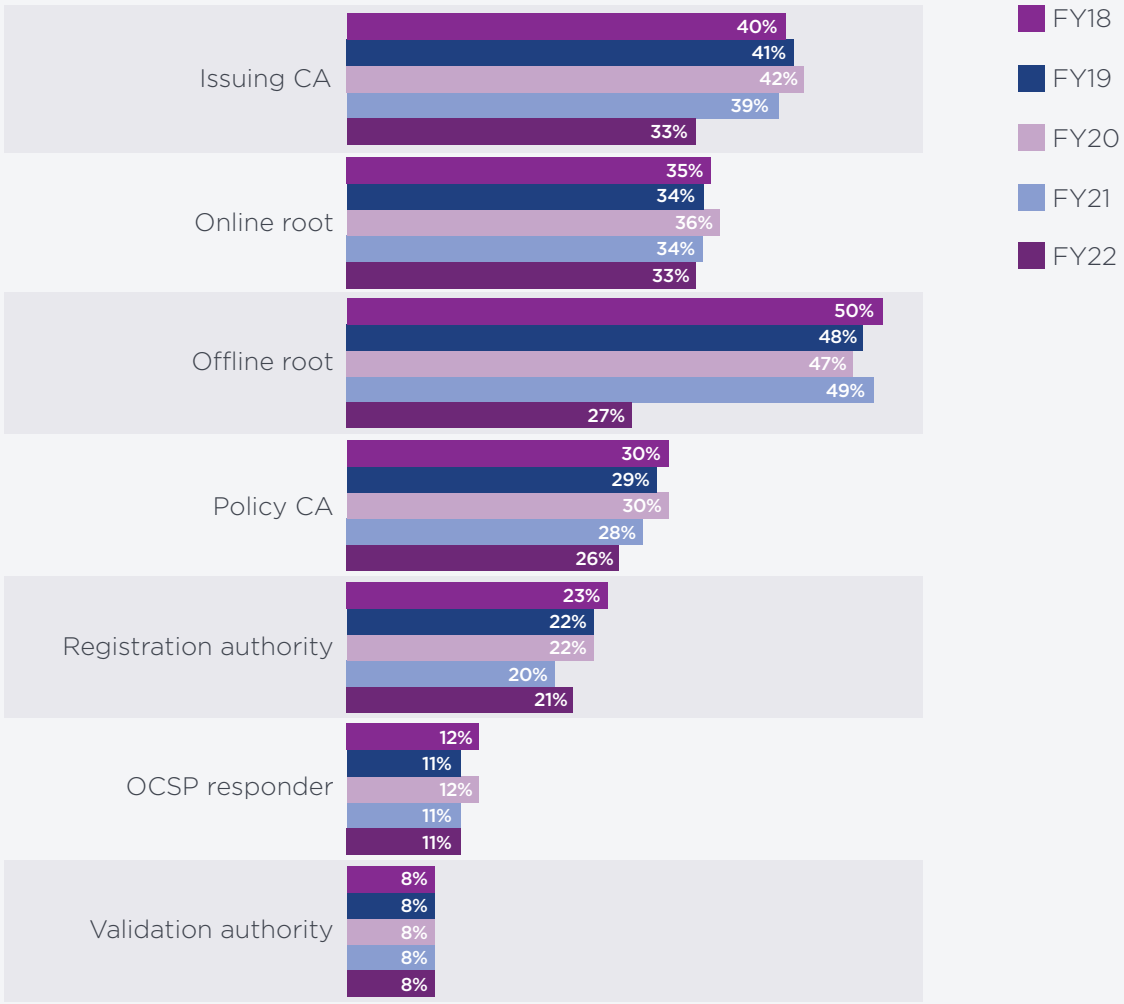
Figure 8. **What is your organization's primary root CA strategy?**
(Only one choice permitted)



Of the 37 percent of organizations in this study that use HSMs to secure PKI, they are used across the entire architecture of the PKI as shown in Figure 9. HSMs deployed in offline roots has declined from 49 percent of respondents in 2021 to 27 percent of respondents in 2022.

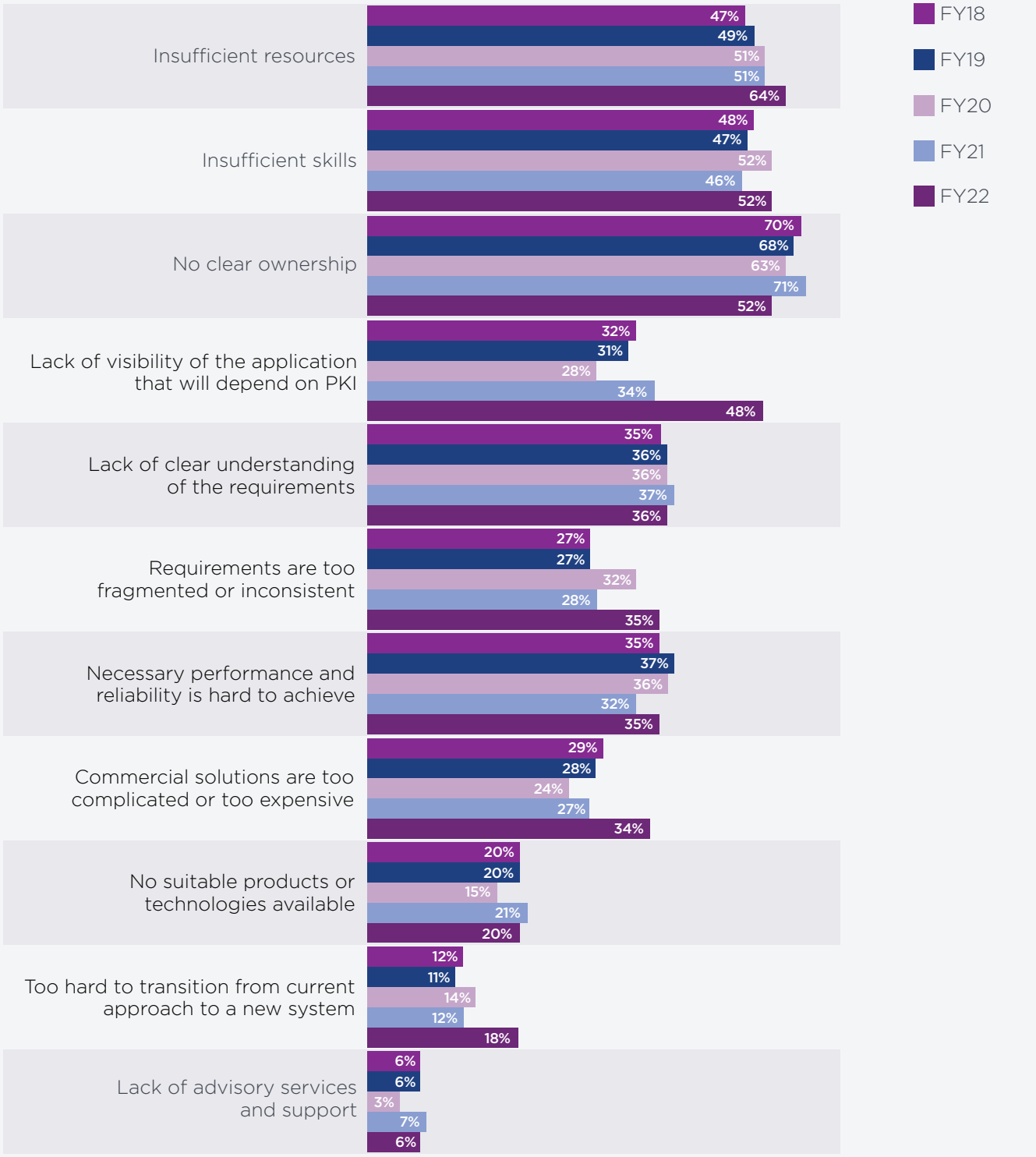
As an example of best practice, NIST calls to "Ensure that Cryptographic modules for CAs, Key Recovery Servers, and OCSP responders are hardware modules validated as meeting FIPS 140-2 Level 3 or higher" (NIST Special Publication 800-57 Part 3). Yet only 11 percent of our respondents indicate the presence of HSMs in their OCSP installations. This is a significant gap between best practices and observed practices.

