THALES

Ponemon INSTITUTE

GLOBAL ENCRYPTION TRENDS STUDY

April 2017

INDEPENDENTLY CONDUCTED BY PONEMON INSTITUTE LLC

Sponsored by Thales e-Security

TABLE OF CONTENTS

PART 1. EXECUTIVE SUMMARY

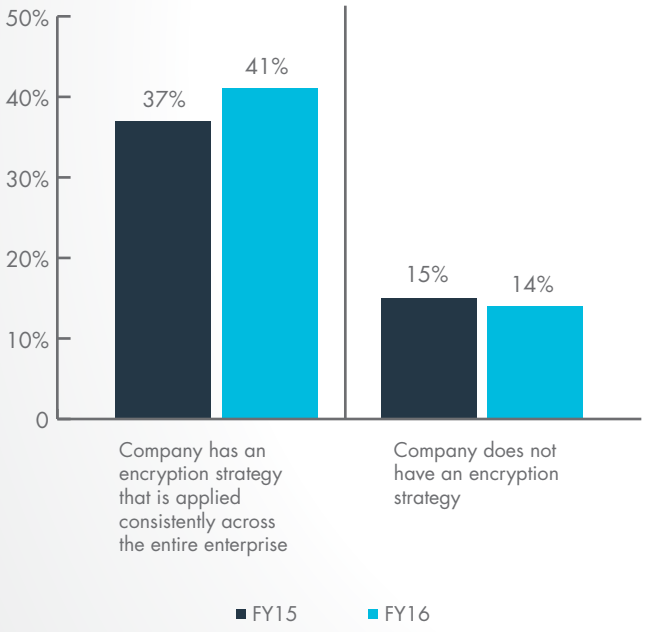
Ponemon Institute is pleased to present the findings of the 2017 Global Encryption Trends Study, sponsored by Thales e-Security. We surveyed 4,802 individuals across multiple industry sectors in 11 countries - the United States, United Kingdom, Germany, France, Australia, Japan, Brazil, the Russian Federation, Mexico, India and Arabia (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates).[2]

The purpose of this research is to examine how the use of encryption has evolved over the past 12 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a U.S. sample of respondents.[3] Since then, we have expanded the scope of the research to include respondents in all regions of the world.

In our research, we consider the threats organizations face and how encryption is being used to reduce these risks. Mega breaches and cyber attacks have increased companies' urgency to improve their security posture. This is reflected in this year's findings as more companies embrace an enterprise-wide encryption strategy—which has increased from 15 percent in FY05 to 41 percent in FY16, as shown in Figure 1.

Following is a summary of our key findings, which is organized in three subsections: (1) overall findings, (2) challenges and drivers, and (3) key management. More details are provided for each key finding listed below in the next section of this report. We believe the findings demonstrate the importance of encryption and key management in achieving a strong security posture.

Figure 1. Does your company have an encryption strategy?



[1]This year's collection of data was completed in January 2017. Throughout the report we present trend data based on the fiscal year (FY) the survey commenced rather than the year the report is finalized. Hence, our most current findings are presented as FY16. The same dating convention is used in prior years.

[2]Country-level results are abbreviated as follows: Germany (DE), Japan (JP), United States (U.S.), United Kingdom (U.K.), Australia (AU), France (FR), Brazil (BZ), Russia (RF), Mexico (MX), India (IN) and Arabian cluster (AB).

[3]The trend analysis shown in this study was performed on combined country samples spanning 12 years (since 2005).

New findings in 2017

In this year's research, we added questions about the use of Hardware Security Modules (HSMs) and public cloud services. Following are the findings.

HSM use in conjunction with cloud-based applications still favors on-premise HSM deployment. Almost half (48 percent of respondents) own and operate HSMs on-premise in support of cloud-based applications. Thirty-six percent of respondents say their organizations rent/use HSMs from a public cloud provider for their cloud applications.

Organizations will increase both on-premise and cloud HSM use in the next 12 months. Respondents say their organizations will grow their use of on-premise HSMs that are accessed real-time by cloud-hosted applications (55 percent of respondents) and will also increase their use of cloud-hosted HSMs (41 percent of respondents).

What best describes an organization's use of HSMs? Fifty-nine percent of respondents say their organization has a centralized team that provides cryptography-as-a-service (including HSMs) to multiple applications/teams within their organization using a private cloud model. Forty-one percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), reflecting a more traditional siloed application-specific data center deployment.

For the first time in the history of the study, **business unit leaders** have the **highest influence over encryption strategy** (higher than IT!)

41% of **companies** now have a consistent enterprise-wide **encryption strategy**

How do organizations protect data at rest in the cloud? Forty-six percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 37 percent of respondents rely on the cloud provider to both generate/manage keys and perform encryption.

Overall findings

Enterprise-wide encryption strategies increase. As shown in Figure 1, 41 percent of respondents in this year's study say their organization has an encryption strategy applied consistently across the entire enterprise. Only 14 percent of respondents say their organization does not have an encryption strategy.

In the first year of this study (FY05), less than 15 percent of respondents said their organization had a comprehensive encryption strategy and 38 percent did not have any strategy in place.

German organizations are more likely to have a comprehensive encryption strategy. Over 65 percent of German respondents say their organization has a comprehensive encryption strategy. In contrast, only 30 percent of Arabian and 31 percent of Mexican organizations have an encryption strategy applied consistently across the entire enterprise.

Lines of business increase their influence in determining the company's encryption strategy. Thirty percent of respondents say lines of business or general management are most influential, 29 percent say IT operations, and only 16 percent of respondents say it is the security function. Only two percent of respondents chose compliance. We see four countries – namely, France, Mexico, the U.K. and U.S. – choosing their organization's lines of business management as being most influential. The remaining seven countries chose IT operations.

The extensive use of encryption technologies increases but budgets decrease. This year we examined the usage rates for 13 encryption technology categories. Our analysis shows a substantial increase in the percentage of respondents who say their organizations are extensive rather than partial users. Extensive use means the encryption technology is used consistently across the entire enterprise. Partial use means the given technology is a point solution or is narrowly deployed.

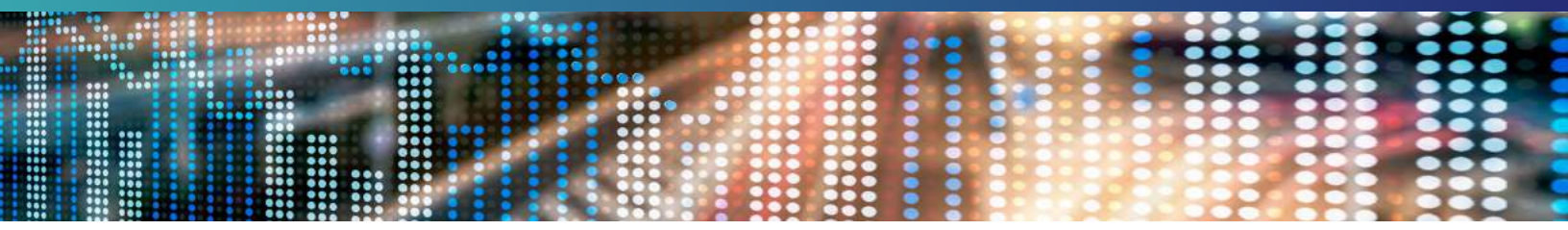
In FY05, only 16 percent of respondents were extensive users as compared to 41 percent in FY16. While the extensive use of encryption has steadily increased over 12 years, the percentage of the IT budget earmarked for encryption has actually decreased in the last three years.

The extensive use of encryption varies considerably by industry segment. Specifically, heavily regulated industries such as financial services and healthcare have the highest use rate; less regulated industries such as manufacturing and consumer products have the lowest use rate. Trends over the past four years suggest a steady increase in all industry segments. The most significant increases in extensive encryption usage occur in public sector, retail and technology and software organizations.

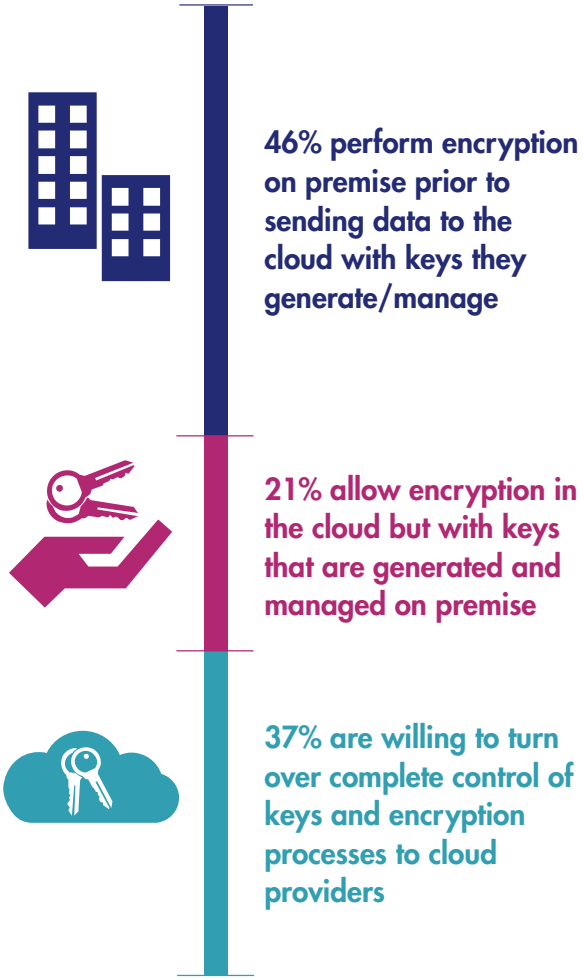
Challenges, drivers and usage

Employee mistakes are the most significant threat to sensitive data. According to 54 percent of respondents, employee error is the most significant threat to sensitive or confidential data. Thirty percent chose hackers and 29 percent chose systems or process malfunction as their most significant threat. The fact that two of the top three findings on threats relate to mistakes or errors, as opposed to targeted threats, is notable.

COMPLIANCE REMAINS THE TOP DRIVER FOR ENCRYPTION, HOWEVER IT IS FOLLOWED BY A CLOSE MARGIN BY IP PROTECTION, CUSTOMER INFORMATION PROTECTION, AND PROTECTION FROM EXTERNAL THREATS



Organizations continue to show a preference for **control over encryption** in the cloud



Compliance continues to be the main driver to invest in the extensive use of encryption. Fifty-five percent of respondents see compliance with privacy and data security requirements as the main driver to extensive encryption use within their company. Not far behind, 51 percent of respondents see protecting enterprise intellectual property as the main driver. The least significant drivers include avoiding data breach disclosures (10 percent of respondents) and compliance with internal policies (19 percent of respondents).

What is the biggest challenge to encryption deployment? Fifty-nine percent of respondents say discovering where sensitive data resides in the organization is their most difficult challenge. This is not surprising for the following reasons: the proliferation of data that is occurring with increased connectivity, larger numbers of endpoint devices and increased use of the cloud. In addition, 47 percent of all respondents cite initially deploying encryption technology as a significant challenge and 36 percent of respondents see classifying what data to encrypt as a significant challenge.

Looking across 13 encryption categories, we observe that no single technology dominates the encryption portfolio because organizations have very diverse needs. Encryption of databases, Internet communications and data center storage are the most likely to be deployed (89 percent, 85 percent and 80 percent, respectively). In contrast, encryption for big data repositories (53 percent of respondents), public cloud services (55 percent of respondents) and private cloud infrastructure (59 percent) have lower use rates but have grown from the previous year.

The use of encryption varies among countries. Respondents in Germany, U.S., Japan and U.K. have the highest deployment rates. Arabia, Mexico and Australia have the lowest deployment rates.

Certain encryption technology features are more important than others. Respondents were asked to rate encryption technology features considered most important to their organization's security posture. According to the consolidated findings, the three most important features are: (1) system performance and latency (2) enforcement of policy and (3) support for cloud and on-premise deployment. The consistent year-over-year top finding of performance and latency underscores the importance organizations place on encryption that is transparent and without negative consequences to other functions and systems.

IT security spending is increasing. The average percentage of IT security spending relative to total IT spending over 12 years has increased. The trend appears to be upward sloping, which suggests the proportion of IT spending dedicated to security activities, including encryption, is increasing over time.

Data protection spending is increasing as well. The percentage of data protection spending relative to the total IT security budget over 12 years has increased. This trend appears to be slightly upward sloping, which suggests data protection spending as a proportion of total IT security is also on the rise.

The 12-year trend in the percentage of encryption spending relative to the total IT security budget has increased from a low of 9.7 percent in FY05 to a high of 18.2 percent in FY13. We postulate three reasons for a recent decrease: (1) price pressure resulting from increased competition among vendors, (2) shifting priorities to other IT security solution areas and (3) more efficient use of presently available encryption tools.

Companies are transferring sensitive or confidential data to the cloud. Fifty-three percent of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking. With respect to the transfer of sensitive or confidential data to the cloud, India (70 percent of respondents), Mexico (67 percent) and the U.S. (60 percent of respondents) have higher use rates than other countries. In contrast, Germany has the lowest rate.

