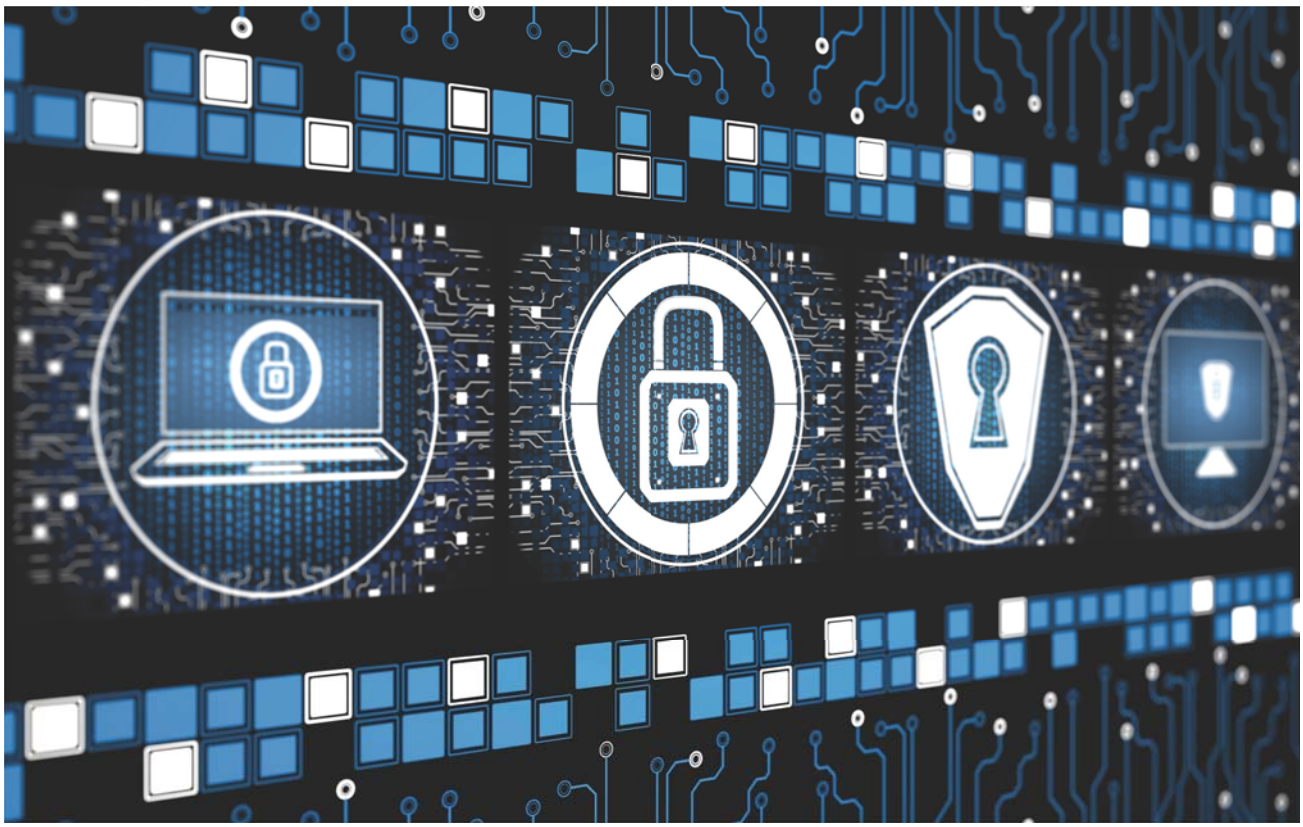
THALES

Ponemon INSTITUTE



2016 Global Encryption Trends Study

Sponsored by Thales e-Security

Independently conducted by Ponemon Institute LLC

Publication Date: February 2016

Ponemon Institute© Research Report

2016 Global Encryption Trends Study

Table of Contents

2016 Global Encryption Trends Study[1]

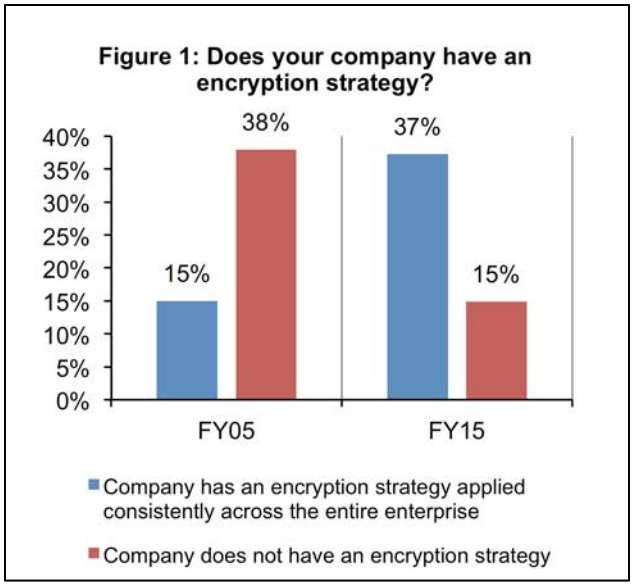
Ponemon Institute, February 2016

Part 1. Executive Summary

Thales is pleased to present the findings of the *2016 Global Encryption Trends Study,* independently conducted by the Ponemon Institute. We surveyed 5,009 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 11 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a US 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 37 percent in FY15, 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.

Overall findings

Enterprise-wide encryption strategies increase. As shown in Figure 1, 37 percent of respondents in this year's study say their organization has an encryption strategy applied consistently across the entire enterprise. Only 15 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.

---

[1]This year's report was completed in February 2016. 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 FY15. The same dating convention is used in prior years.

[2]Country-level results are abbreviated as follows: Germany (DE), Japan (JP), United States (US), United Kingdom (UK), 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 11 years (since 2005).

German organizations are more likely to have a comprehensive encryption strategy. Over 61 percent of German respondents say their organization has a comprehensive encryption strategy. In contrast, only 26 percent of Australian and 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-two percent of respondents say IT operations are most influential, 27 percent say lines of business or general management and 16 percent of respondents say it is the security function. Only two percent of respondents chose compliance.

The 11-year trend shows IT operations have become less influential (from 53 percent in FY05 to 32 percent in FY15). The converse is true for lines of business management, which has become more influential (from 10 percent in FY05 to over 27 percent in FY15). We see three countries – namely, the US, UK and France – choosing their organization's lines of business management as being most influential. The remaining eight countries chose IT operations.