Figure 9. **Where HSMs are deployed to secure PKI**
(Consolidated view — more than one response permitted)



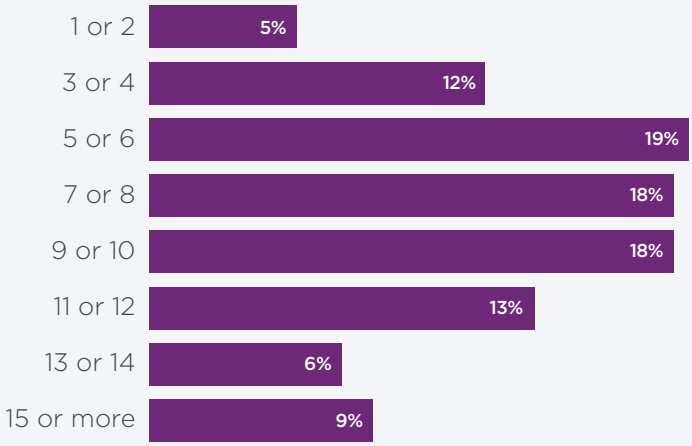
Insufficient resources, lack of skills, and no clear ownership are the top three challenges to enabling applications to use PKI. As shown in Figure 10, the challenge of not having sufficient resources has increased significantly from 51 percent of respondents in 2021 to 64 percent of respondents in 2022. Other challenges are insufficient skills (52 percent) and no clear ownership (52 percent of respondents). The lack of visibility of the applications that will depend upon PKI increased from 34 percent of respondents in 2021 to 48 percent of respondents in this year's research.

Figure 10. **The challenges in deploying and managing PKI** (Consolidated view — four responses permitted)



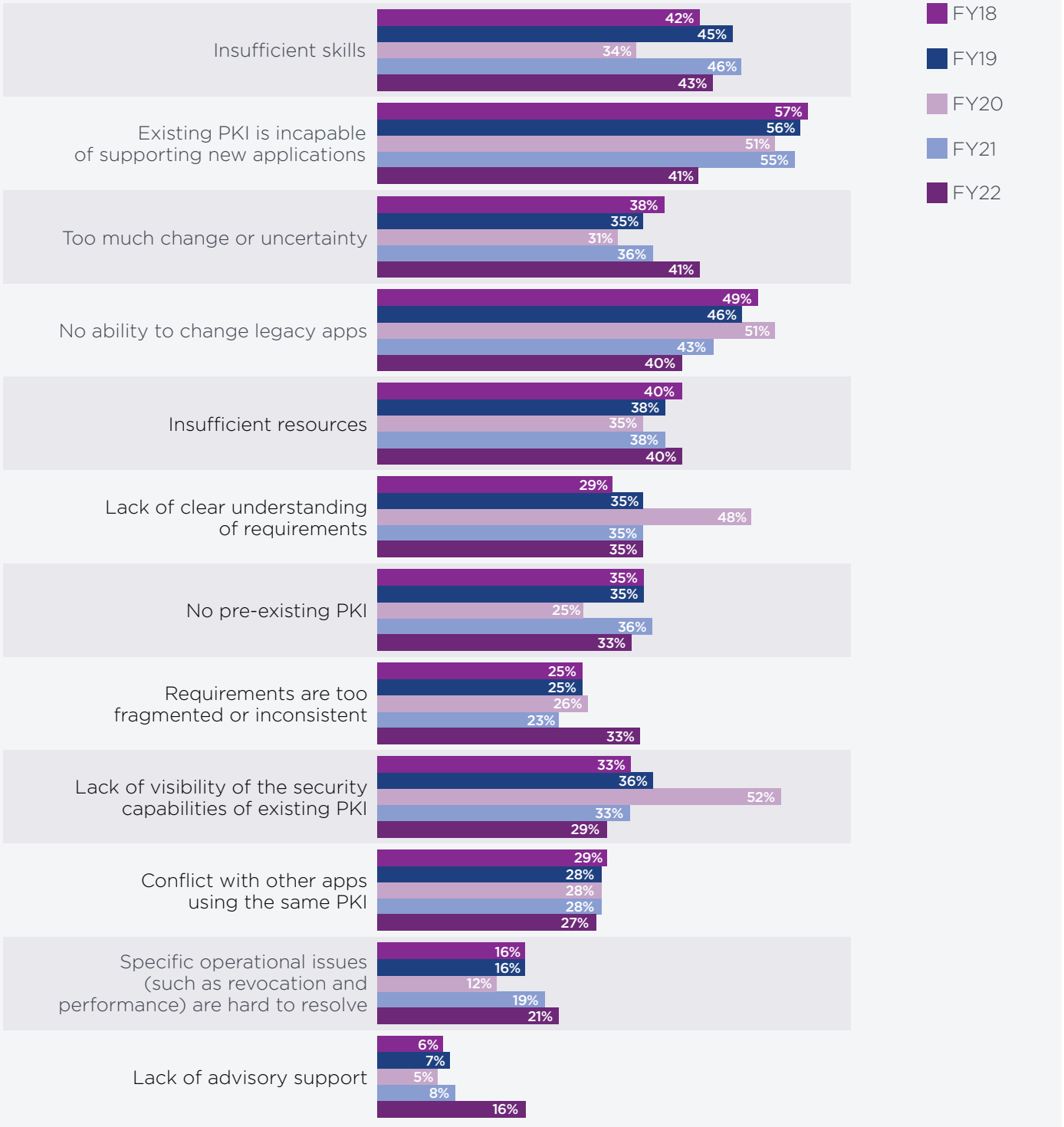
Organizations with internal CAs use an average of 6.8 separate CAs, managing an average of 52,022 internal or externally acquired certificates. As shown in Figure 11, an average of 8.4 distinct applications, such as email and network authentication, are managed by an organization's PKI. This indicates that the PKI is at the core of the enterprise IT backbone. 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 11. **How many distinct applications does your PKI manage certificates on behalf of?**
(Consolidated view — extrapolated value is 8.4 distinct applications)



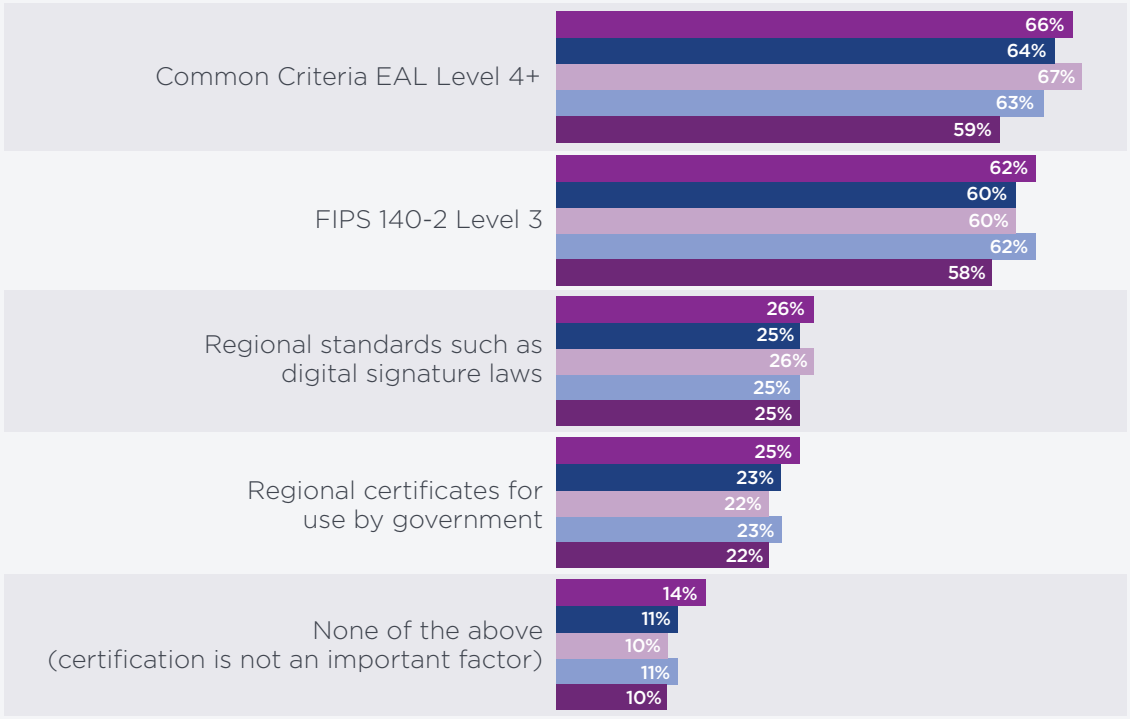
The challenge of PKI supporting new applications has declined significantly since 2021. As shown in Figure 12, the previous number one challenge has been that existing PKI is incapable of supporting new applications. However, that concern has decreased significantly from 55 percent of respondents in 2021 to 41 percent of respondents in 2022. The lack of visibility of the security capabilities of existing PKI also has decreased significantly from 52 percent of respondents in 2020 to 29 percent of respondents in 2022.