Encryption deployment grew the most in **Big Data, Databases, and Public Cloud**

Key management and HSMs

Respondents rated the overall "pain" associated with managing keys within their organization. Fifty-nine percent of respondents rate the management of keys at a fairly high pain level. With respect to country-level results, Arabia has the highest pain level and Russia has the lowest pain level.

Why is the pain level high? The following are the top three reasons why the management of keys is so painful: (1) no clear ownership of the key management function, (2) lack of skilled personnel and (3) isolated or fragmented key management systems.

According to respondents, the types of keys that are most difficult to manage include: (1) keys for external cloud or hosted services and (2) SSH keys. The least difficult are: (1) embedded device keys, (2) encryption keys for backups and storage and (3) encryption keys for archived data.

Companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) manual process (paper or spreadsheets), (2) formal key management policy and (3) central key management system/ server. The fact that manual processes remain the most popular indicates reluctance to adopt tools, possibly due to lack of standardization or lack of general awareness.

Respondents in Germany, U.S. and Japan are most likely to deploy HSMs as part of their organization's key management program – an indication of their overall higher encryption and security maturity. The overall usage rate for HSMs has steadily increased over the past four years—and rose from 34 percent in FY15 to 38 percent in FY16.

The importance of HSMs to encryption and key management activities has increased. The overall average importance rating in the current year is 56 percent of respondents, which represents an increase from prior years. The pattern of responses suggests organizations in Germany, US and Japan are most likely to attribute high importance to HSMs.

What are the primary purposes for deploying HSMs? According to respondents, the two top choices are SSL/TLS and application-level encryption. Several application areas were noted as growing 4% or more over the next 12 months, including SSL/TLS, database encryption, PKI credential management, payment transaction processing, and payment credential issuing.

KEY FINDINGS:

Strategy and adoption of encryption

Enterprise-wide encryption strategies increase. Since first conducting this study 12 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having an encryption plan or strategy. The results have essentially reversed over the years of the study, and this year's study additionally revealed the largest year-over-year increase in encryption strategy since FY12 to FY13. Figure 2 shows these changes over time.

Overall Hardware Security Module (HSM) use grew to 38%

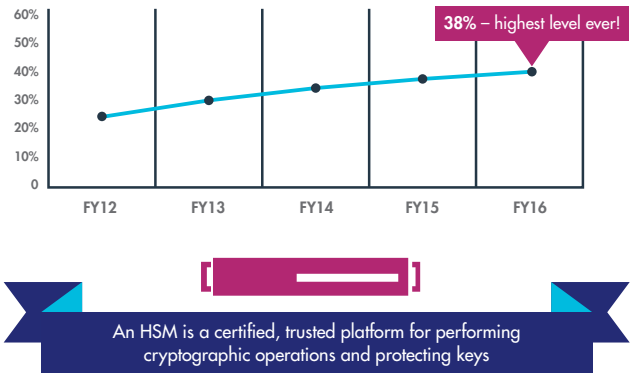
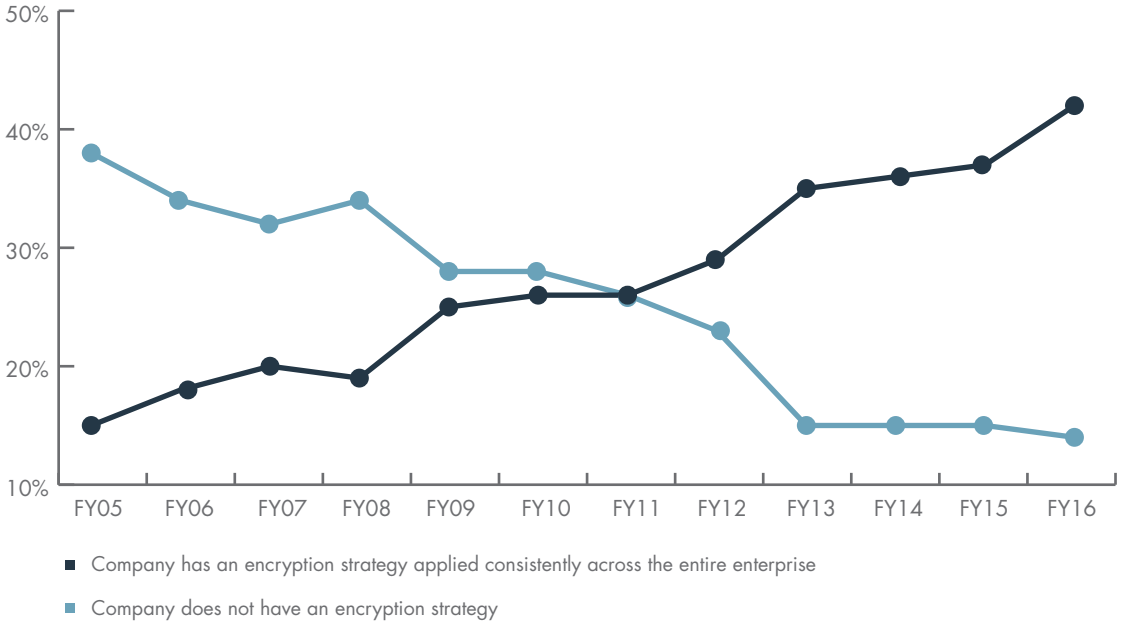


Figure 2. Trends in encryption strategy
Country samples are consolidated



According to Figure 3, the prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany followed by the U.S. and Japan. Respondents in Arabia, Mexico, Australia and Brazil report the lowest adoption of an enterprise encryption strategy.

Figure 3. Differences in enterprise encryption strategies by country

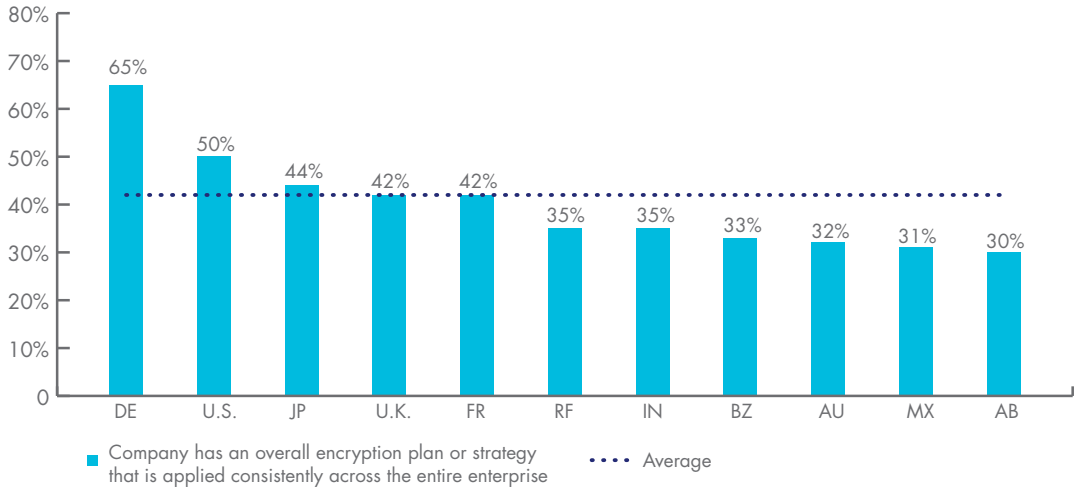


Figure 4 shows that lines of business have overtaken IT operations in terms of their influence over encryption strategy. It is interesting to note that this is a significant change from the early years of this study, with business unit leaders gradually gaining influence over their company's encryption strategy – from 10 percent in FY05 to 30 percent in FY16. In contrast, IT operations decreased significantly from 53 percent in FY05 to 29 percent in FY16.

We posit that the rising influence of business leaders reflects a general increase in concerns over data privacy and the importance of demonstrating compliance with privacy and data protection mandates. It is also probable that the rise of employee-owned devices or BYOD and the general consumerization of IT have had an effect. It is interesting to note that the influence of the security function on encryption strategy has slightly increased over time.

Figure 4. Influence of IT operations, lines of business and security
Country samples are consolidated

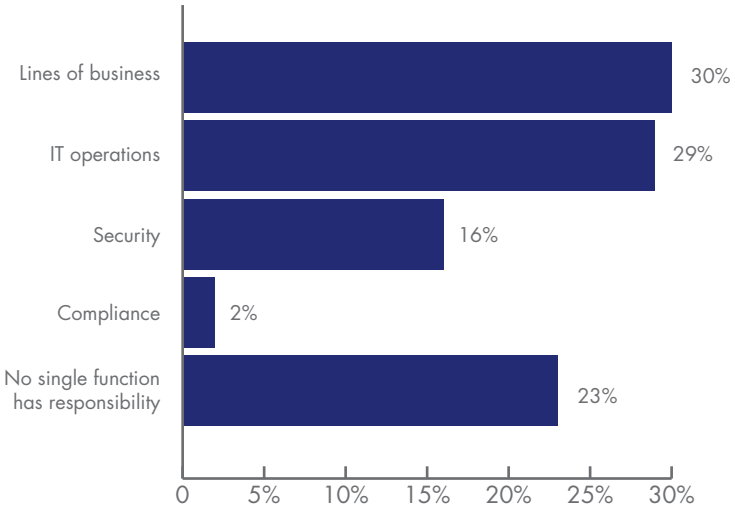
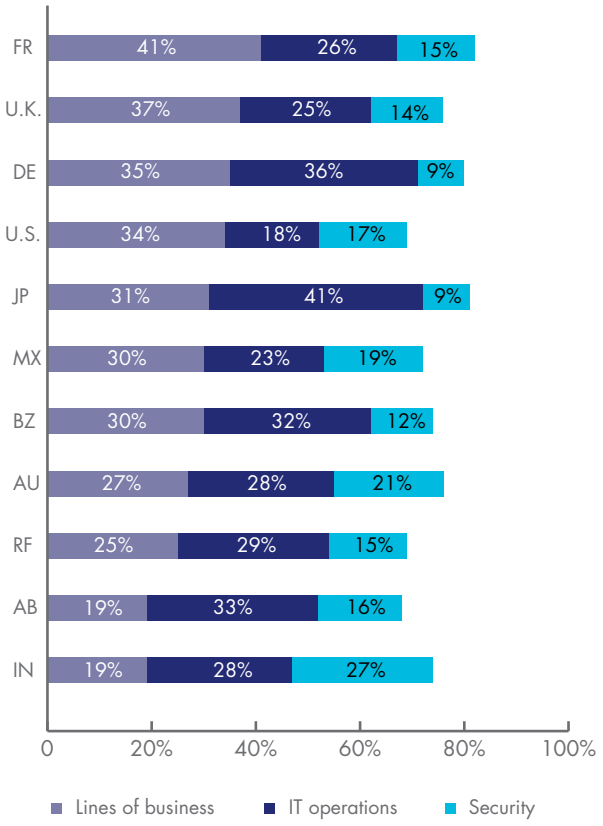


Figure 5 shows the percentage distribution of respondents who rate lines of business (LOB), IT operations, and security as most influential in determining their organization's encryption strategy. This chart shows four countries rating LOB as most influential, and seven rating IT operations as most influential in determining the company's encryption strategy.

Figure 5. Influence of lines of business, IT operations, and security by country



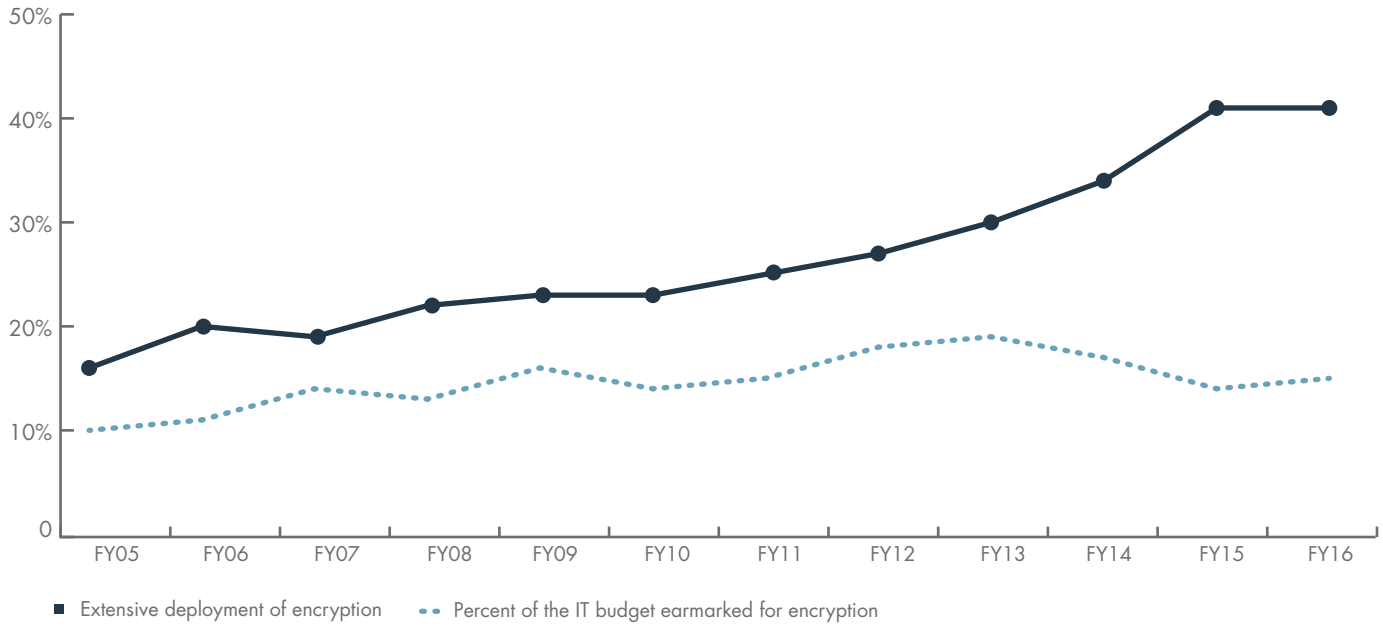
Trends in adoption of encryption

The extensive use of encryption technologies increases. Since we began tracking the enterprise-wide use of encryption in 2005, there has been a steady increase in the encryption solutions extensively used by organizations.[4]

Figure 6 summarizes enterprise-wide usage consolidated for various encryption technologies over 12 years. This continuous growth in enterprise deployment suggests encryption is important to an organization's security posture. Figure 6 also shows the percentage of the overall IT security budget dedicated to encryption-related activities.