The extensive use of encryption technologies increases but budgets decrease. This year we examined the usage rates for 14 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 FY15. While the extensive use of encryption has steadily increased over 11 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 52 percent of respondents, employee error is the most significant threat to sensitive or confidential data. Thirty percent chose system or process malfunction and 28 percent chose hackers, as their most significant threat. The fact that the top two findings on threats relate to mistakes or errors, as opposed to targeted threats, is notable.

Compliance is the main driver to invest in the extensive use of encryption. Sixty-one percent of respondents see compliance with privacy and data security requirements as the main driver to extensive encryption use within their company. Fifty percent of respondents see protecting enterprise intellectual property as the main driver. The least significant drivers include avoiding data breach disclosures (8 percent of respondents) and compliance with internal policies (15 percent of respondents).

What is the biggest challenge to encryption deployment? Fifty-seven 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, 49 percent of all respondents cite initially deploying encryption technology as a

significant challenge and 35 percent of respondents see classifying what data to encrypt as a significant challenge.

Looking across 14 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. In contrast, encryption for big data repositories (26 percent of respondents), public cloud services (25 percent of respondents) and private cloud infrastructure (27 percent) has lower use rates but has grown from the previous year.

The use of encryption varies among countries. Respondents in Germany, US, UK and Japan have the highest deployment rates. Mexico, Australia and Brazil 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) support for both cloud and on-premise deployment, (2) system performance and latency and (3) integration with other security tools.

IT security spending is increasing. The average percentage of IT security spending relative to total IT spending over 11 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 11 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 11-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 encrypting sensitive and confidential data transferred to the cloud. Fifty-six 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 (63 percent of respondents), Brazil (60 percent of respondents), US (59 percent of respondents) and Germany (58 percent of respondents) have higher use rates than other countries. In contrast, the Russian Federation (48 percent of respondents), Mexico (49 percent of respondents), and both Arabia and France (50 percent of respondents) have the lowest rates.