Figure 12. **What are the challenges to enable applications to utilize PKI?**
(Consolidated view — four responses permitted)



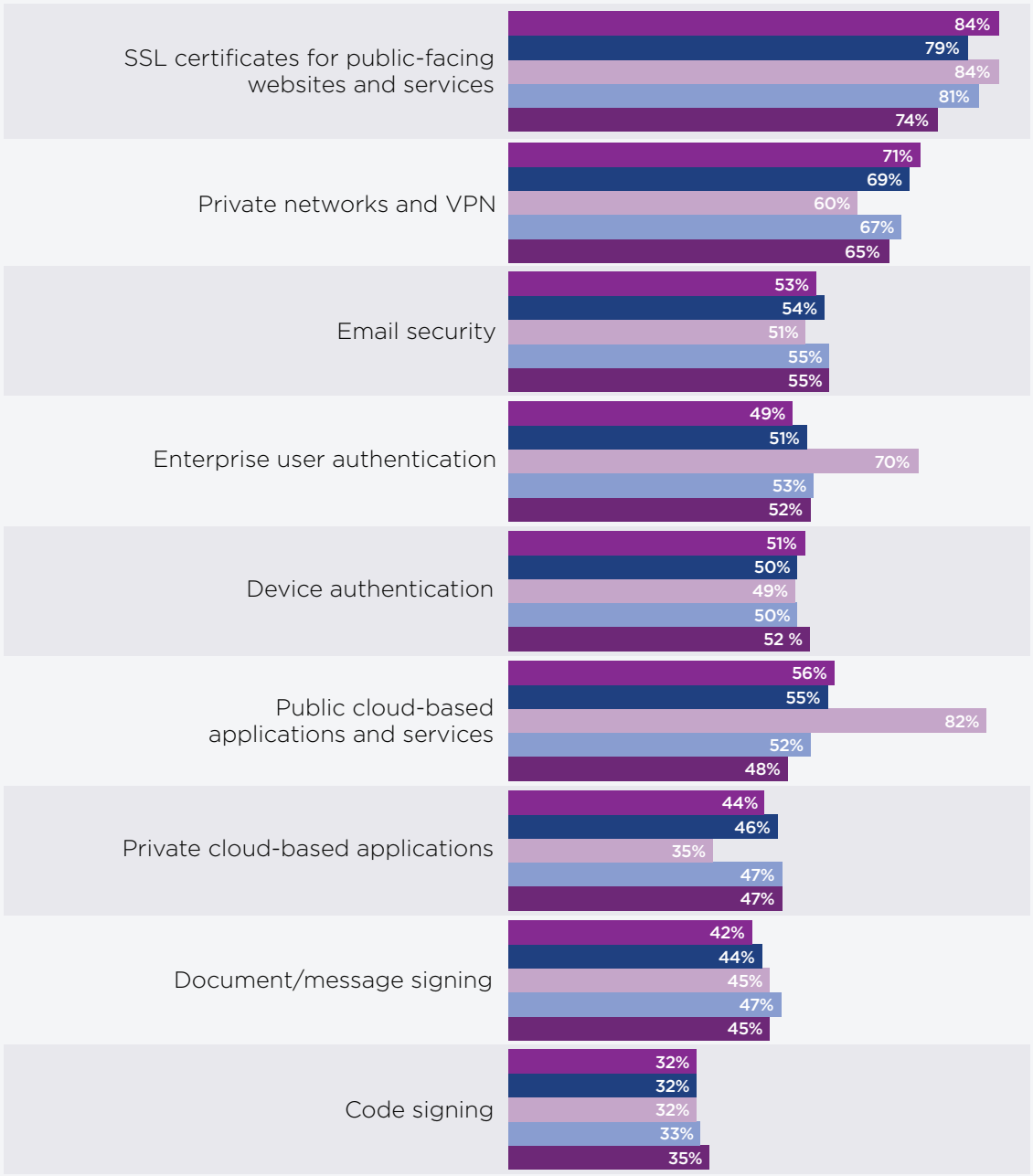
Common Criteria EAL Level 4+ and FIPS 140-2 Level 3 continue to be the most important security certifications when deploying PKI infrastructure and PKI-based applications. According to Figure 13, 59 percent say Common Criteria followed by 58 percent who say FIPS 140 are the most important certificate certifications 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. Twenty-five percent of respondents say regional standards such as digital signature laws are important.

Figure 13. **Security certifications important when deploying PKI infrastructure**
(Consolidated view — more than one response permitted)



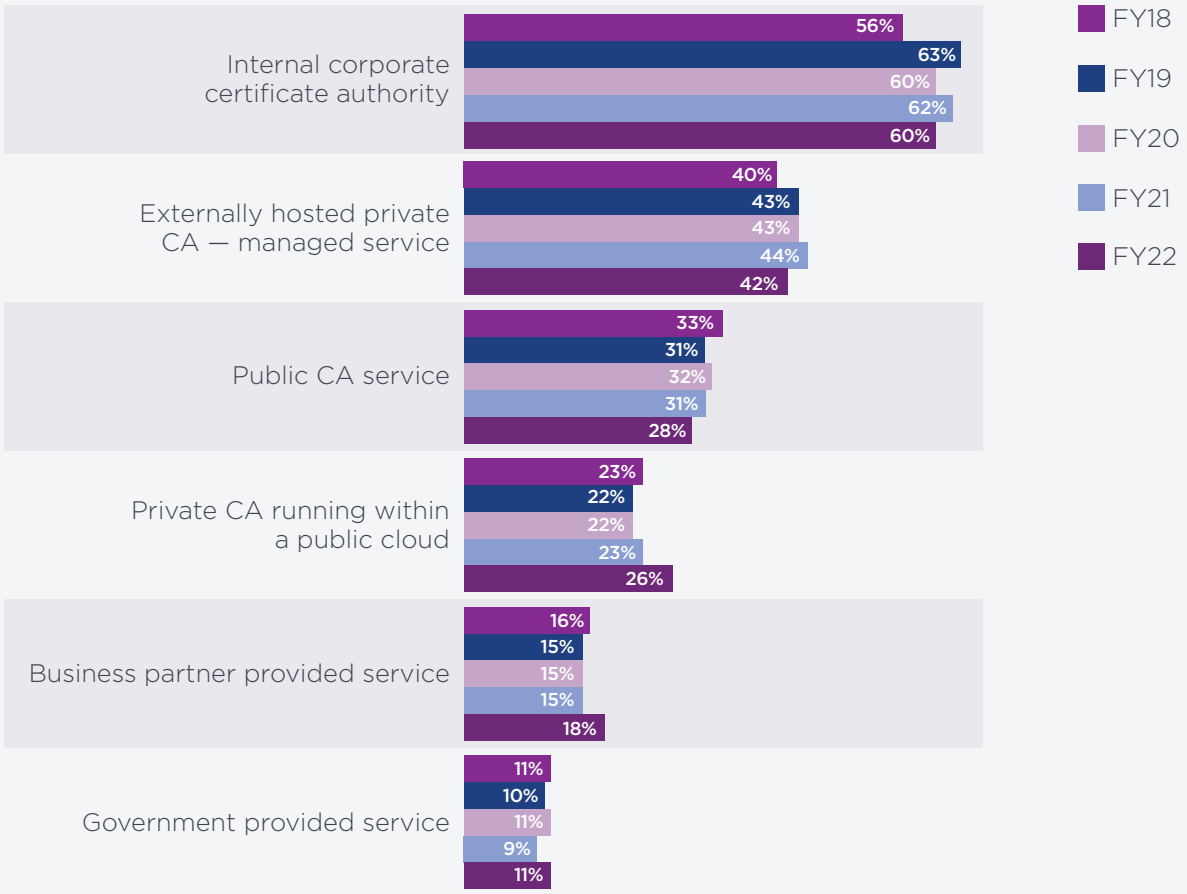
SSL certificates for public-facing websites and services are most often using PKI credentials. According to Figure 14, 74 percent of respondents say the application most often using PKI credentials is SSL certificates for public-facing websites and services. However, enterprise user authentication has decreased significantly from 70 percent of respondents in 2020 to 52 percent of respondents in 2022, and the use of public cloud-based applications and services has decreased significantly from 82 percent in 2020 to 48 percent of respondents in 2022.