The pattern for deployment and budget show a positive correlation through FY12 and inverse relationship through FY16. We postulate three reasons for this downward trend: (1) price pressure resulting from increased competition among vendors, (2) shifting priorities to other IT security solution areas and (3) more efficient use of presently available encryption tools.

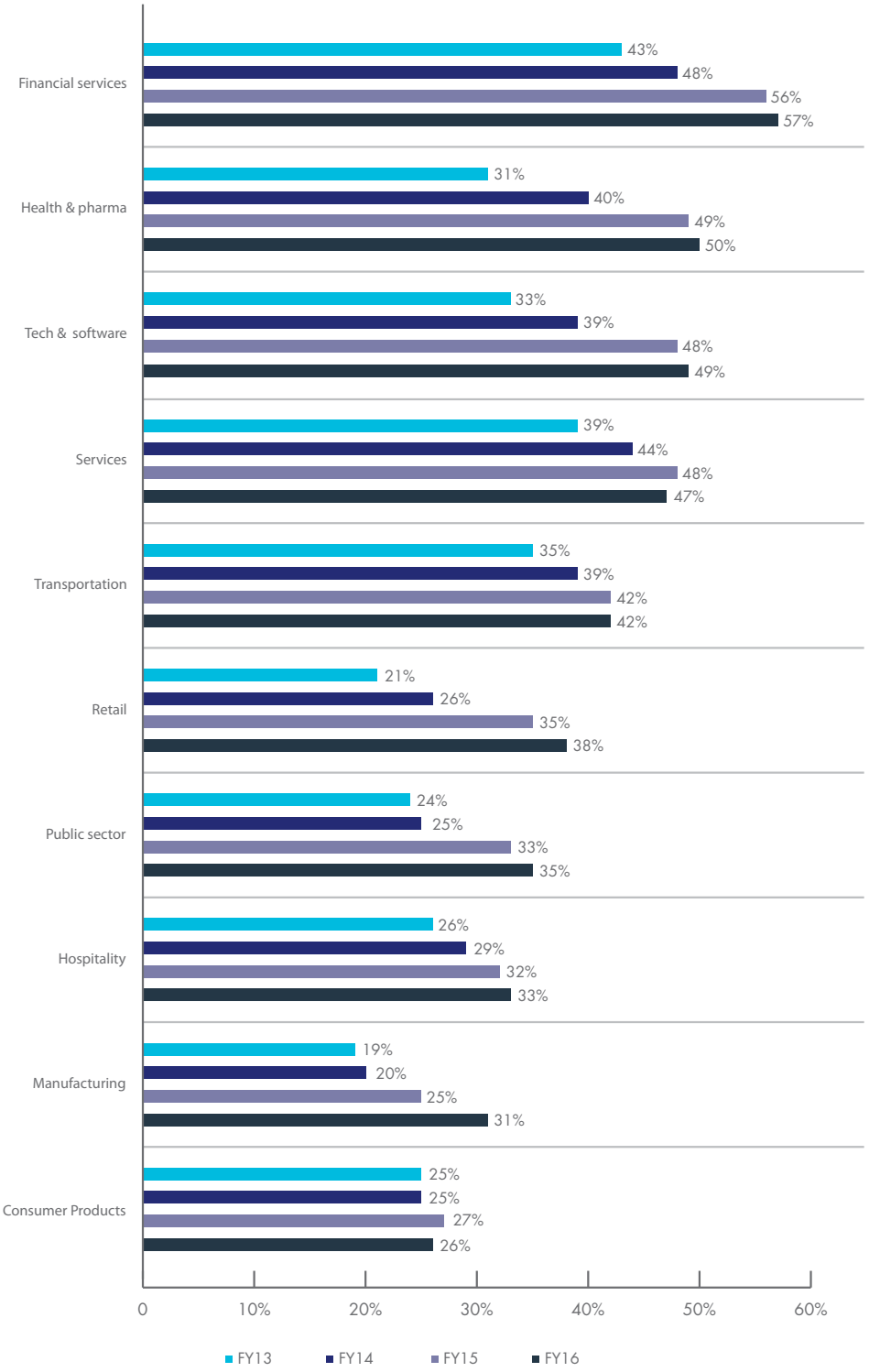
Figure 6. Trend on the extensive use of encryption technologies
Country samples are consolidated



[4]The combined sample used to analyze trends is explained in Appendix 1.

The use of encryption increases in all industries. Figure 7 shows the extensive usage of encryption solutions for 10 industry sectors over four years. Results suggest a steady increase in all industry sectors. The most significant increases in extensive encryption usage occur in public sector, retail and technology and software organizations.

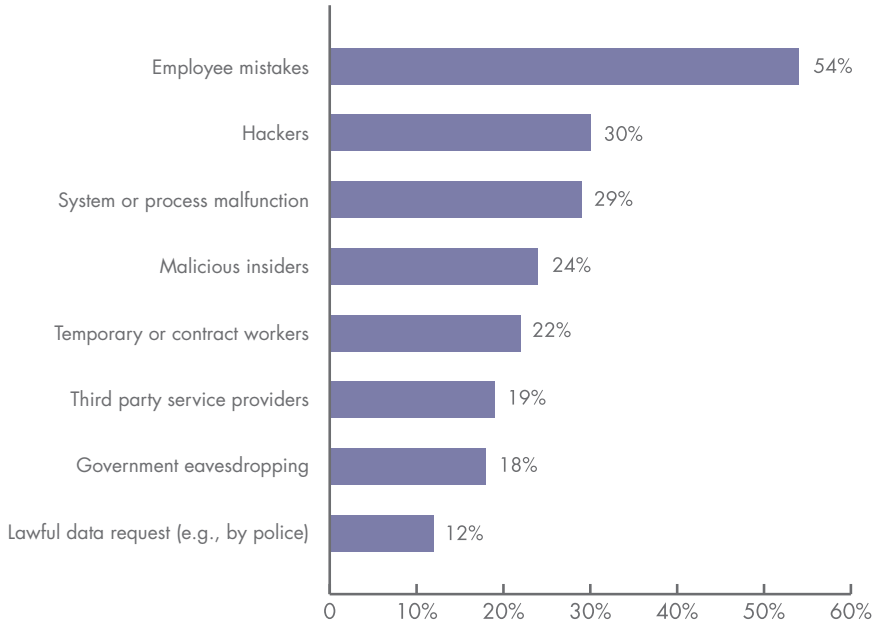
Figure 7. The extensive use of encryption by industry
Country samples are consolidated (Avg of 13 encryption categories)



Threats, main drivers and priorities

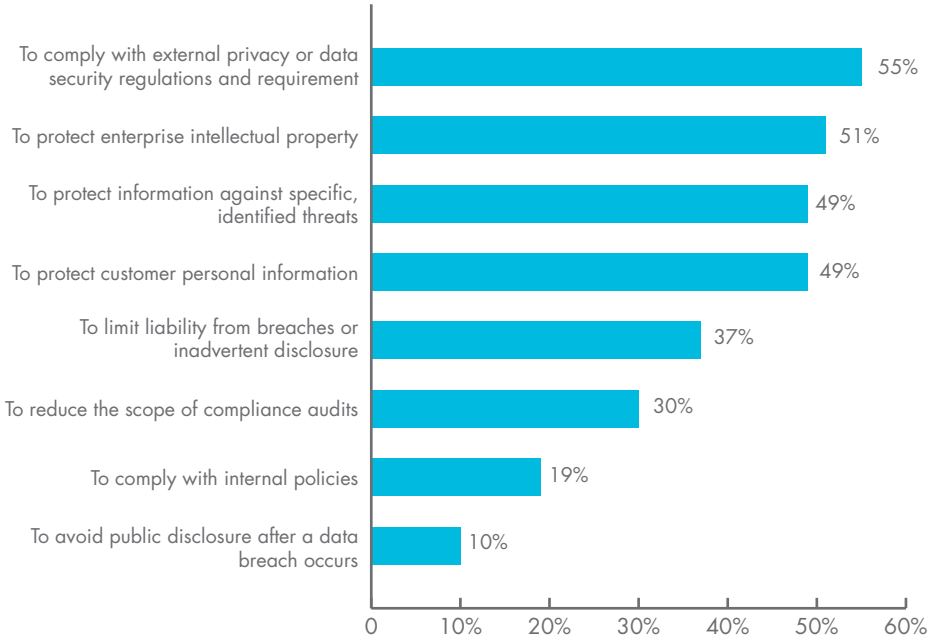
Employee mistakes are the most significant threat to sensitive data. Figure 8 shows that the most significant threats to the exposure of sensitive or confidential data are employee mistakes and hackers. In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) significantly outweigh concerns over actual attacks by hackers and malicious insiders. It is interesting to note that the employee mistake threat is equal to the combined threat by both hackers and insiders.

Figure 8. The most salient threats to sensitive or confidential data
Country samples are consolidated (More than one choice permitted)



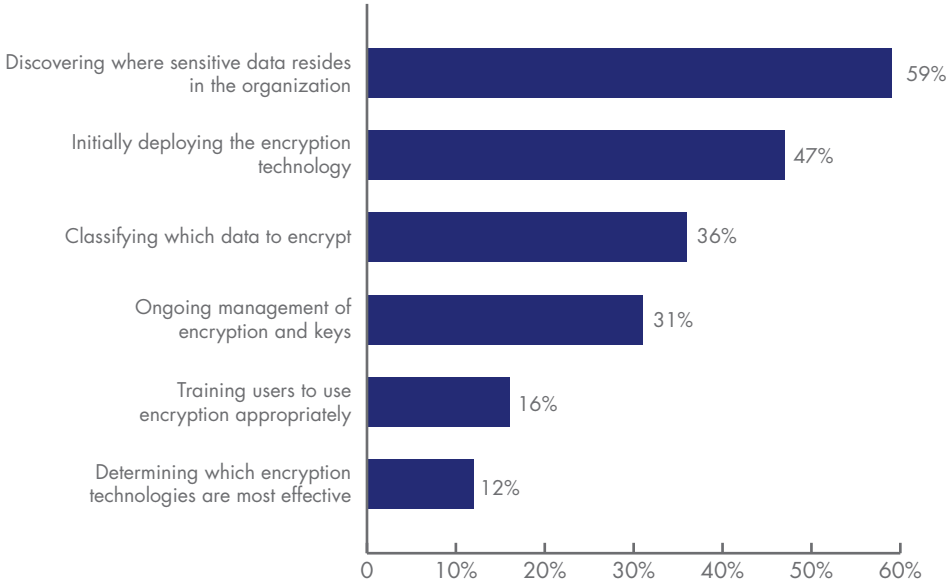
Fifty-five percent of respondents see compliance with privacy and data security requirements as the main driver to using encryption technologies. Eight drivers for deploying encryption are presented in Figure 9. Respondents report compliance with regulations as the top driver, which is consistent with previous years where mandated usage is the strongest reason to deploy encryption. However, the results that follow that indicate that respondents are increasingly likely to deploy encryption as a best practice in their security protection profile. The least significant drivers include avoiding data breach disclosures and compliance with internal policies.

Figure 9. The main drivers for using encryption technology solutions
Country samples are consolidated (Three responses permitted)



Discovering where sensitive data resides in the organization is the biggest challenge. Figure 10 provides a list of six aspects that present challenges to the organization's effective execution of its data encryption strategy in descending order of importance. Remaining in the top position from FY05, 59 percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 47 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-six percent cite classifying which data to encrypt as difficult.