Forty-four percent of respondents say their organizations protect sensitive or confidential data at rest in the cloud using encryption. Another 17 percent of respondents say data at rest is made unreadable using some other mechanism such as tokenization or data masking. German organizations are most likely to deploy encryption to protect sensitive or confidential data at rest in the cloud. In contrast, Mexican organizations are least likely to use encryption to secure data at rest in the cloud.

Key management and HSMs

Respondents rated the overall "pain" associated with managing keys within their organization. Fifty-three 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 (high rating at 62 percent) and Russia has the lowest pain level (high rating at 43 percent).

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) SSH keys, (2) keys for external services and (3) keys for third-party systems. The least difficult are: (1) embedded device keys, (2) encryption keys for backups and storage and (3) network encryption keys.

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, US and UK 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 has steadily increased over the past four years from 26 percent in FY12 to 34 percent in FY15.

Key management program or activities increase in importance. The overall average importance rating in the current year is 49 percent of respondents, which represents a slight increase from prior years. The pattern of responses suggests organizations in Germany, US and Japan are most likely to attribute high importance to HSMs as part of key management.

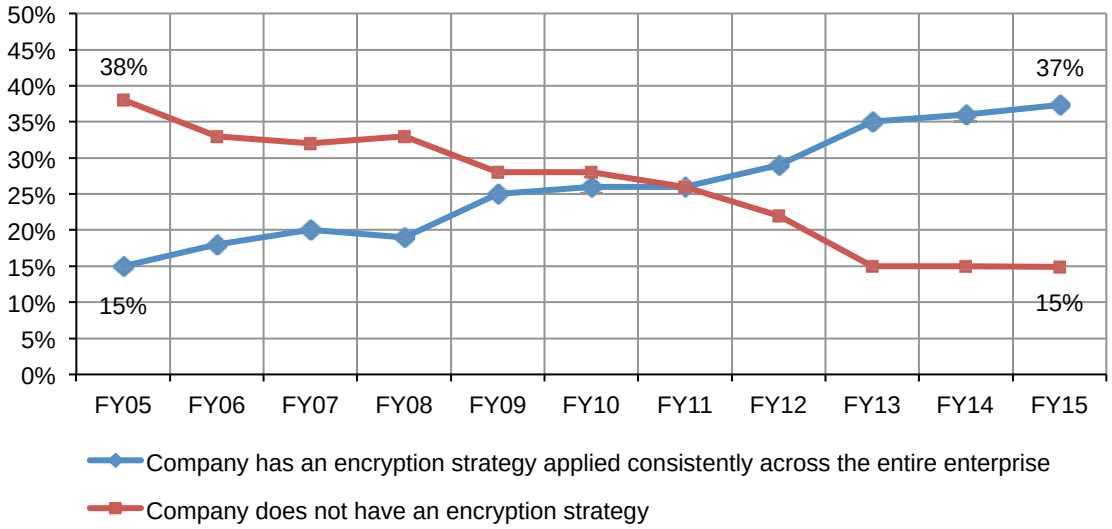
What are the primary purposes for deploying HSMs? According to respondents, the two top choices are SSL/TLS and database encryption. The most significant increases predicted for the next 12 months are: (1) database encryption (30 percent of respondents), (2) application level encryption (28 percent of respondents), (3) payment credential issuing (26 percent of respondents) and (4) both SSL/TLS and public cloud encryption (25 percent of respondents).

Part 2. Key Findings

Strategy and adoption of encryption

Enterprise-wide encryption strategies increase. Since conducting this study 11 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. Figure 2 shows these changes over time.

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 US and Japan. Respondents in Mexico, Australia, Arabia and Brazil report the lowest adoption of an enterprise encryption strategy.