Figure 14. **What applications use PKI credentials in organizations?**
(Consolidated view — more than one response permitted)



What are the most popular methods for deploying enterprise PKI? The most cited method for deploying enterprise PKI, according to Figure 15, is through an internal corporate certificate authority (CA) or an externally hosted private CA — managed service, according to 60 percent and 42 percent of respondents, respectively.

Figure 15. **How is PKI deployed?** (Consolidated view — more than one response permitted)



Organizations prefer the single sign-on to all apps and platforms if they use the PKI credential for enterprise user authentication or device authentications. As shown in Figure 16, 48 percent of respondents say the single sign-on to all apps and platforms is the most important authentication requirement. This is followed by the option that it works with any device (42 percent of respondents).

Figure 16. **If you use PKI credential for enterprise user authentication or device authentications, what are your most important authentication requirements?** (Two responses permitted)

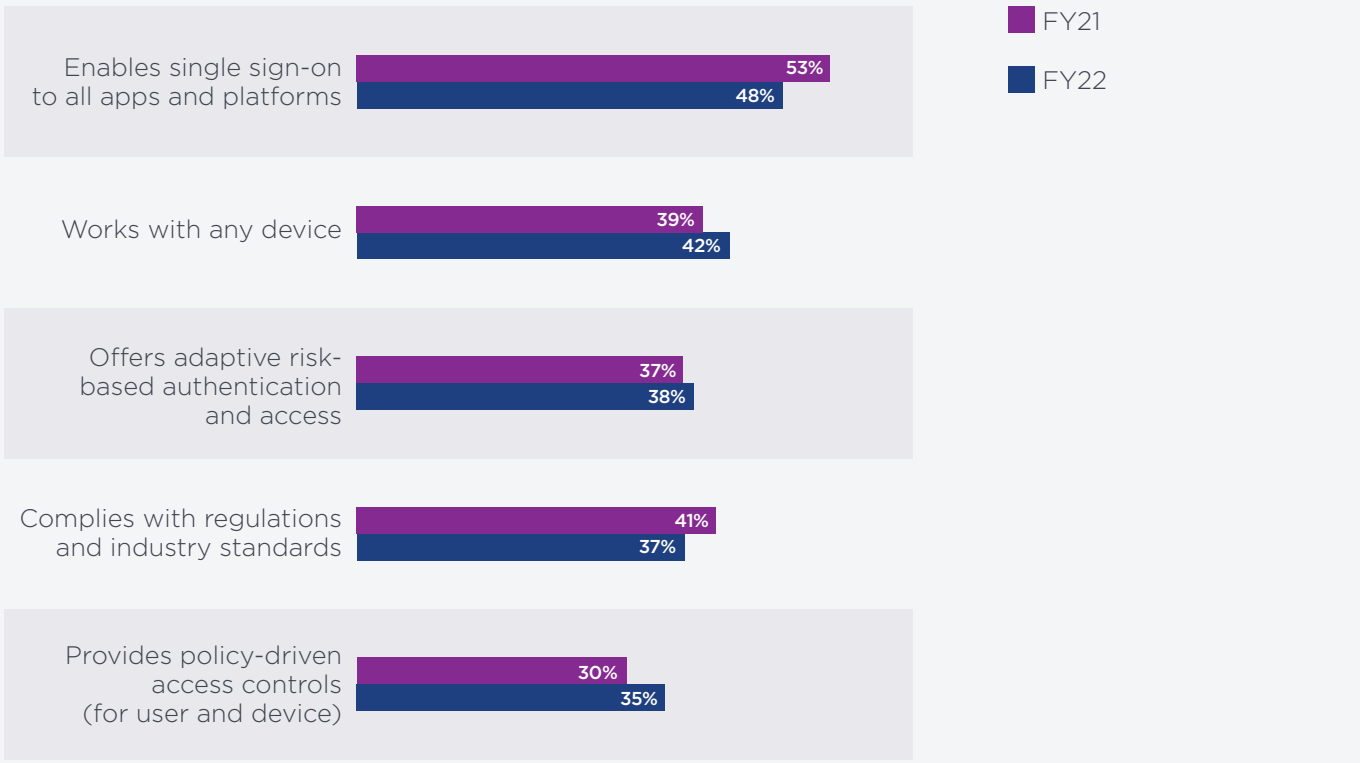
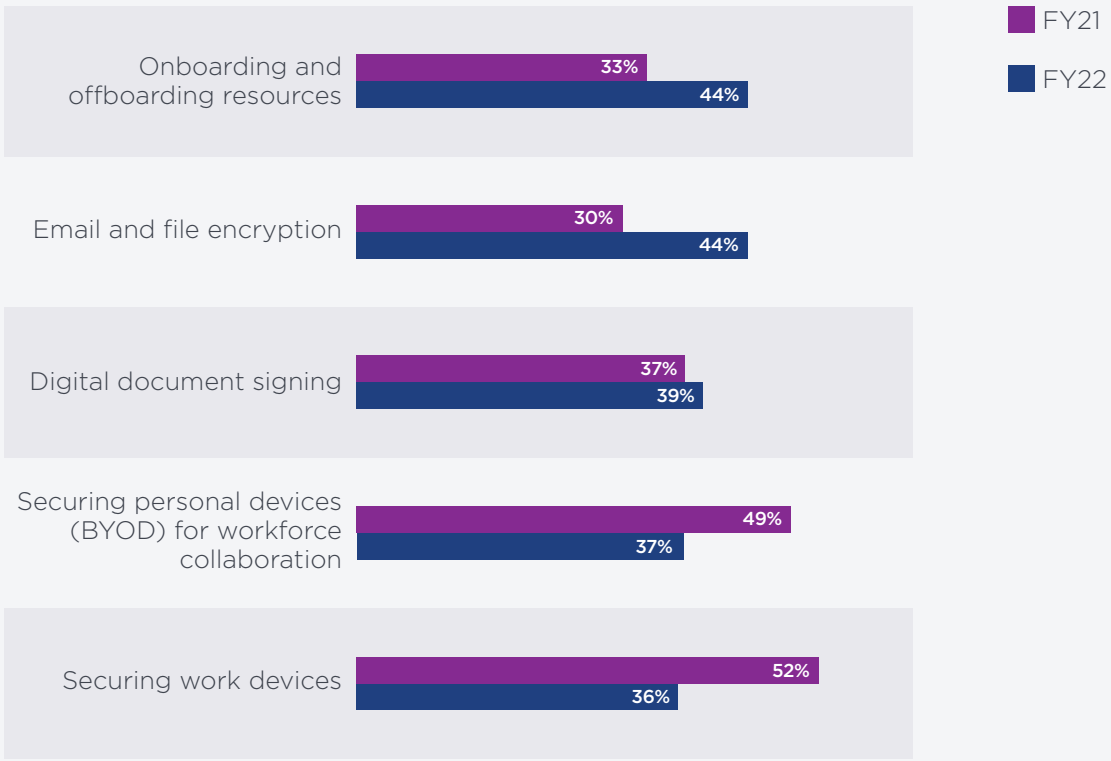


Figure 17 lists the use cases that would benefit from an integrated authentication and PKI solution. Onboarding and offboarding resources and email and file encryption have increased significantly since last year to 44 percent of respondents. Securing personal devices for workforce collaboration as a beneficial use case has decreased from 49 percent of respondents to 37 percent of respondents.