Figure 10. Biggest challenges in planning and executing a data encryption strategy
Country samples are consolidated (More than one choice permitted)

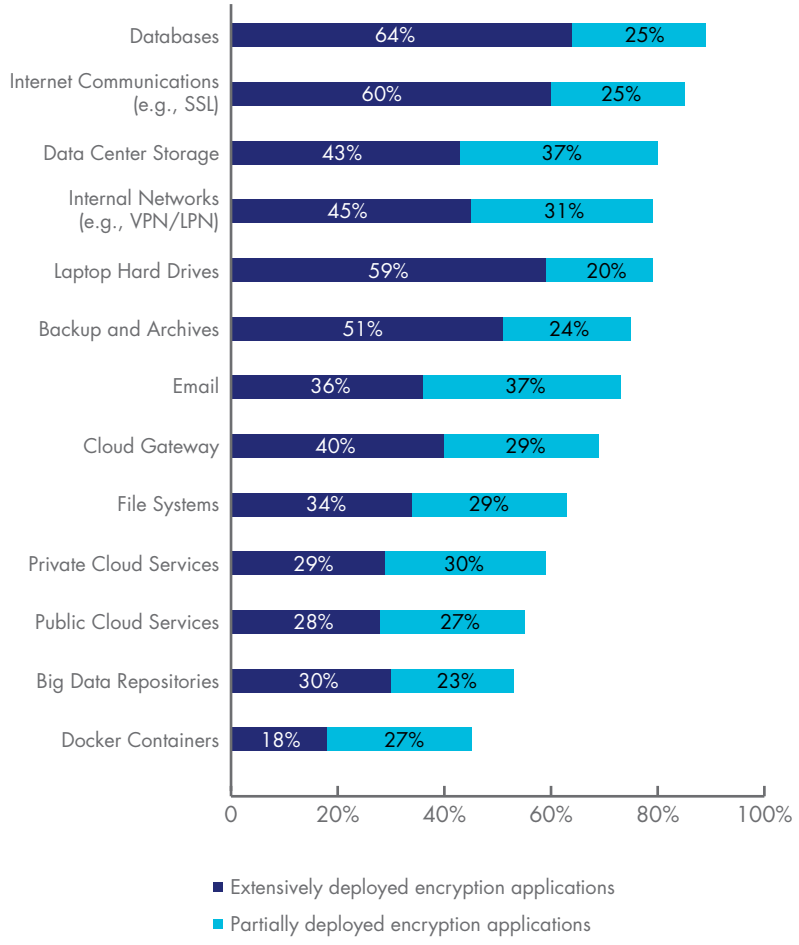


Deployment choices

No single encryption technology dominates in organizations. We asked respondents to indicate if specific encryption technologies are widely or only partially deployed within their organizations. "Extensive deployment" means that the encryption technology is deployed enterprise-wide. "Partial deployment" means the encryption technology is confined or limited to a specific purpose (a.k.a. point solution).

As shown in Figure 11, no single technology dominates because organizations have very diverse needs. Encryption of databases, Internet communications and data center storage are the most likely to be deployed and correspond to mature use cases. In contrast, encryption technologies for use cases that continue to emerge – such as big data repositories, public cloud services, private cloud infrastructure and docker containers – have a lower deployment rate but are all demonstrating year on year growth.

Figure 11. Consolidated view on the use of 13 encryption technologies
Country samples are consolidated



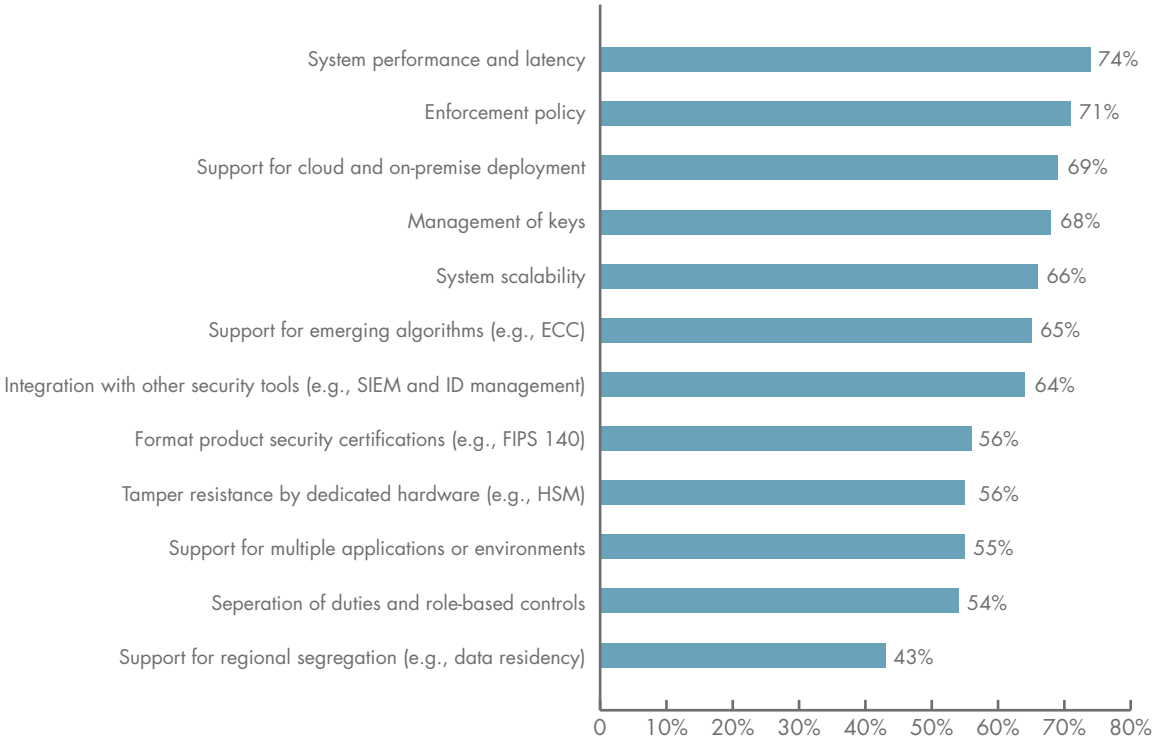
Encryption features considered most important

Certain encryption features are considered more critical than others. Figure 12 lists encryption technology features. Each percentage defines the very important response (on a four point scale). Respondents were asked to rate encryption technology features considered most important to their organization's security posture.

According to consolidated findings, system performance and latency, enforcement of policy and support for cloud and on-premise deployment are the three most important features. The performance finding is not surprising given that encryption in networking is a prominent use case, as well as the often emphasized requirement for transparency of encryption solutions. Support for both cloud and on-premise deployment has risen in importance as organizations have increasingly embraced cloud computing and look for consistency across computing styles.

In fact, the top findings in this area all correspond to features considered increasingly important for cloud solutions. Integration with other security tools such as SIEM and ID management has increased since last year as an important feature of encryption technology solutions.

Figure 12. Most important features of encryption technology solutions
Country samples are consolidated (Very important response)



Which data types are most often encrypted? Figure 13 provides a list of seven data types that are routinely encrypted by respondents' organizations. As can be seen, human resource data is the most likely data type to be encrypted – suggesting that encryption has now moved into the realm where it needs to be addressed by companies of all types. Of these data types, the largest percentage increase in the use of encryption was for customer information.

Figure 13. Data types routinely encrypted
Country samples are consolidated (More than one choice permitted)

Attitudes about key management

How painful is key management? Using a 10-point scale, respondents were asked to rate the overall "pain" associated with managing keys within their organization, where 1 = minimal impact to 10 = severe impact. Figure 14 clearly shows that 59 (23+36) percent of respondents in FY16 chose ratings at or above 7; thus, suggesting a fairly high pain threshold.

Figure 14. Rating on the overall impact, risk and cost associated with managing keys (Country samples are consolidated)

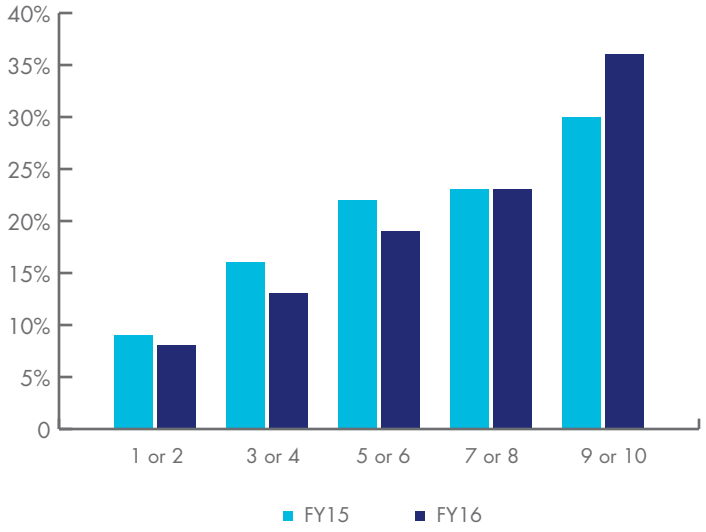
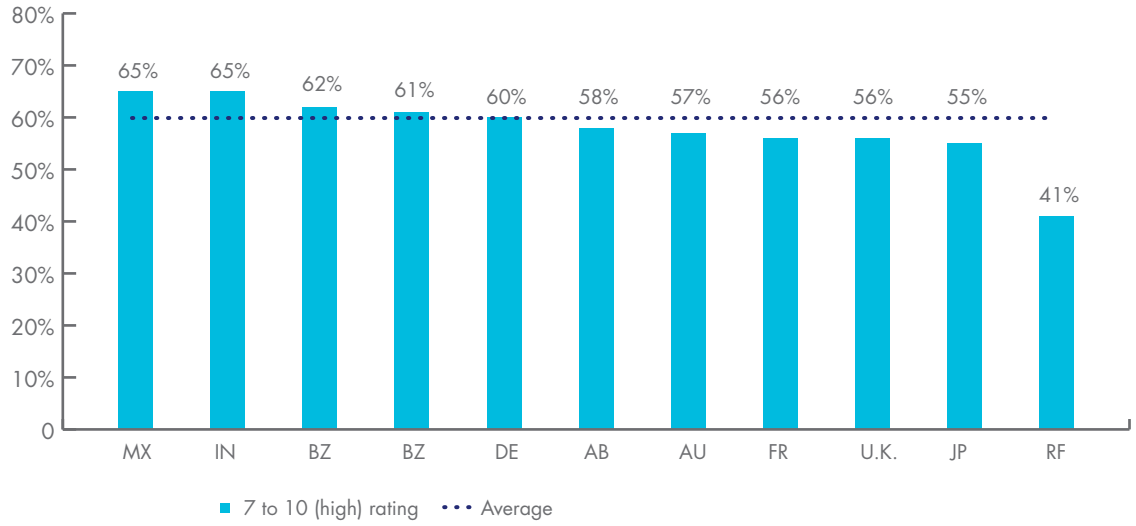


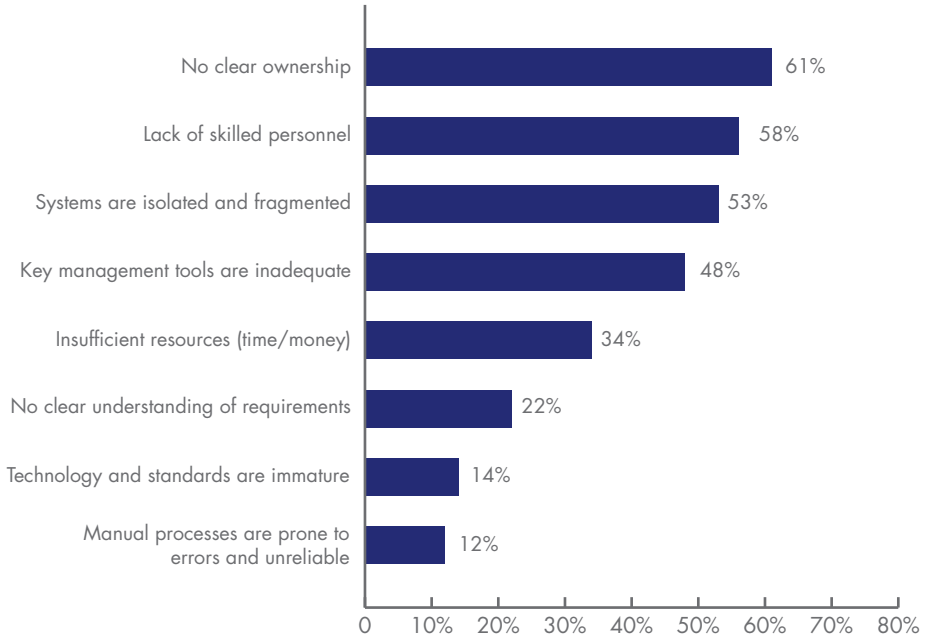
Figure 15 shows the 7+ ratings on a 10-point scale for each country. As can be seen, the average percentage in all country samples is 59 percent, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 65 percent occurs in Mexico and India. At 41 percent, the lowest pain level occurs in Russia.