Figure 3. Differences in enterprise encryption strategies by country

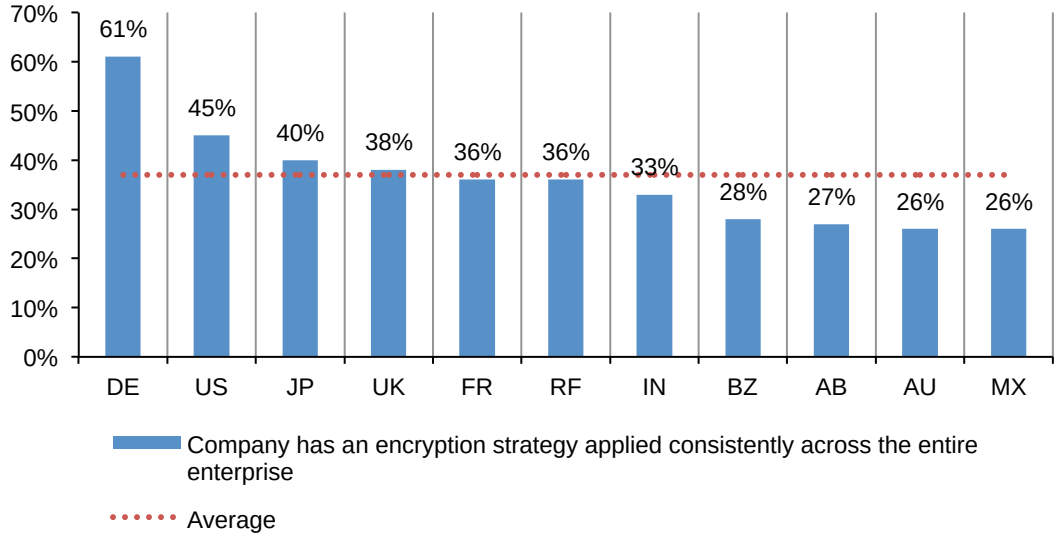


Figure 4 shows that the IT operations function has consistently been most influential in framing the organization's encryption strategy over 11 years. However, that picture is steadily changing with business unit leaders gaining influence over their company's encryption strategy – from 10 percent in FY05 to 27 percent in FY15. In contrast, IT operations decreased significantly from 53 percent in FY05 to 32 percent in FY15.