Figure 17. **What use cases would benefit most from an integrated authentication and PKI solution?** (Two responses permitted)



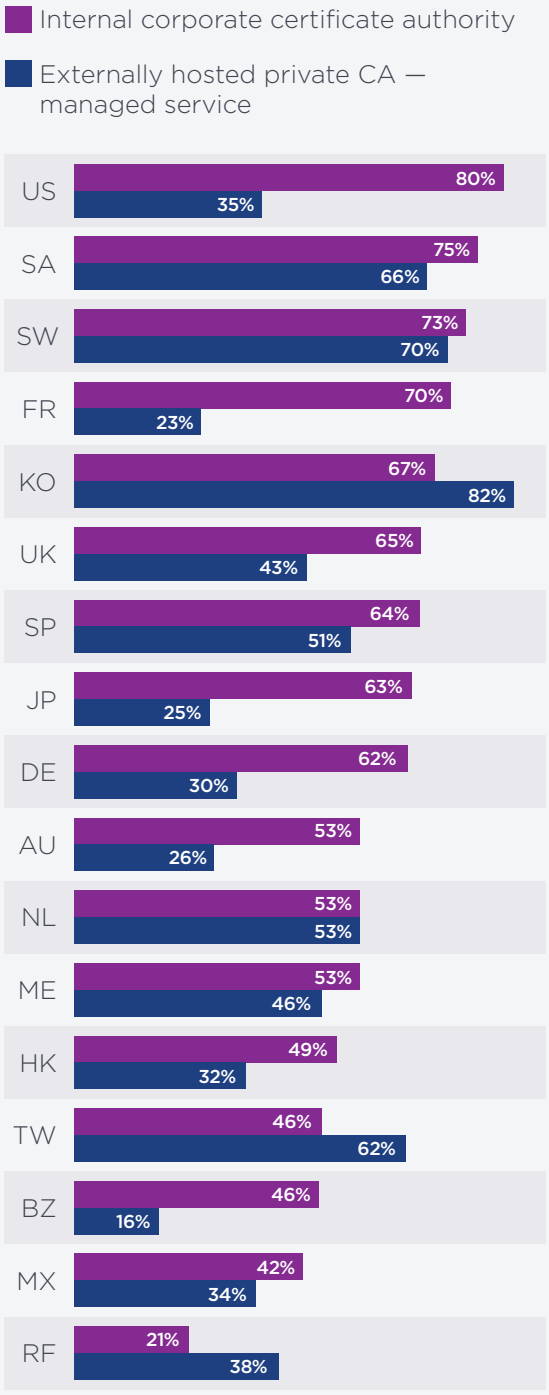
Global analysis

In this section, we provide the most salient differences among the 17 countries represented in this study: Australia (AU), Brazil (BZ), France (FR), Germany (DE), Hong Kong (HK), Japan (JP), Korea (KO), Mexico (MX), Middle East (ME) Netherlands (NL), Russia (RF), Spain (SP), Southeast Asia (SA), Sweden (SW), Taiwan (TW), United Kingdom (UK), and United States (US).

Figure 18 shows how PKI is deployed within respondents' organizations. As shown, the U.S. (80 percent of respondents), Southeast Asia (75 percent of respondents), Sweden (73 percent of respondents), and France (70 percent of respondents are most likely to choose internal corporate certificate authority.

In contrast, Korea (82 percent of respondents), Sweden (70 percent of respondents), Southeast Asia (66 percent of respondents), and Taiwan (62 percent of respondents) are most likely to choose external hosted private certificate authorities as a managed service.

Figure 18. **How would you describe how your organization's enterprise PKI is deployed?** (Top 2 choices)

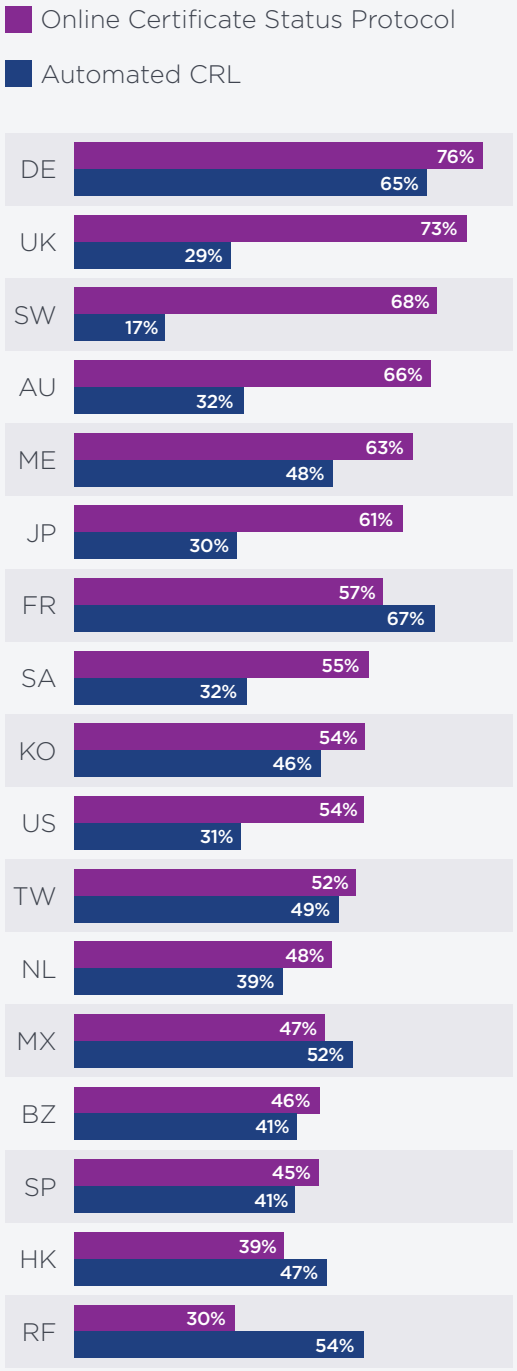


When asked about the revocation techniques deployed, 32 percent of respondents globally say none. As shown in Figure 19, of those respondents who say their organizations use a certificate revocation technique, Germany (76 percent), UK (73 percent), Sweden (68 percent), and Australia (66 percent) are most likely to use online certificate status protocols (OCSP). France (67 percent), Germany (65 percent), Russia (54 percent), and Mexico (52 percent) respondents are most likely to use automated CRLs.

As noted above, this implies a true chasm between operational best practices and observed practices. Certificates have a life span. During that life span circumstances change and certificates outlive their purpose. Without a method of revoking certificates, the population of valid, extant certificates simply grows.

We can surmise that there are connections between this observed deviation from best practices and the significant lack of dedicated personnel and skills called out in the study. When something as basic as lack of revocation processes is this common, one wonders about the currency of documentation on and processes for managing the average of seven major enterprise applications that are dependent on the PKI.

Figure 19. **Which certificate revocation technique does your organization deploy?** (Top 2 choices = OCSP and Automated CRL)



According to Figure 20, the U.S. and France have the most individual CAs deployed within their organizations (8.9 and 7.9, respectively). Russia and Spain have the least number of individual CAs (both 5.6).

Again, this reinforced the penetration of the PKI into the core IT backbone of the modern organization. And, given the stated lack of skilled personnel and organizational clarity, combined with the lack of consistent revocation practices, one has to draw attention to risks to the health and integrity of these CAs and the important core enterprise applications that use their certificates.