Figure 15. Percentage "pain threshold" by country
Percentage 7 to 10 rating on a 10 point scale



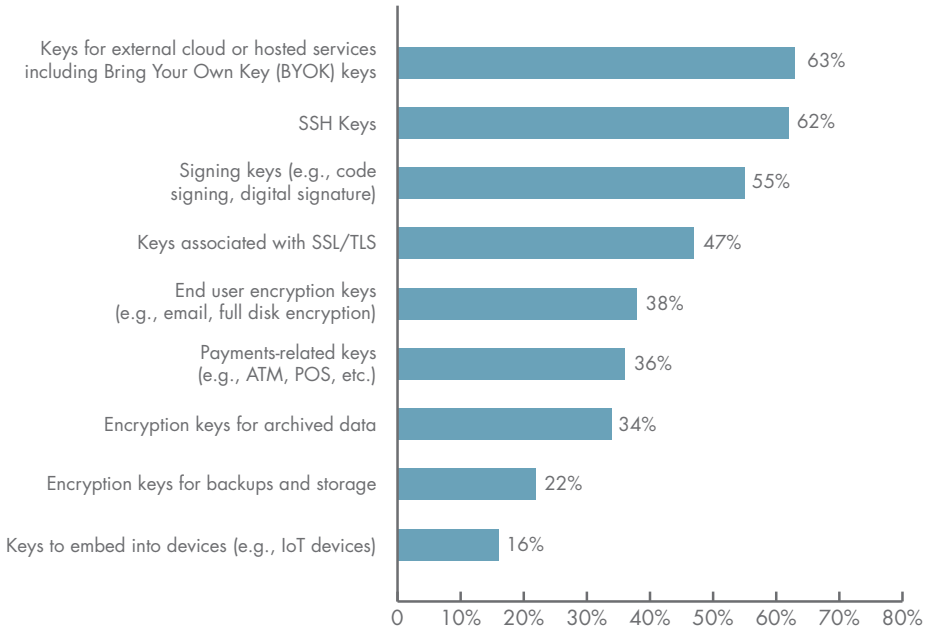
Why is key management painful? Figure 16 shows the reasons why the management of keys is so difficult. The top three reasons are: (1) no clear ownership of the key management function, (2) lack of skilled personnel and (3) isolated or fragmented key management systems.

Figure 16. What makes the management of keys so painful?
Country samples are consolidated (More than one choice permited)



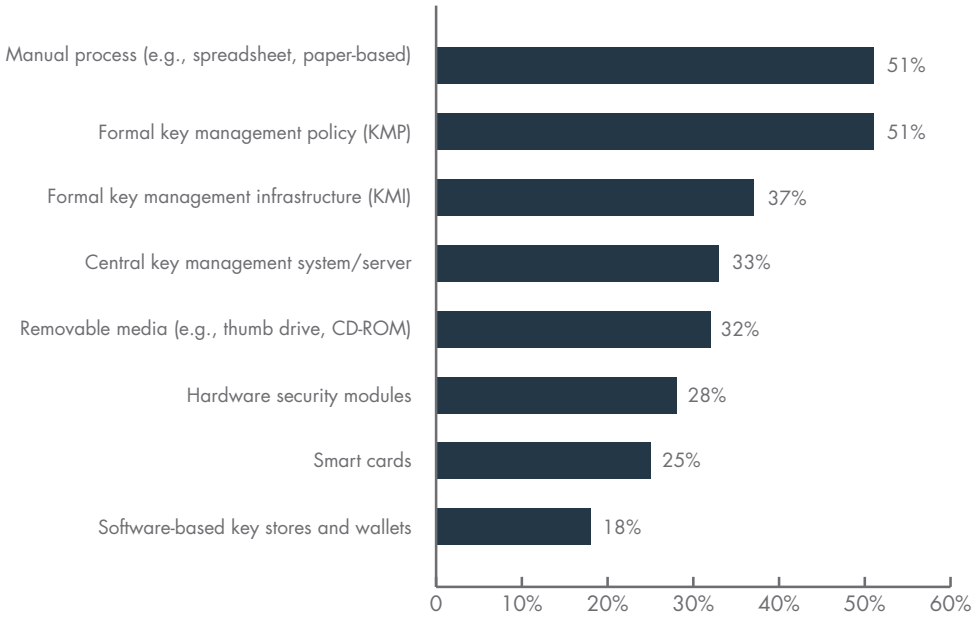
Which keys are most difficult to manage? Moving into the top position on this list for the first time this year, keys for external cloud or hosted services rank as the most difficult keys to manage. As shown in Figure 17, this is followed by SSH keys, signing keys and keys for SSL/TLS. The least difficult include: (1) encryption keys for archived data, (2) encryption keys for backups and storage and (3) embedded device keys and certificates.

Figure 17. Types of keys most difficult to manage
Country samples are consolidated (Very painful and painful response)



As shown in Figure 18, respondents' companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) manual process, (2) formal key management policy and (3) formal key management infrastructure (KMI).

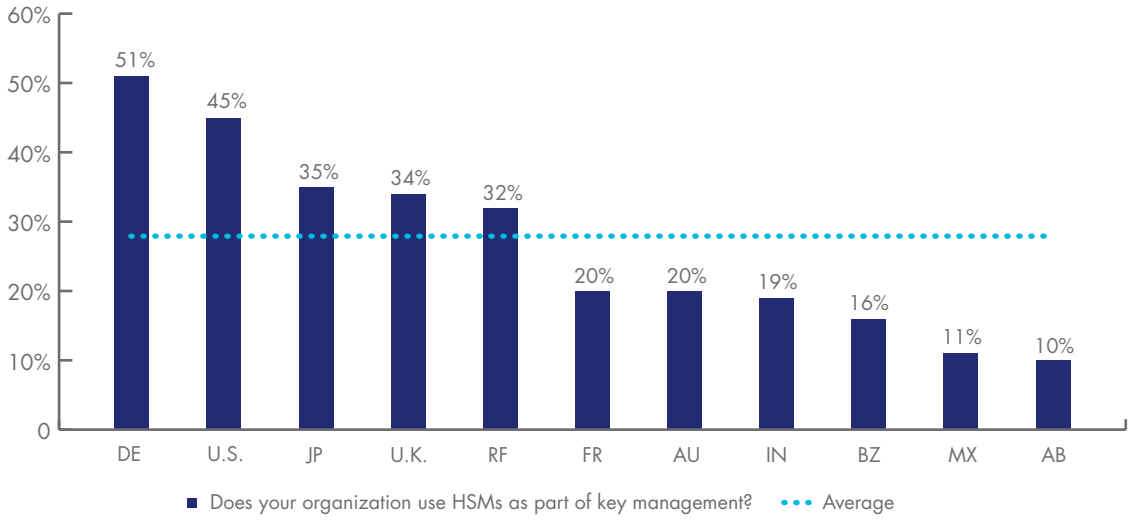
Figure 18. What key management systems does your organization presently use?
Country samples are consolidated (More than one choice permitted)



Importance of Hardware Security Modules (HSMs)[5]

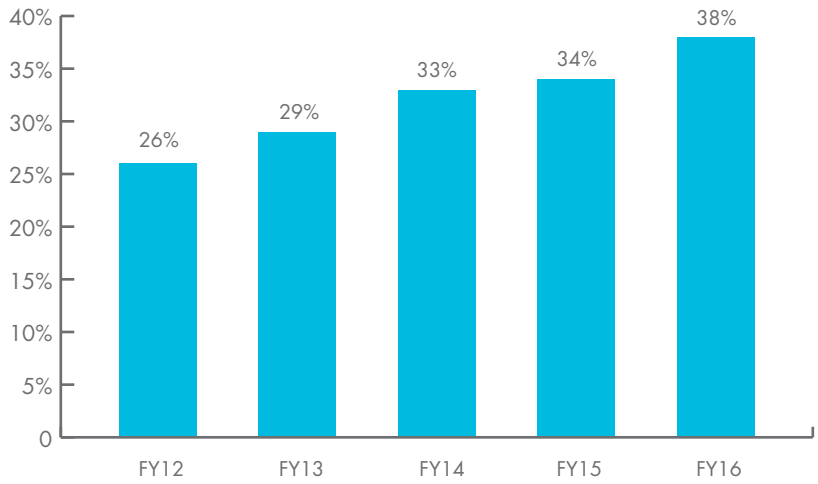
German, U.S. and Japanese organizations are more likely to deploy HSMs for key management. Figure 19 summarizes the percentage of respondents that deploy HSMs specifically as part of their organization's key management program or activities. The overall average deployment rate for HSMs as part of key management activities is 28 percent.

Figure 19. Deployment HSMs as part of key management



Deployment of HSMs increases steadily. Figure 20 shows a five-year trend for overall deployment of HSMs. As can be seen, the rate of global HSM deployment has steadily increased and reached an all time high in this year's study.

Figure 20. HSM deployment rate over five years
Country samples are consolidated



[5]HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g. encryption or digital signing) and to manage the keys associated with those processes. These devices are used to protect critical data processing activities and can be used to strongly enforce security policies and access controls. HSMs are typically validated to formal security standards such as FIPS 140-2.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. As shown in Figure 21, almost half (48 percent of respondents) own and operate HSMs on-premise for cloud-based applications and 36 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, both figures will increase by 7 and 5 percent, respectively. Interestingly, the use of HSMs with Cloud Access Security Brokers is expected to double in the next 12 months.

Figure 21. Use of HSMs in conjunction with public cloud-based applications today and in the next 12 months

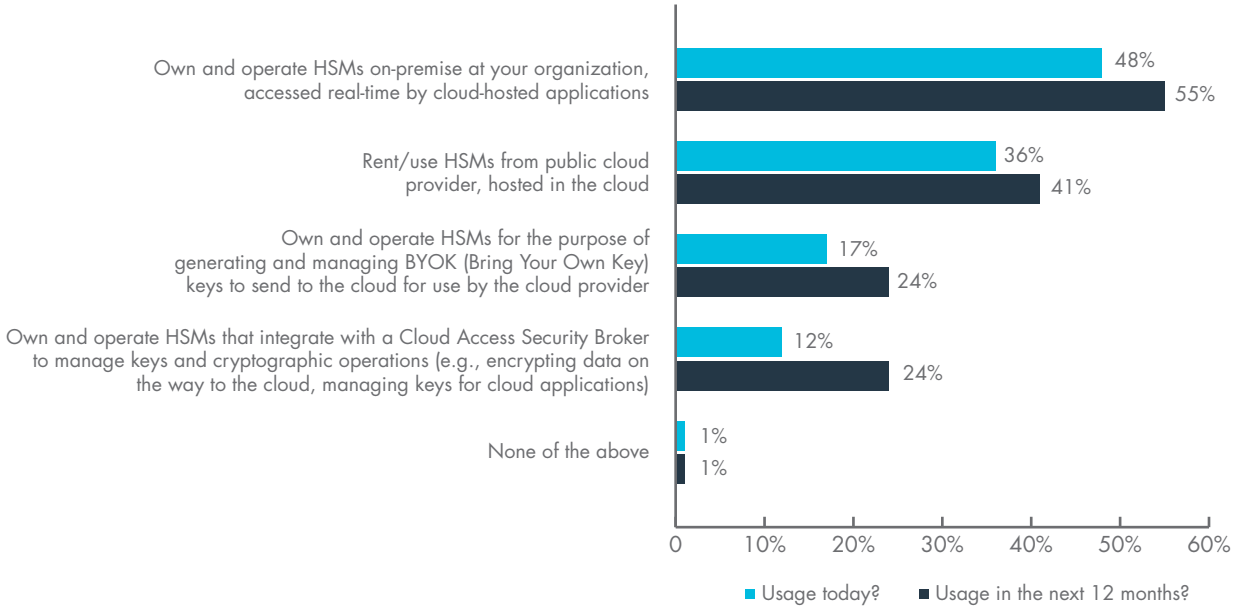


Figure 22 summarizes the percentage of respondents in 11 countries that rate HSMs as either very important or important to their organization's encryption or key management program or activities. The overall average importance rating in the current year is 56 percent. The pattern of responses suggests Germany, U.S. and Japan are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

Figure 22. Perceived Importance of HSMs as a part of key management
Important & Very important response