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

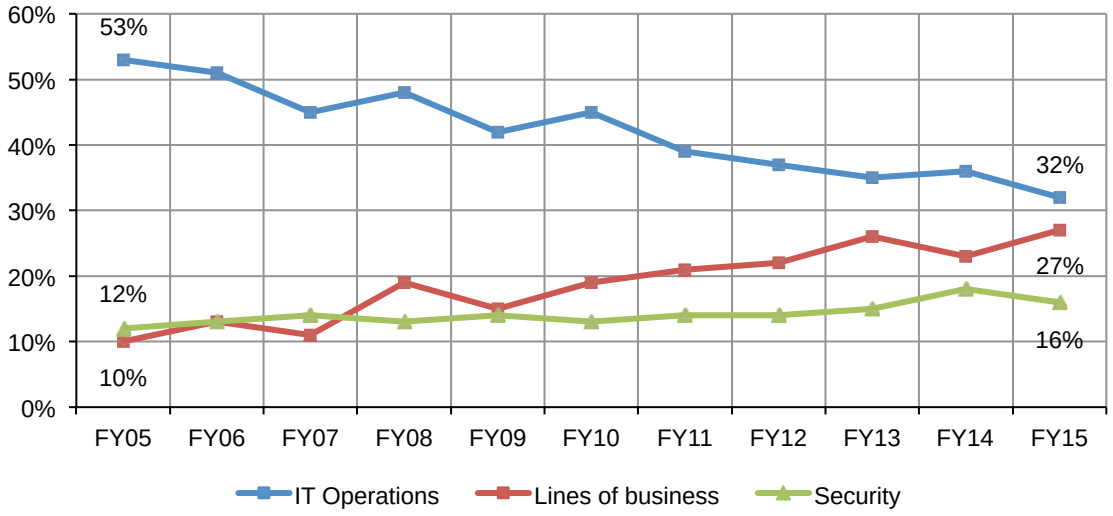
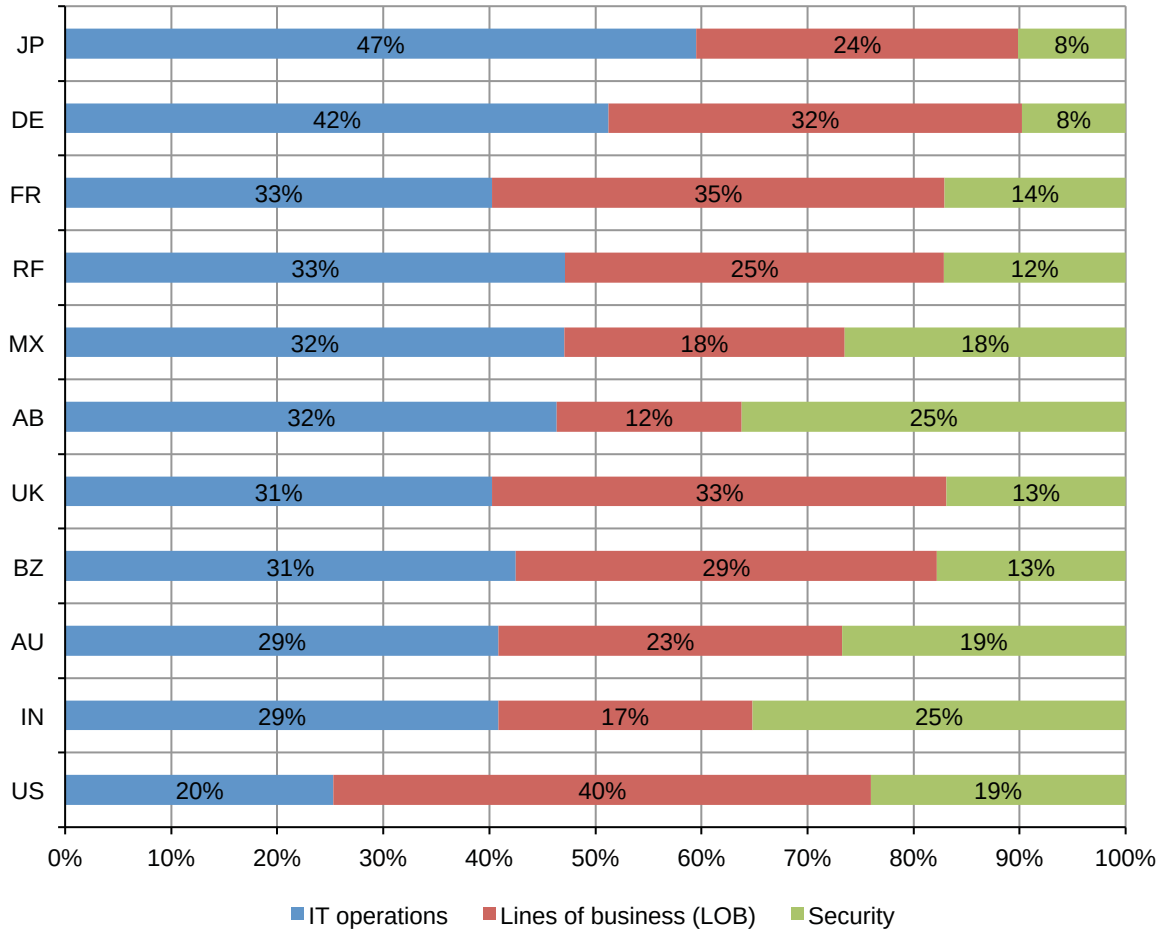


Figure 5 shows the percentage distribution of respondents who rate IT operations, LOB and security as most influential in determining their organization's encryption strategy. This chart shows IT operations as most influential in eight of 11 countries. In contrast, the US, UK and France see business managers as most influential in determining the company's encryption strategy.