Figure 20. **What best describes the number of issuing CAs in your organization?**
(Extrapolated average values)

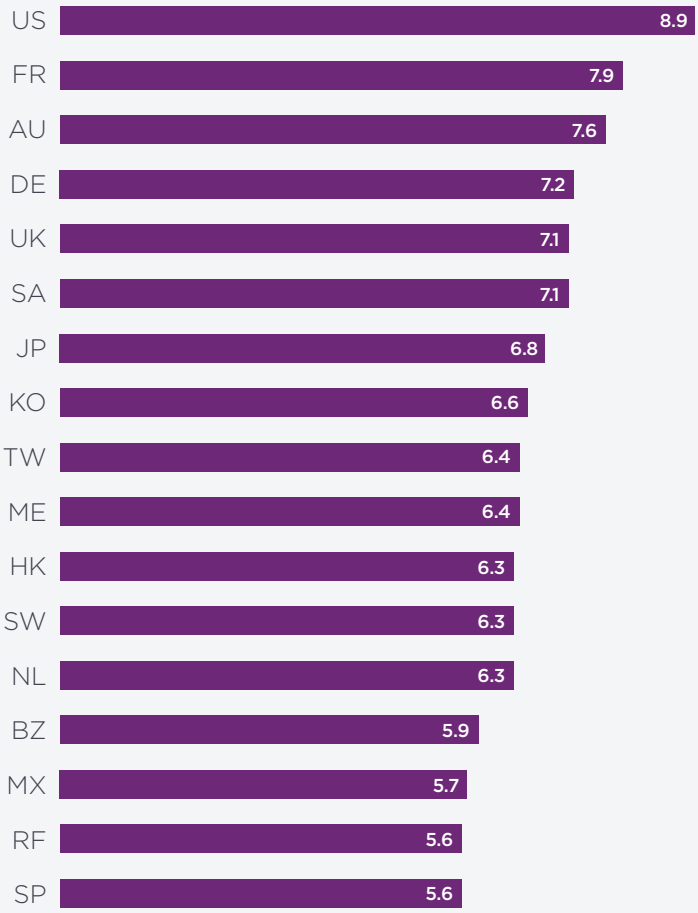


Figure 21 is the number of distinct applications (e.g., email, network authentication, etc.) for which PKI manages certificates. The U.S. at 11.2 has the largest number of distinct applications. Taiwan (6.9) and Russia (6.5) have the smallest number of distinct applications, respectively.

One should note that even in the lowest figures that the average number of applications is just north of 6. Given previous responses, we can extrapolate that these likely include email, SSL certificates, device identification, and logon credentials. These are non-trivial applications, the failure of which could pose existential risks to the host organization.

Figure 21. **How many distinct applications does your PKI manage certificates on behalf of?**
(Extrapolated average values)

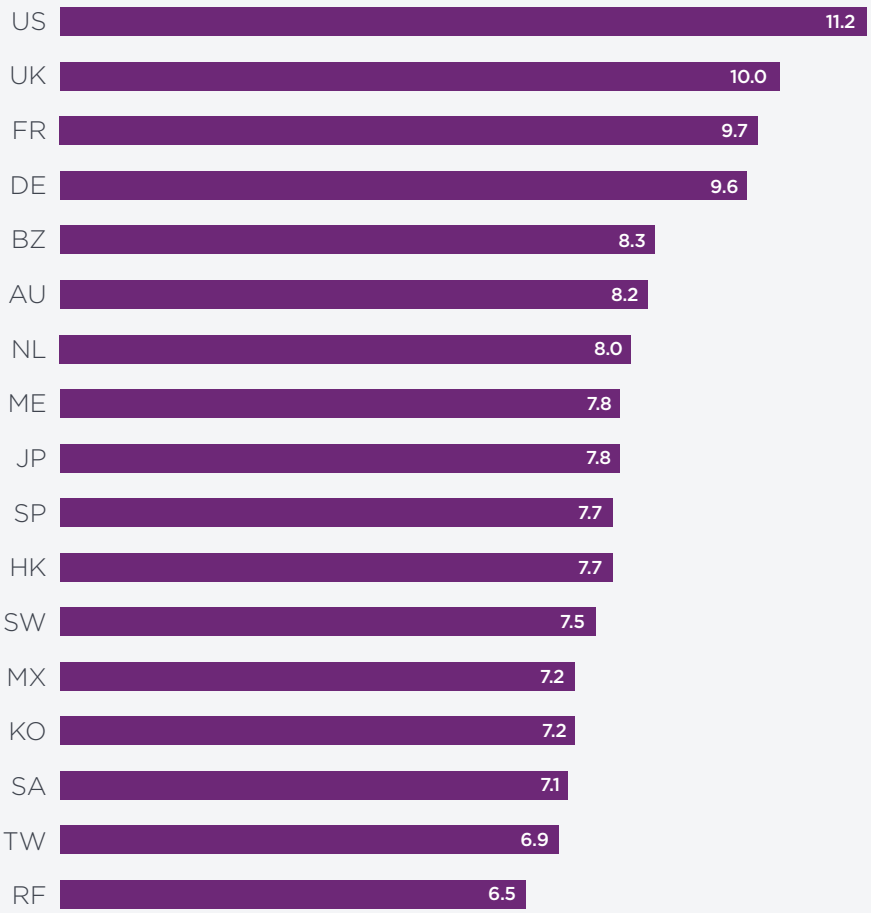
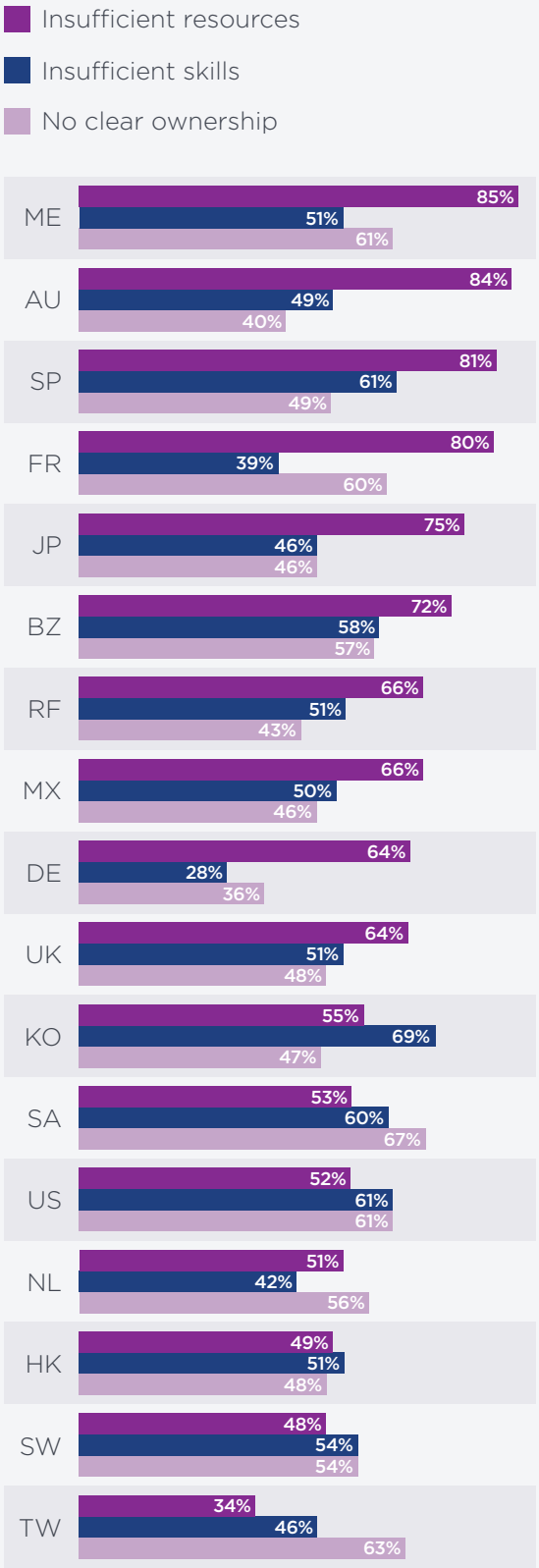


Figure 22 reports the three most salient challenges in deploying and managing PKI. As shown, Southeast Asia, Taiwan, the Middle East, and the U.S. are most likely to cite no clear ownership as their most significant challenge. The Middle East, Australia, Spain, and France are more likely to say insufficient resources is a challenge and Korea, Spain, and the U.S. say they are challenged by insufficient skills.

There is a consistent theme in these responses. We can see the importance of the 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 a lack of trained people and tendency toward fuzzy ownership of the PKI. This is a significant departure from known best practices that require direct lines of responsibility for all PKI-dependent applications and clear documentation of the dependencies and risk mitigation strategies. One wonders about the condition of required PKI documentation and processes given these high rates of skills and personnel shortages.