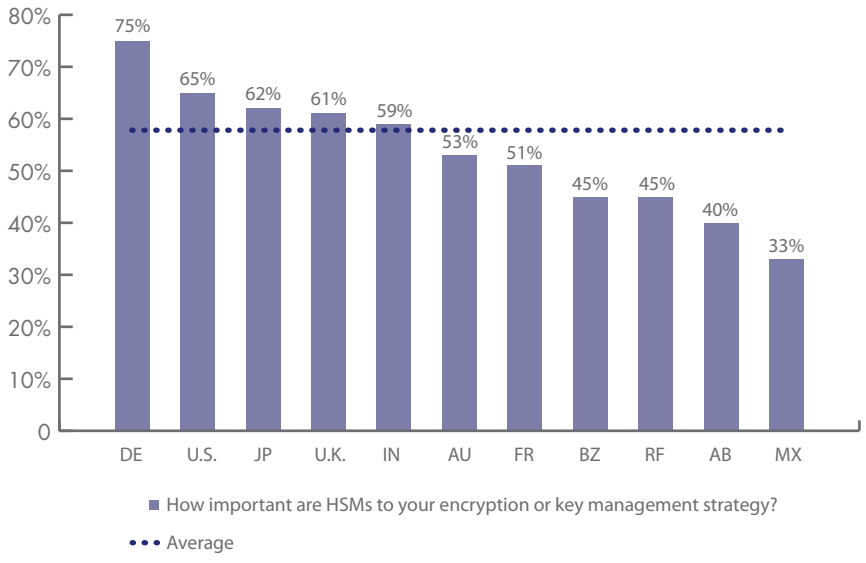
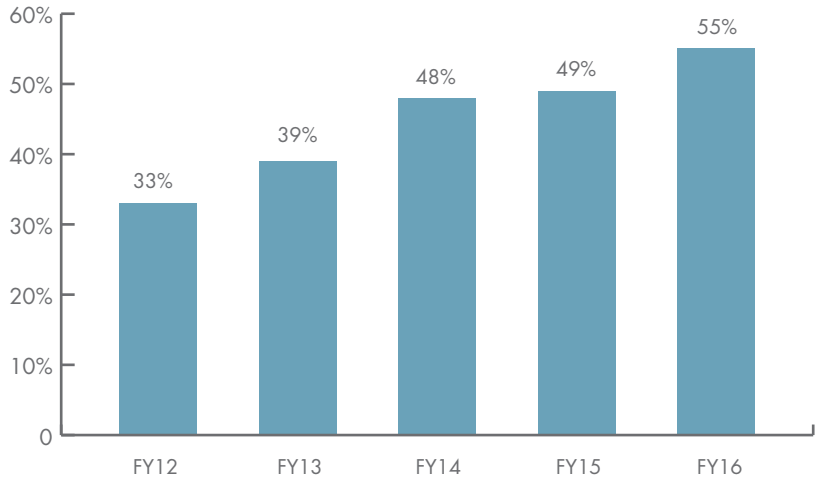


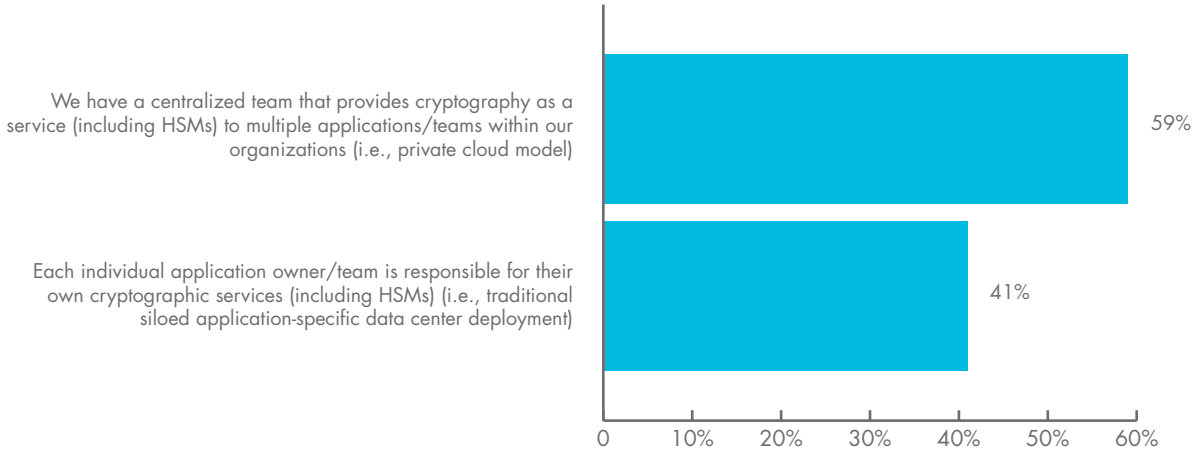
Figure 23 shows a five-year trend in the importance of HSMs for encryption or key management, which has steadily increased over time.

Figure 23. Perceived Importance of HSMs as part of encryption or key management over five years
Important & Very important response (Country samples are consolidated)



What best describes an organization's use of HSMs? As shown in Figure 24, 59 percent of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model). Forty-one percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional, siloed application-specific data center deployment approach.

Figure 24. Which statement best describes how your organization uses HSMs?

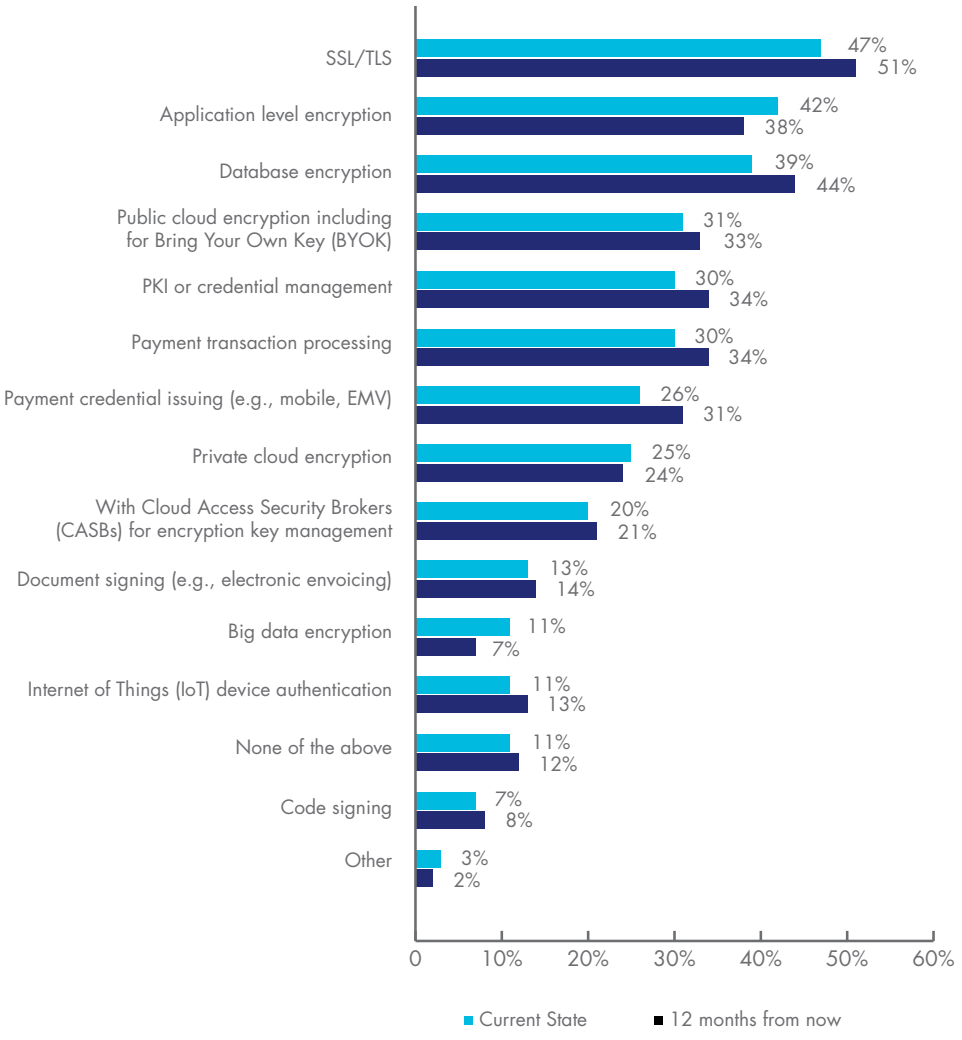


What are the primary purposes or uses for HSMs? Figure 25 summarizes the primary purposes or use cases for deploying HSMs. As can be seen, the two top choices are SSL/TLS and application-level encryption, followed by database encryption. This chart shows that the majority of these use cases are planned to grow in the next 12 months.

The most significant increases predicted for the next 12 months, according to respondents, are database encryption, SSL/TLS, PKI, payment transaction processing, and payment credential issuing. It is significant to note that HSM use for SSL/TLS will soon be in place in 50 percent of the organizations represented in this study.

Figure 25. How HSMs are deployed or planned to be deployed in the next 12 months

Country samples are consolidated (More than one choice permitted)



Budget allocations

The percentages below are calculated from the responses to survey questions about resource allocations to IT security, data protection, encryption, and key management. These calculated values are estimates of the current state and we do not make any predictions about the future state of budget funding or spending.

Figure 26 reports the average percentage of IT security spending relative to total IT spending over the last 12 years. As shown, the trend appears to be upward sloping, which suggests the proportion of IT spending dedicated to security activities including encryption is increasing over time.

Figure 26. Trend in the percent of IT security spending relative to the total IT budget
Country samples are consolidated

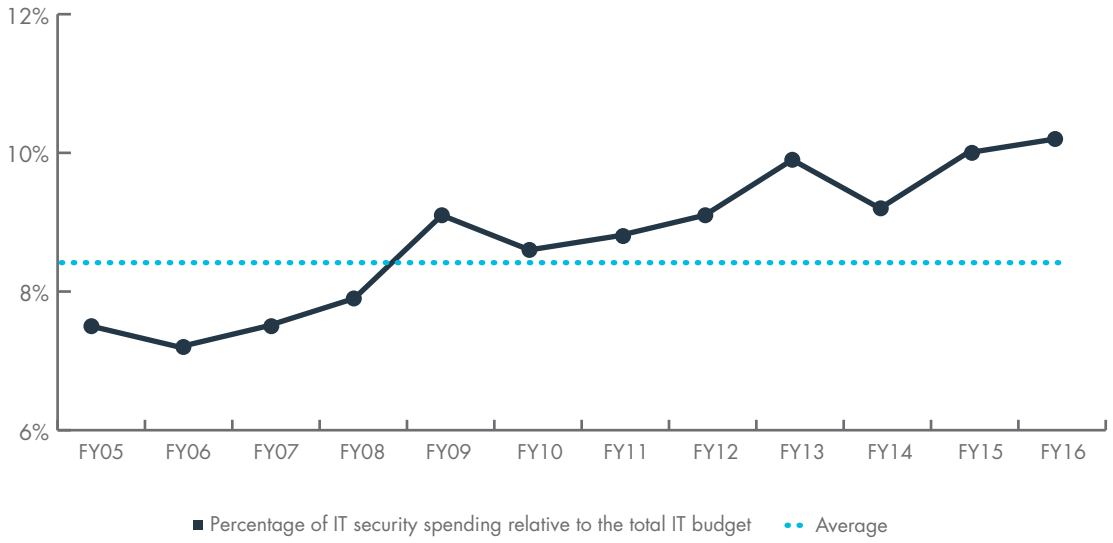
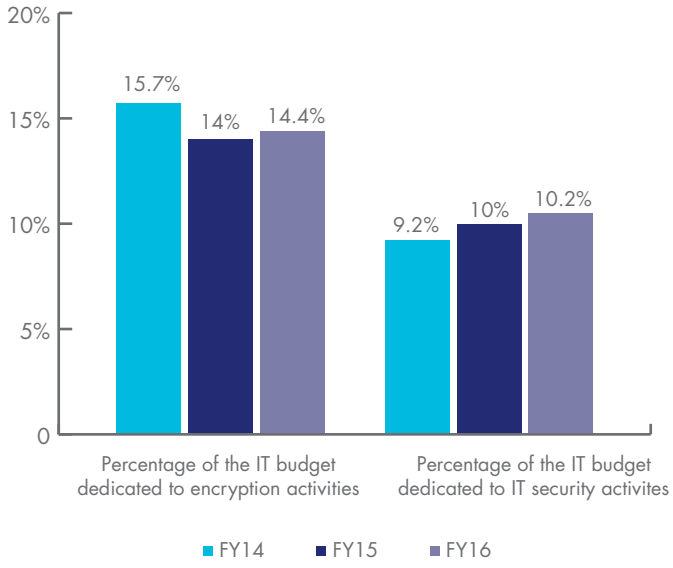


Figure 27 reports the percentage of data protection spending relative to the total IT security budget over 3 years. This trend appears to be slightly upward sloping, which suggests data protection spending as a proportion of total IT security is on the rise.

Figure 27. Trend in the percent of IT security spending dedicated to encryption and security activities
Country samples are consolidated



Cloud encryption

According to Figure 28, 53 percent of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking. Another 24 percent of respondents expect to do so in the next one to two years. These findings indicate the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

According to Figure 29, with respect to the transfer of sensitive or confidential data to the cloud, India, Mexico and the U.S. – a mix of both developing and mature countries from an encryption adoption perspective – have higher rates than other countries. Germany and France have the lowest transfer rate.