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



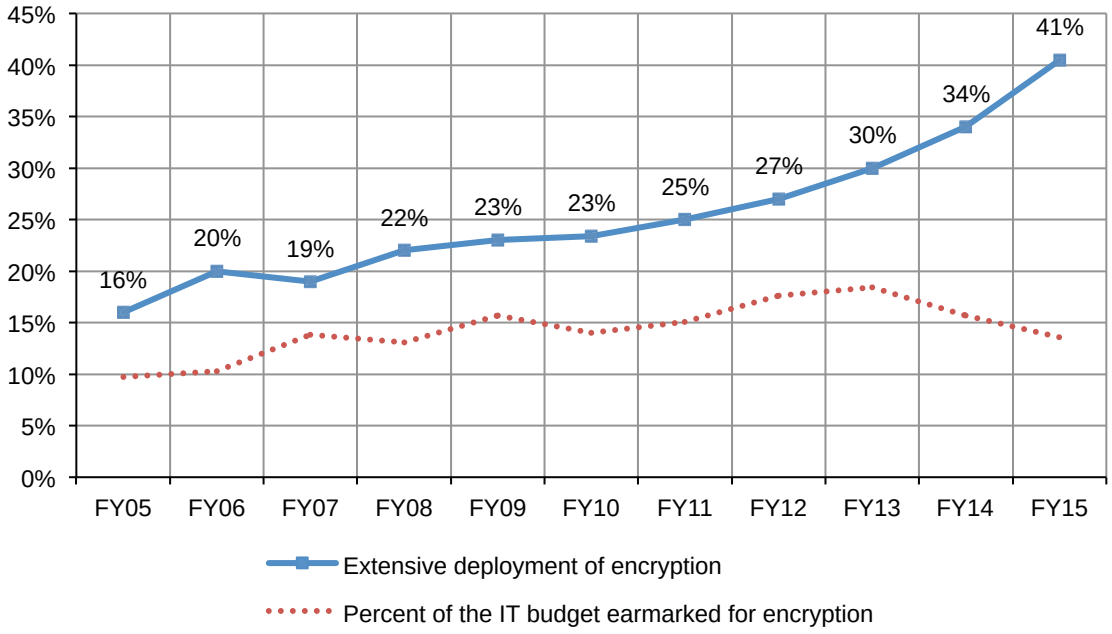
Trends in encryption adoption

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 11 years. This continuous growth in enterprise deployment suggests encryption is important to an organization's security posture. Figure 7 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 FY15. 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.

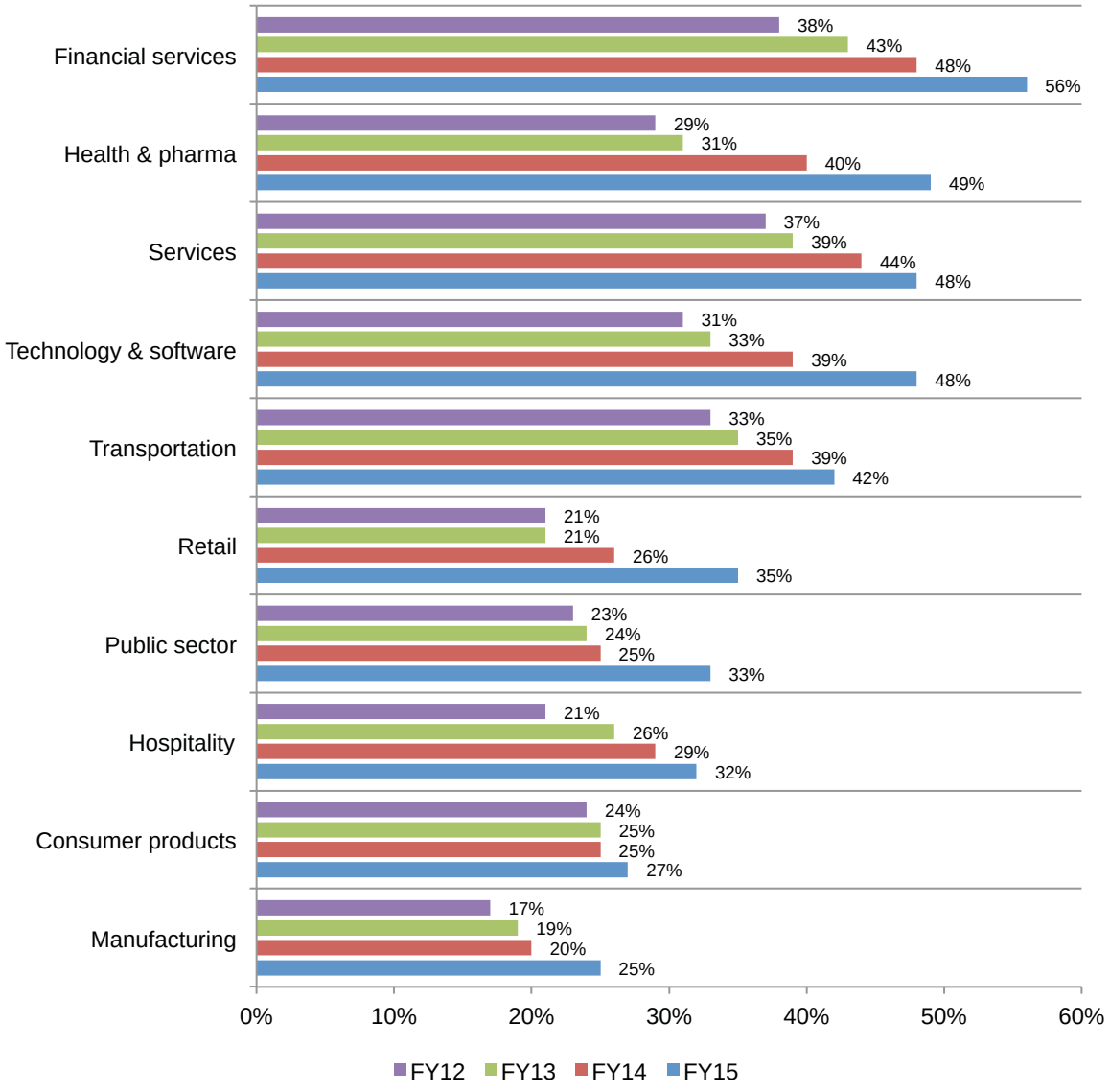
Figure 6. Trend on the extensive use of encryption technologies
Country samples are consolidated