Figure 22. **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 23 provides the top two choices. Accordingly, U.S., Taiwan, and Russia respondents say new applications such as IoT are driving change and uncertainty. France, U.S., and Hong Kong respondents say external mandates and standards are driving change and uncertainty.

Figure 23. **Where are the greatest areas of change and uncertainty in the evolution of your PKI?** (Top 2 choices)

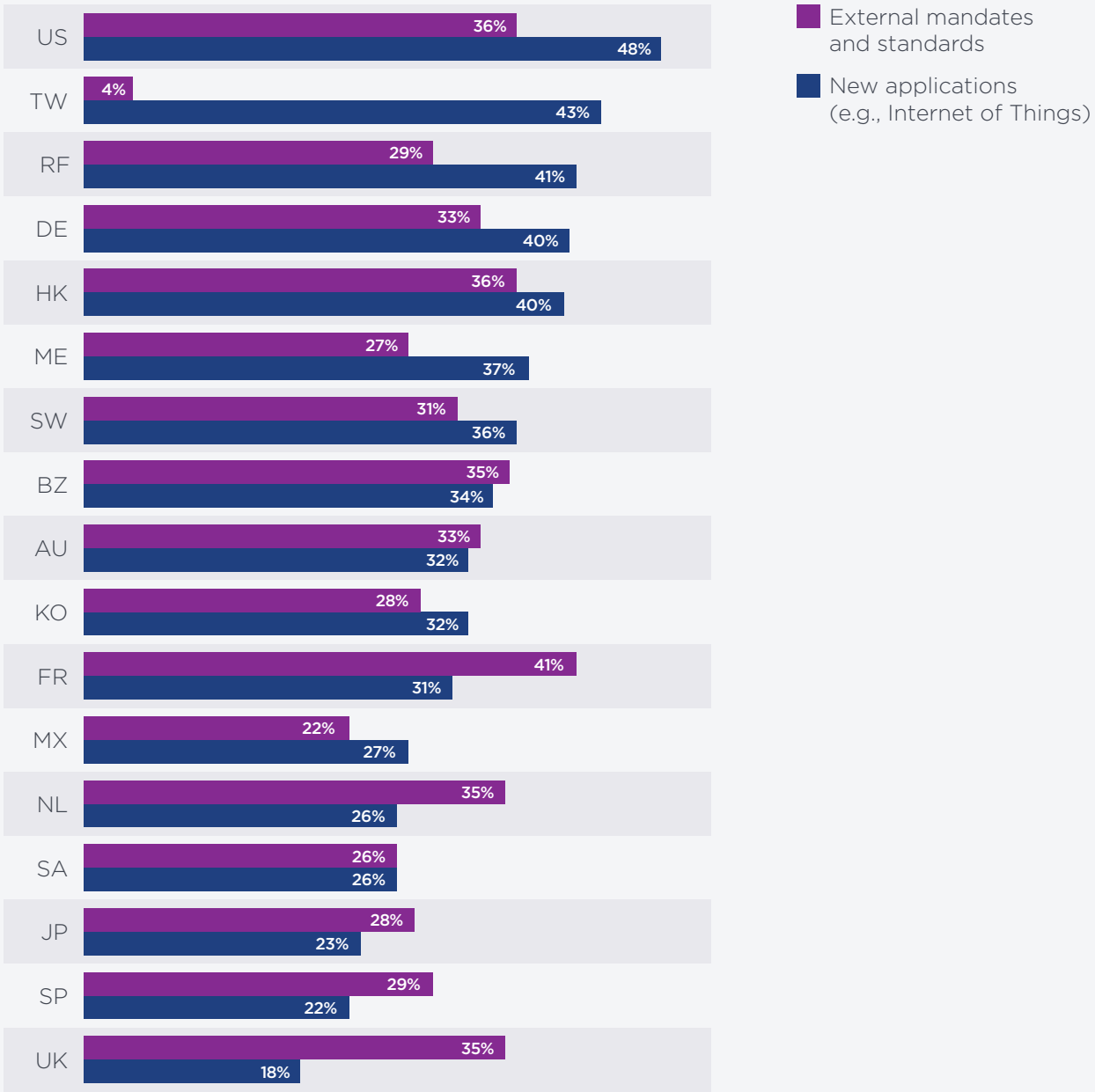
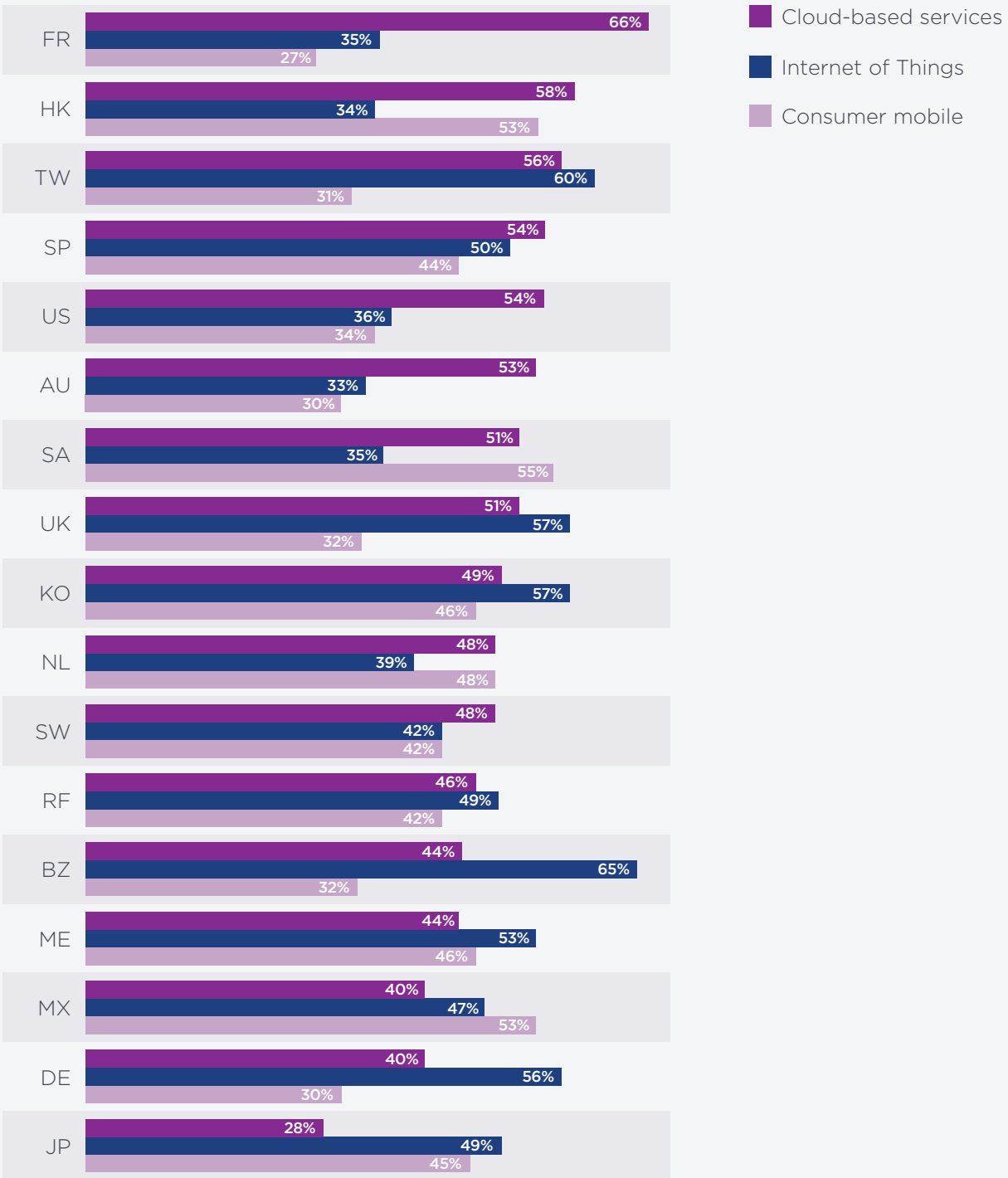


Figure 24 reports what respondents believe are the most important trends that are driving the deployment of applications that make use of PKI. As can be seen, France, Hong Kong, and Taiwan are most likely to cite cloud-based services as driving the deployment of applications that make use of PKI. Brazil, Taiwan, the UK, and Korea are most likely to see IoT as a driver to PKI adoption. Southeast Asia, Hong Kong, and Mexico are more likely to see consumer mobile as a driver.