Figure 28. Do you currently transfer sensitive or confidential data to the cloud? Country samples are consolidated

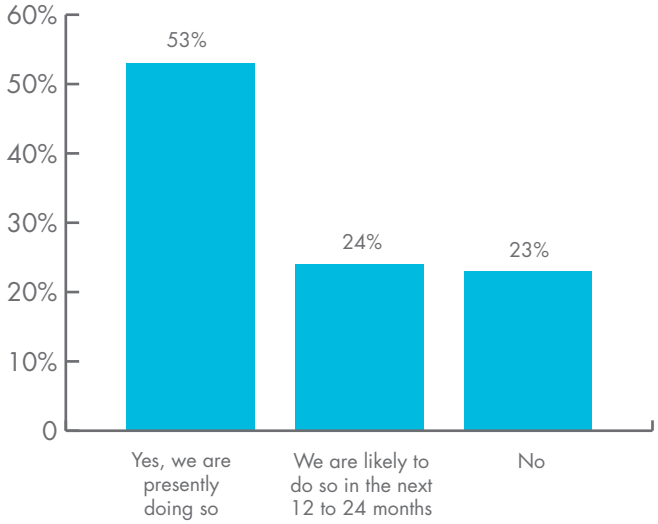
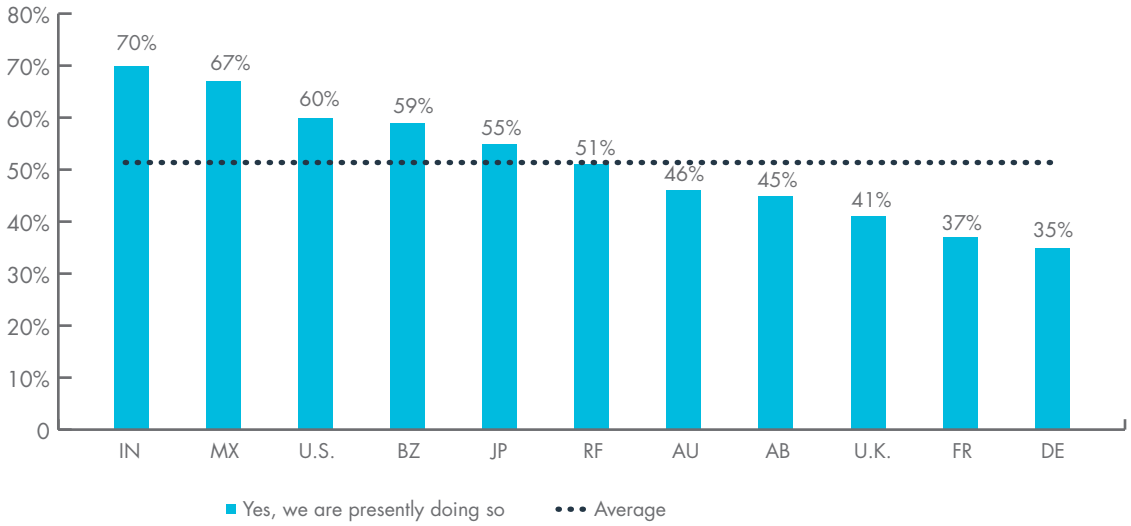
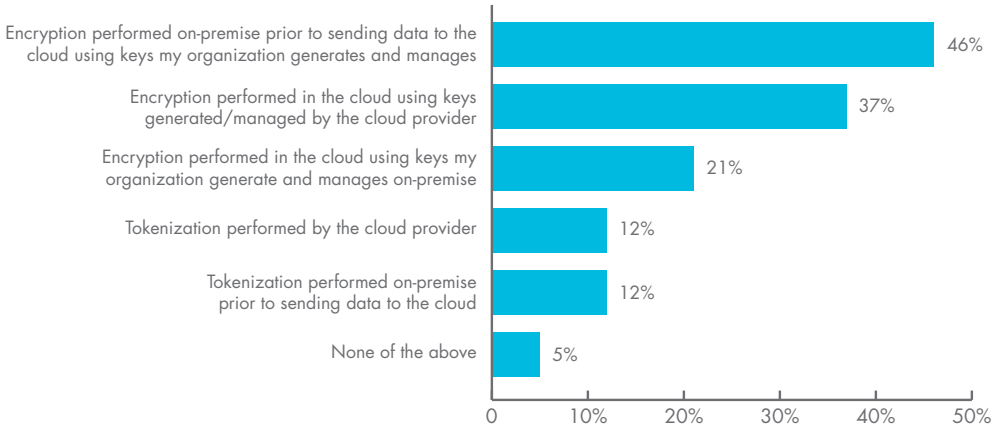


Figure 29. Organizations that transfer sensitive or confidential data to the cloud by country



How do organizations protect data at rest in the cloud? As shown in Figure 30, 46 percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 37 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys, and 21 percent of respondents are using some form of Bring Your Own Key (BYOK) approach.

Figure 30. How does your organization protect data at rest in the cloud?
Country samples are consolidated (More than one choice permitted)



APPENDIX 1. METHODS & LIMITATIONS

Table 1 reports the sample response for 11 separate country samples. The sample response for this study was conducted over a 49-day period ending in January 2017. Our consolidated sampling frame of practitioners in all countries consisted of 138,530 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 5,397 returns of which 595 were rejected for reliability issues. Our final consolidated sample was 4,802, thus resulting in an overall 3.5% response rate.

The first encryption trends study was conducted in the U.S. in 2005. Since then we have expanded the scope of the research to include 11 separate country samples. Trend analysis was performed on combined country samples. As noted before, we added the Arabian sample (AB) (composed of Saudi Arabia and United Arab Emirates) for the first time to last year's study.

The respondents' average (mean) experience in IT, IT security or related fields is 8.6 years. Approximately 26 percent of respondents are female and 74 percent male.[6]

Table 1. Survey response in 11 countries

Legend	Survey response	Sampling frame	Final sample	Response rate
AB	Arabian Cluster	9,146	316	3.5%
AU	Australia	8,277	331	4.0%
BZ	Brazil	12,830	463	3.6%
DE	Germany	14,079	531	3.8%
FR	France	12,756	345	2.7%
IN	India	16,093	548	3.4%
JP	Japan	13,667	450	3.3%
MX	Mexico	11,482	451	3.9%
RF	Russian Federation	6,400	206	3.2%
UK	United Kingdom	12,901	460	3.6%
US	United States	20,899	701	3.4%

[6]This skewed response showing a much lower frequency of female respondents in our study is consistent with earlier studies – all showing that males outnumber females in the IT and IT security professions within the 11 countries sampled.

Table 2 summarizes our survey samples for 11 countries over an 11-year period.

Table 2. Sample history over 11 years

Legend	FY16	FY15	FY14	FY13	FY12	FY11	FY10	FY09	FY08	FY07	FY06
AB	316	368	0	0	0	0	0	0	0	0	0
AU	331	334	359	414	938	471	477	482	405	0	0
BZ	463	460	472	530	637	525	0	0	0	0	0
DE	531	563	564	602	499	526	465	490	453	449	0
FR	345	344	375	478	584	511	419	414	0	0	0
IN	548	578	532	0	0	0	0	0	0	0	0
JP	450	487	476	521	466	544	0	0	0	0	0
MX	451	429	445	0	0	0	0	0	0	0	0
RF	206	201	193	201	0	0	0	0	0	0	0
UK	460	487	509	637	550	651	622	615	638	541	489
US	701	758	789	892	531	912	964	997	975	768	918
Total	4,802	5,009	4,714	4,275	4,205	4,140	2,947	2,998	2,471	1,758	1,407

Figure 31 summarizes the approximate position levels of respondents in our study. As can be seen, the majority of respondents are at or above the supervisory level.

Figure 32 identifies the organizational location of respondents in our study. The majority of respondents (59%) are located within IT operations, followed by security at 18 percent of respondents.

Figure 31. Distribution of respondents according to position level (Country samples are consolidated)

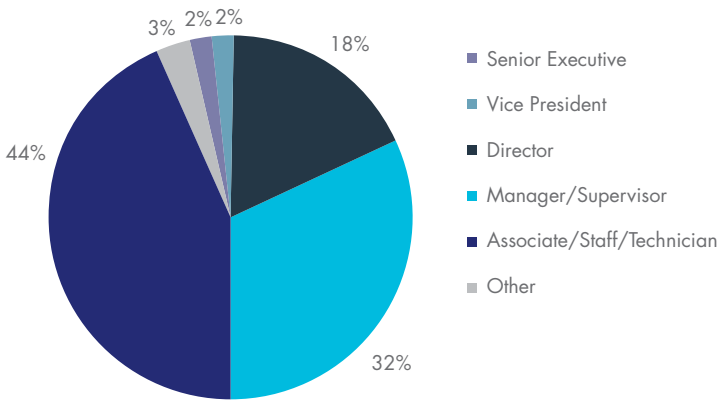


Figure 32. Distribution of respondents according to organizational location (Country samples are consolidated)

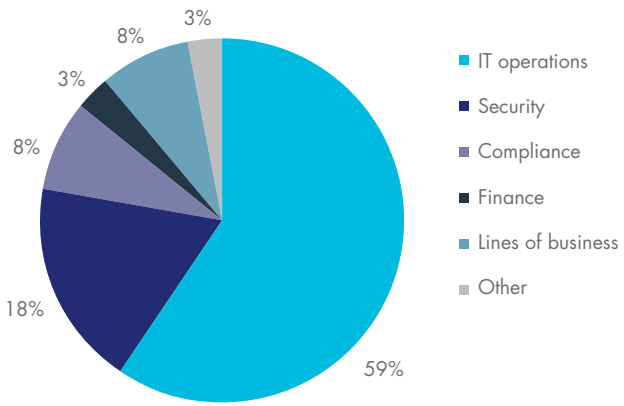
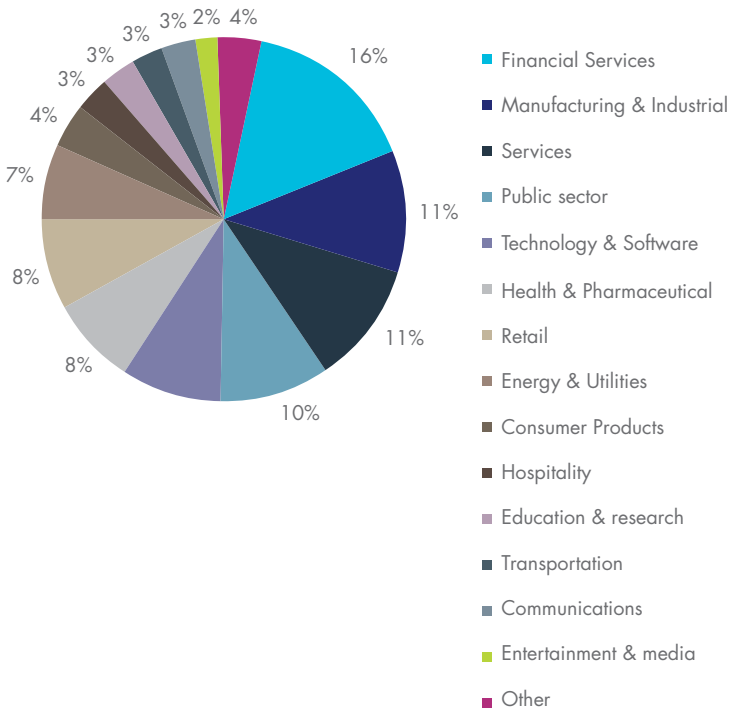


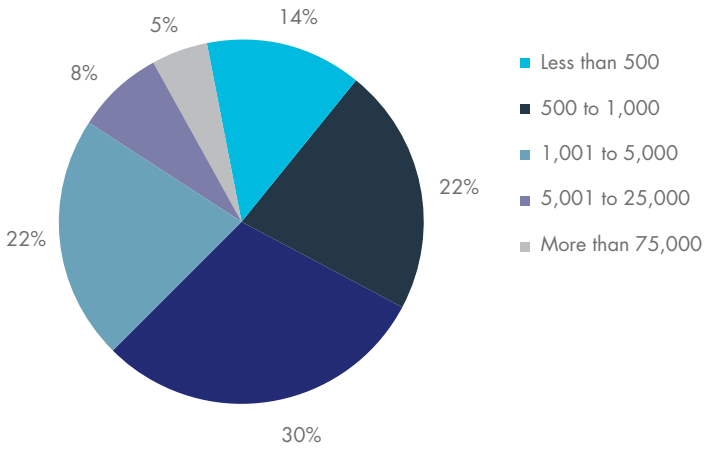
Figure 33 reports the respondents' organizations primary industry segments. As shown, 16 percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Eleven percent are located in manufacturing companies and 11 percent are in services organizations. Another 10 percent are located in public sector, including central and local government.

Figure 33. Distribution of respondents according to primary industry classification (Country samples are consolidated)



According to Figure 34, the majority of respondents (65 percent) are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 34. Distribution of respondents according to organizational headcount (Country samples are consolidated)



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 11 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 the sample of 11 countries selected.

- **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.

APPENDIX 2. SURVEY DATA TABLES

The following tables provide the consolidated results for 11 country samples.

Survey response	Consolidated
Sampling frame	138,530
Total returns	5,397
Rejected or screened surveys	595
Final sample	4,802
Response rate	3.5%
Sample weights	100%

Part 1. Encryption Posture

Q1. Please select one statement that best describes your organization's approach to encryption implementation across the enterprise.	Consolidated
We have an overall encryption plan or strategy that is applied consistently across the entire enterprise	41%
We have a limited encryption plan or strategy that is applied to certain applications and data types	44%
We don't have an encryption plan or strategy	14%
Total	100%

Q2. Following are areas where encryption technologies can be deployed. Please check those areas where encryption is extensively deployed, partially deployed or not as yet deployed by your organization.