[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.

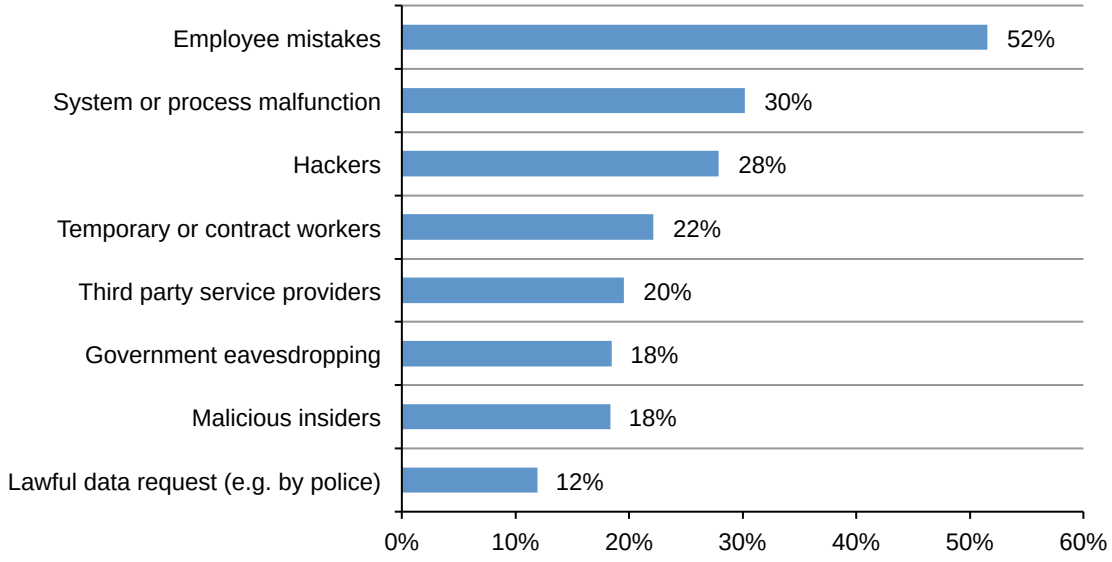
Figure 7. The extensive use of encryption by industry
Country samples are consolidated
Average of 14 encryption categories