Figure 24. **What are the most important trends that are driving the deployment of applications that make use of PKI?** (Top 3 choices)



PART 3

Methods

Table 1 reports the consolidated sample response for 17 separate country samples. Data collection was conducted in January 2022. Our consolidated sampling frame of practitioners in all countries consisted of 162,436 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 7,056 returns of which 792 were rejected for reliability issues. From our final consolidated 2022 sample of 6,264, we calculated the PKI subsample to be 2,505.

Table 1. Sample response	**Frequency**
Sampling frame	162,436
Total returns	7,056
Rejected or screened surveys	792
Overall sample (encryption trends)	6,264
PKI subsample	2,505
Ratio subsample to overall sample	41%

Figure 25 reports the respondent's organizational level within participating organizations. By design, 62 percent of respondents are at or above the supervisory levels and 37 percent of respondents reported their position as associate/staff/technician. Respondents have on average 10.4 years of security experience with approximately 9.2 years of experience in their current position.

Figure 25. **Distribution of respondents according to position level**
(Country samples are consolidated)

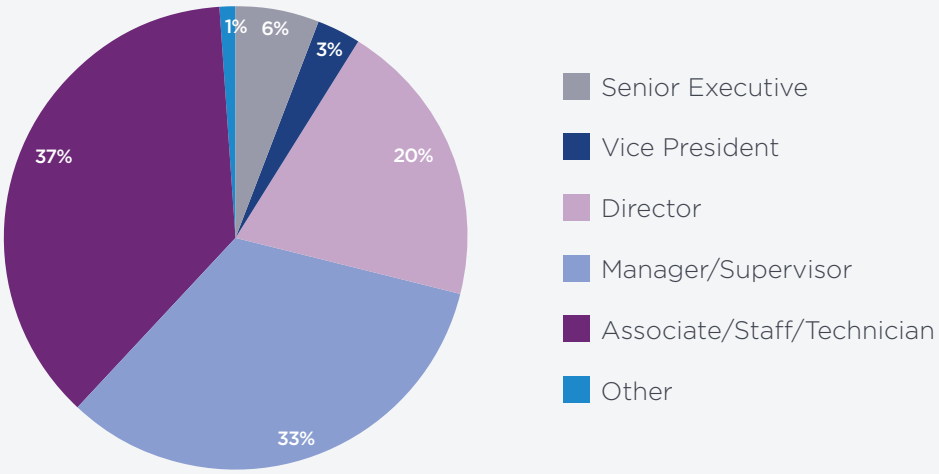


Figure 26 identifies the organizational location of respondents in our study. Almost half (46 percent) of respondents are located within IT operations. This is followed by security at 21 percent of respondents and lines of business at 13 percent of respondents.

Figure 26. **Distribution of respondents according to functional area**

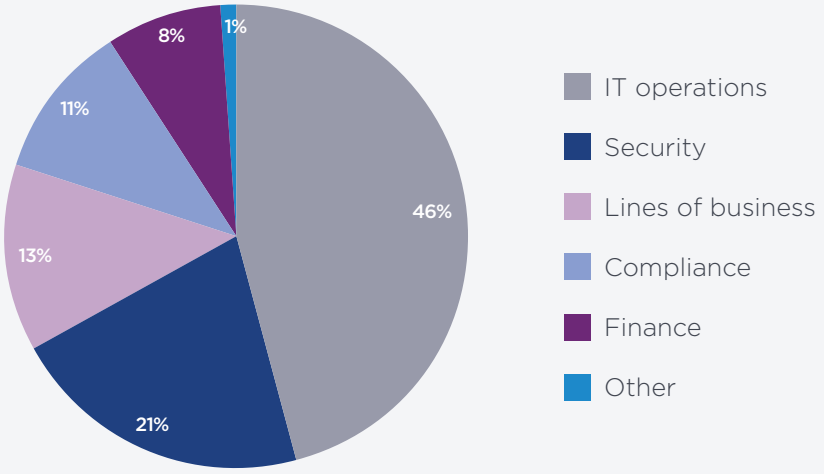
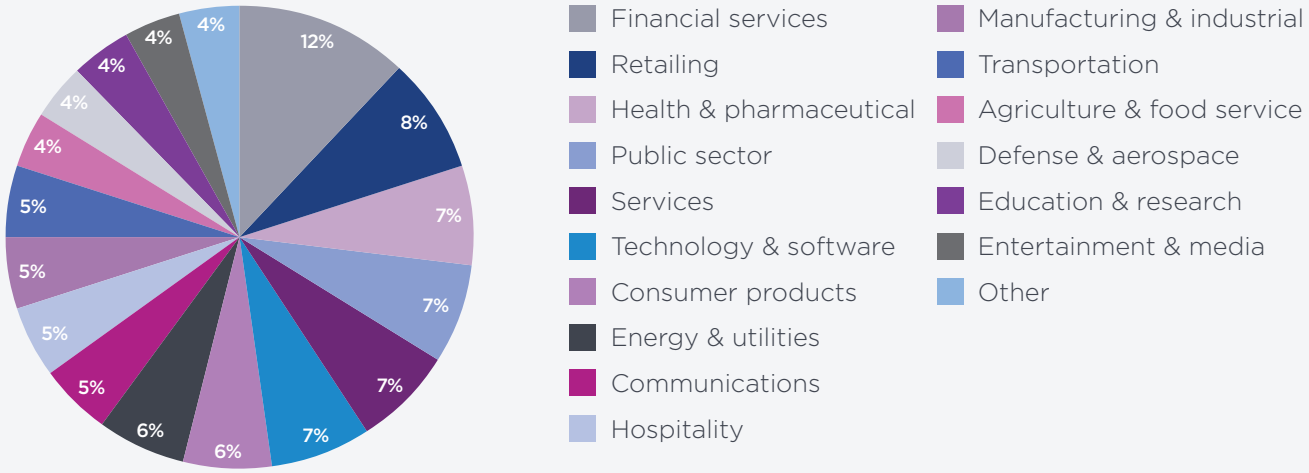


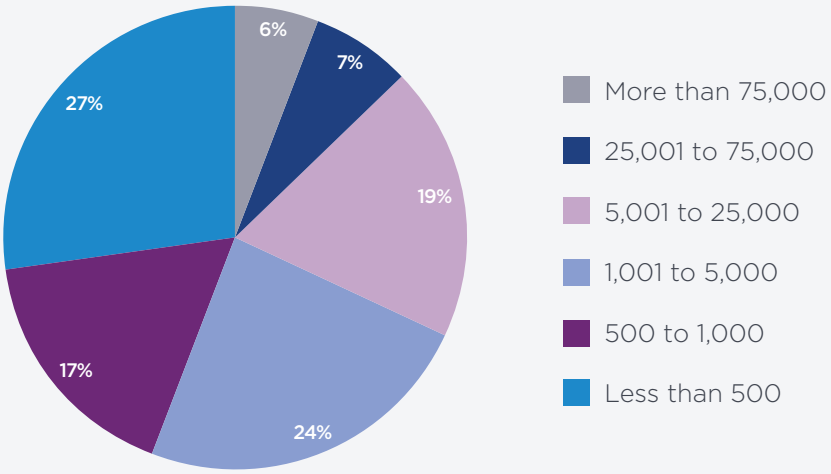
Figure 27 reports the industry classification of respondents' organizations. Twelve percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments, and credit cards. Eight percent of respondents are located in retailing and seven percent of respondents are in each of the following: health and pharmaceuticals, public sector, services, and technology and software.

Figure 27. **Distribution of respondents according to primary industry classification**
(Country samples are consolidated)



According to Figure 28, more than half (56 percent) of respondent are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 28. **Distribution of respondents according to organizational headcount**
(Country samples are consolidated)



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 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 17 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.

Ponemon INSTITUTE

About Ponemon Institute

The 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.

ENTRUST
SECURING A WORLD IN MOTION

About Entrust Corporation

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. For more information, visit **entrust.com**.

PK23Q2-2022-pki-iot-trends-study-re