Q2a-1 Backup and archives	Consolidated
Extensively deployed	51%
Partially deployed	24%
Not deployed	25%
Total	100%

Q2b-1. Big data repositories	Consolidated
Extensively deployed	30%
Partially deployed	23%
Not deployed	48%
Total	100%

Q2c-1 Cloud gateway	Consolidated
Extensively deployed	40%
Partially deployed	29%
Not deployed	30%
Total	100%

Q2d-1. Data center storage	Consolidated
Extensively deployed	43%
Partially deployed	37%
Not deployed	20%
Total	100%

Q2e-1. Databases	Consolidated
Extensively deployed	64%
Partially deployed	25%
Not deployed	11%
Total	100%

Q2f-1 Docker containers	Consolidated
Extensively deployed	18%
Partially deployed	27%
Not deployed	55%
Total	100%

Q2g-1 Email	Consolidated
Extensively deployed	36%
Partially deployed	37%
Not deployed	27%
Total	100%

Q2h-1 Public cloud services	Consolidated
Extensively deployed	28%
Partially deployed	27%
Not deployed	44%
Total	100%

Q2i-1 File systems	Consolidated
Extensively deployed	34%
Partially deployed	29%
Not deployed	37%
Total	100%

Q2j-1 Internet communications (e.g., SSL)	Consolidated
Extensively deployed	60%
Partially deployed	25%
Not deployed	15%
Total	100%

Q2k-1 Internal networks (e.g., VPN/LPN)	Consolidated
Extensively deployed	45%
Partially deployed	34%
Not deployed	21%
Total	100%

Q2l-1 Laptop hard drives	Consolidated
Extensively deployed	59%
Partially deployed	20%
Not deployed	22%
Total	100%

Q2m-1 Private cloud infrastructure	Consolidated
Extensively deployed	29%
Partially deployed	30%
Not deployed	41%
Total	100%

Q3. Who is most influential in directing your organization's encryption strategy? Please select one best choice.	Consolidated
IT operations	29%
Security	16%
Compliance	2%
Lines of business (LOB) or general management	30%
No single function has responsibility	23%
Total	100%

Q4. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top three reasons.	Consolidated
To protect enterprise intellectual property	51%
To protect customer personal information	49%
To limit liability from breaches or inadvertent disclosure	37%
To avoid public disclosure after a data breach occurs	10%
To protect information against specific, identified threats	49%
To comply with internal policies	19%
To comply with external privacy or data security regulations and requirement	55%
To reduce the scope of compliance audits	30%
Total	300%

Q5. What are the biggest challenges in planning and executing a data encryption strategy? Please select the top two reasons.	Consolidated
Discovering where sensitive data resides in the organization	59%
Classifying which data to encrypt	36%
Determining which encryption technologies are most effective	12%
Initially deploying the encryption technology	47%
Ongoing management of encryption and keys	31%
Training users to use encryption appropriately	16%
Total	200%

Q6. How important are the following features associated with encryption solutions that may be used by your organization? Very important and important response combined.	Consolidated
Enforcement of policy	71%
Management of keys	68%
Support for multiple applications or environments	55%
Separation of duties and role-based controls	54%
System scalability	66%
Tamper resistance by dedicated hardware (e.g., HSM)	55%
Integration with other security tools (e.g., SIEM and ID management)	64%
Support for regional segregation (e.g., data residency)	43%
System performance and Latency	74%
Support for emerging algorithms (e.g., ECC)	65%
Support for cloud and on-premise deployment	69%
Formal product security certifications (e.g., FIPS 140)	56%

Q7. What types of data does your organization encrypt? Please select all that apply.	Consolidated
Customer information	40%
Non-financial business information	32%
Intellectual property	47%
Financial records	49%
Employee/HR data	61%
Payment related data	56%
Healthcare information	19%

Q8. What are the main threats that might result in the exposure of sensitive or confidential data? Please select the top two choices.	Consolidated
Hackers	30%
Malicious insiders	24%
System or process malfunction	29%
Employee mistakes	54%
Temporary or contract workers	22%
Third party service providers	19%
Lawful data request (e.g. by police)	12%
Government eavesdropping	18%
Total	209%

Part 2. Key Management

Q9. Please rate the overall "pain" associated with managing keys or certificates within your organization, where 1 = minimal impact to 10 = severe impact?	Consolidated
1 or 2	8%
3 or 4	13%
5 or 6	19%
7 or 8	23%
9 or 10	36%
Total	100%

Q10. What makes the management of keys so painful? Please select the top three reasons.	Consolidated
No clear ownership	61%
Insufficient resources (time/money)	34%
Lack of skilled personnel	56%
No clear understanding of requirements	22%
Key management tools are inadequate	48%
Systems are isolated and fragmented	53%
Technology and standards are immature	14%
Manual processes are prone to errors and unreliable	12%
Total	300%

Q11. Following are a wide variety of keys that may be managed by your organization. Please rate the overall "pain" associated with managing each type of key. Very painful and painful response combined.	Consolidated
Encryption keys for backups and storage	22%
Encryption keys for archived data	34%
Keys associated with SSL/TLS	47%
SSH keys	62%
End user encryption keys (e.g., email, full disk encryption)	38%
Signing keys (e.g., code signing, digital signatures)	55%
Payments-related keys (e.g., ATM, POS, etc.)	36%
Keys to embed into devices (e.g. at the time of manufacture in device production environments, or for IoT devices you use)	16%
Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys	63%

Q12a. What key management systems does your organization presently use?	Consolidated
Formal key management policy (KMP)	51%
Formal key management infrastructure (KMI)	37%
Manual process (e.g., spreadsheet, paper-based)	51%
Central key management system/server	33%
Hardware security modules	28%
Removable media (e.g., thumb drive, CDROM)	32%
Software-based key stores and wallets	18%
Smart cards	25%
Total	276%

Q12b. What key management systems does your organization presently use?	Consolidated
Formal key management policy (KMP)	46%
Formal key management infrastructure (KMI)	61%
Manual process (e.g., spreadsheet, paper-based)	47%
Central key management system/server	65%
Hardware security modules	69%
Removable media (e.g., thumb drive, CDROM)	65%
Software-based key stores and wallets	80%
Smart cards	72%
Total	507%

Part 3. Hardware Security Modules

Q13. What best describes your level of knowledge about HSMs?	Consolidated
Very knowledgeable	30%
Knowledgeable	29%
Somewhat knowledgeable	16%
No knowledge (skip to Q17a)	23%
Total	100%

Q14a. Does your organization use HSMs?	Consolidated
Yes	38%
No (skip to Q17a)	62%
Total	100%

Q14b. For what purpose does your organization presently deploy or plan to use HSMs? Please select all that apply.

Q14b-1. HSMs used today	Consolidated
Application level encryption	42%
Database encryption	39%
Big data encryption	11%
Public cloud encryption including for Bring Your Own Key (BYOK)	31%
Private cloud encryption	25%
SSL/TLS	47%
PKI or credential management	30%
Internet of Things (IoT) device authentication	11%
Document signing (e.g. electronic invoicing)	13%
Code signing	7%
Payment transaction processing	30%
Payment credential issusing (e.g., mobile, EMV)	26%
With Cloud Access Security Brokers (CASBs) for encryption key management	20%
None of the above	11%
Other	3%
Total	345%

Q14b-2. HSMs planned to be deployed in the next 12 months	Consolidated
Application level encryption	38%
Database encryption	44%
Big data encryption	7%
Public cloud encryption including for Bring Your Own Key (BYOK)	33%
Private cloud encryption	24%
SSL/TLS	51%
PKI or credential management	34%
Internet of Things (IoT) device authentication	13%
Document signing (e.g. electronic invoicing)	14%
Code signing	8%
Payment transaction processing	34%
Payment credential issusing (e.g., mobile, EMV)	31%
With Cloud Access Security Brokers (CASBs) for encryption key management	21%
None of the above	12%
Other	2%
Total	365%

Q14c-1. If you use HSMs in conjunction with public cloud based applications, what models do you use today? Please select all that apply.	Consolidated
Rent/use HSMs from public cloud provider, hosted in the cloud	36%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	48%
Own and operate HSMs for the purpose of generating and managing BYOK (Bring Your Own Key) keys to send to the cloud for use by the cloud provider	17%
Own and operate HSMs that integrate with a Cloud Access Security Broker to manage keys and cryptographic operations (e.g., encrypting data on the way to the cloud, managing keys for cloud applications)	12%
None of the above	1%
Total	113%

Q14c-2. If you use HSMs in conjunction with public cloud based applications, what models do you plan to use in the next 12 months Please select all that apply.	Consolidated
Rent/use HSMs from public cloud provider, hosted in the cloud	41%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	55%
Own and operate HSMs for the purpose of generating and managing BYOK (Bring Your Own Key) keys to send to the cloud for use by the cloud provider	24%
Own and operate HSMs that integrate with a Cloud Access Security Broker to manage keys and cryptographic operations (e.g., encrypting data on the way to the cloud, managing keys for cloud applications)	24%
None of the above	1%
Total	144%

Q15. In your opinion, how important are HSMs to your encryption or key management strategy? Very important and important response combined	Consolidated
Q15a. Importance today	55%
Q15b. Importance in the next 12 months	61%

Q16. Which statement best describes how your organization uses HSMs?	Consolidated
We have a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within our organization (i.e. private cloud model).	59%
Each individual application owner/team is responsible for their own cryptographic services (including HSMs) (i.e. traditional siloed, application-specific data center deployment).	41%
Total	100%

Part 4. Budget Questions

Q17a. Are you responsible for managing all or part of your organization's IT budget this year?	Consolidated
Yes	55%
No (skip to Q18)	45%
Total	100%

	Consolidated
Q17b. Approximately, what percentage of the 2017 IT budget will go to IT security activities?	10.2%

	Consolidated
Q17c. Approximately, what percentage of the 2017 IT budget will go to encryption activities?	14.4%

Part 6: Cloud encryption: When responding to the following questions, please assume they refer only to public cloud services.

Q35a. Does your organization currently use cloud computing services for any class of data or application – both sensitive and non-sensitive?	Consolidated
Yes, we are presently doing so	60%
No, but we are likely to do so in the next 12 to 24 months	21%
No (Go to Part 7 if you do not use cloud services for any class of data or application)	20%
Total	100%

Q35b. Do you currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism)?	Consolidated
Yes, we are presently doing so	53%
No, but we are likely to do so in the next 12 to 24 months	24%
No (Go to Part 7 if you do not use or plan to use any cloud services for sensitive or confidential data)	23%
Total	100%

Q35c. In your opinion, who is most responsible for protecting sensitive or confidential data transferred to the cloud?	Consolidated
The cloud provider	45%
The cloud user	21%
Shared responsibility	34%
Total	100%

Q35d. How does your organization protect data at rest in the cloud?	Consolidated
Encryption performed in the cloud using keys generated/managed by the cloud provider	37%
Encryption performed in the cloud using keys my organization generates and manages on-premise	21%
Encryption performed on-premise prior to sending data to the cloud using keys my organization generates and manages	46%
Tokenization performed by the cloud provider	12%
Tokenization performed on-premise prior to sending data to the cloud	12%
None of the above	5%
Total	133%

Q35e. For encryption of data at rest in the cloud, my organization's strategy is to . . .	Consolidated
Only use keys controlled by my organization	39%
Only use keys controlled by the cloud provider	20%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by my organization	22%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by the cloud provider	18%
Total	100%

Q35f. Do you currently encrypt, or plan to encrypt, with any of the following SaaS applications (please check all that apply)?	Consolidated
Microsoft Office 365	54%
Salesforce.com	42%
Box	29%
Concur	7%
Workday	6%
Google Apps	44%
ServiceNow	8%
DocuSign	15%
ZenDesk	13%
Other	4%
Total	222%

Part 7: Role and organizational characteristics

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	2%
Vice President	2%
Director	18%
Manager/Supervisor	32%
Associate/Staff/Technician	44%
Other	3%
Total	100%

D2. Select the functional area that best describes your organizational location.	Consolidated
IT operations	59%
Security	18%
Compliance	8%
Finance	3%
Lines of business (LOB)	8%
Other	3%
Total	100%

D3. What industry best describes your organization's industry focus?	Consolidated
Agriculture & food services	1%
Communications	3%
Consumer products	4%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	7%
Entertainment & media	2%
Financial services	16%
Health & pharmaceutical	8%
Hospitality	3%
Manufacturing & industrial	11%
Public sector	10%
Retail	8%
Services	11%
Technology & software	9%
Transportation	3%
Other	2%
Total	100%

D4. What is the worldwide headcount of your organization?	Consolidated
Less than 500	14%
500 to 1,000	22%
1,001 to 5,000	30%
5,001 to 25,000	22%
25,001 to 75,000	8%
More than 75,000	5%
Total	100%

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.

ABOUT THALES E-SECURITY

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and, with the internet of things (IoT), even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

ABOUT THALES

Thales is a global technology leader for the Aerospace, Transport, Defence and Security markets. With 64,000 employees in 56 countries, Thales reported sales of €14.9 billion in 2016. With over 25,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its exceptional international footprint allows it to work closely with its customer all over the world.

THALES

www.thalesesecurity.com