Threats, main drivers and priorities

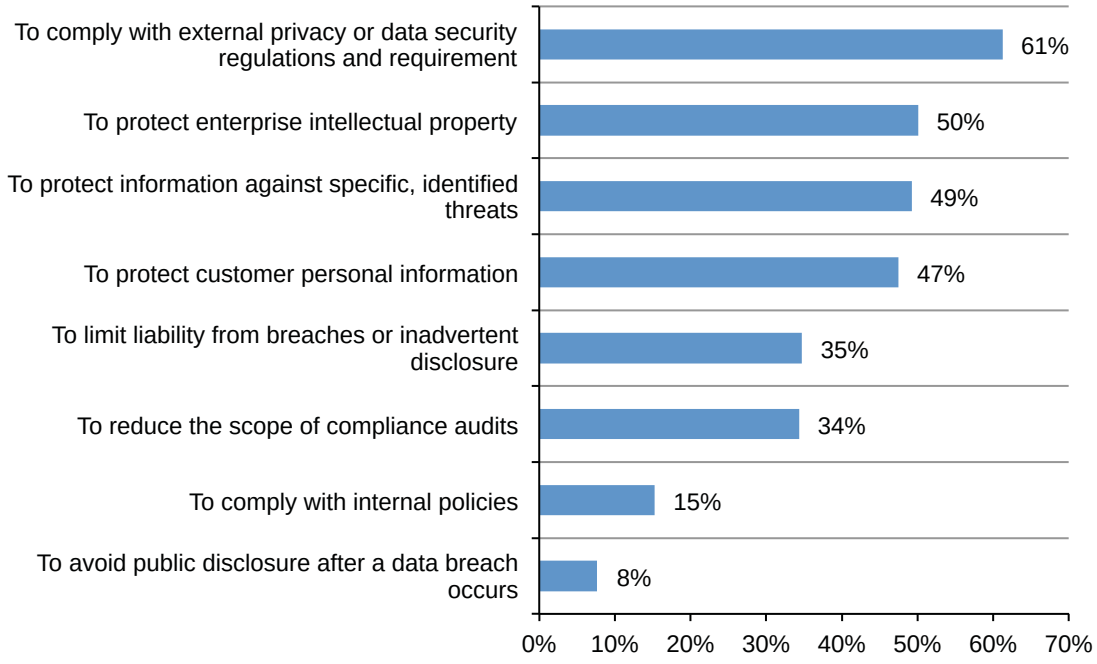
Employee mistakes are the most significant threats to sensitive data. Figure 8 shows that the most significant threats to the exposure of sensitive or confidential data are employee mistakes and system process malfunctions. In contrast, the least significant threats to the exposure of sensitive or confidential data include malicious insiders and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) outweigh concerns over actual attacks by hackers and malicious insiders.

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



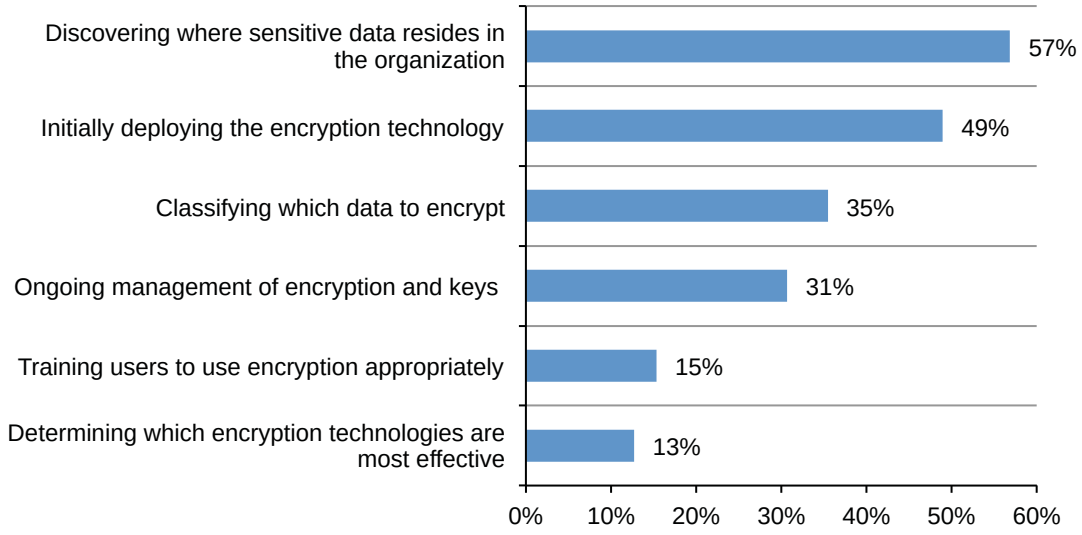
Sixty-one percent of respondents see compliance with privacy and data security requirements as the main driver to using encryption technologies. Eight drivers for deploying encryption are presented in Figure 9. Respondents report compliance with regulations as the top driver, which is consistent with 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
More than one choice 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. Fifty-seven percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 49 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-five 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

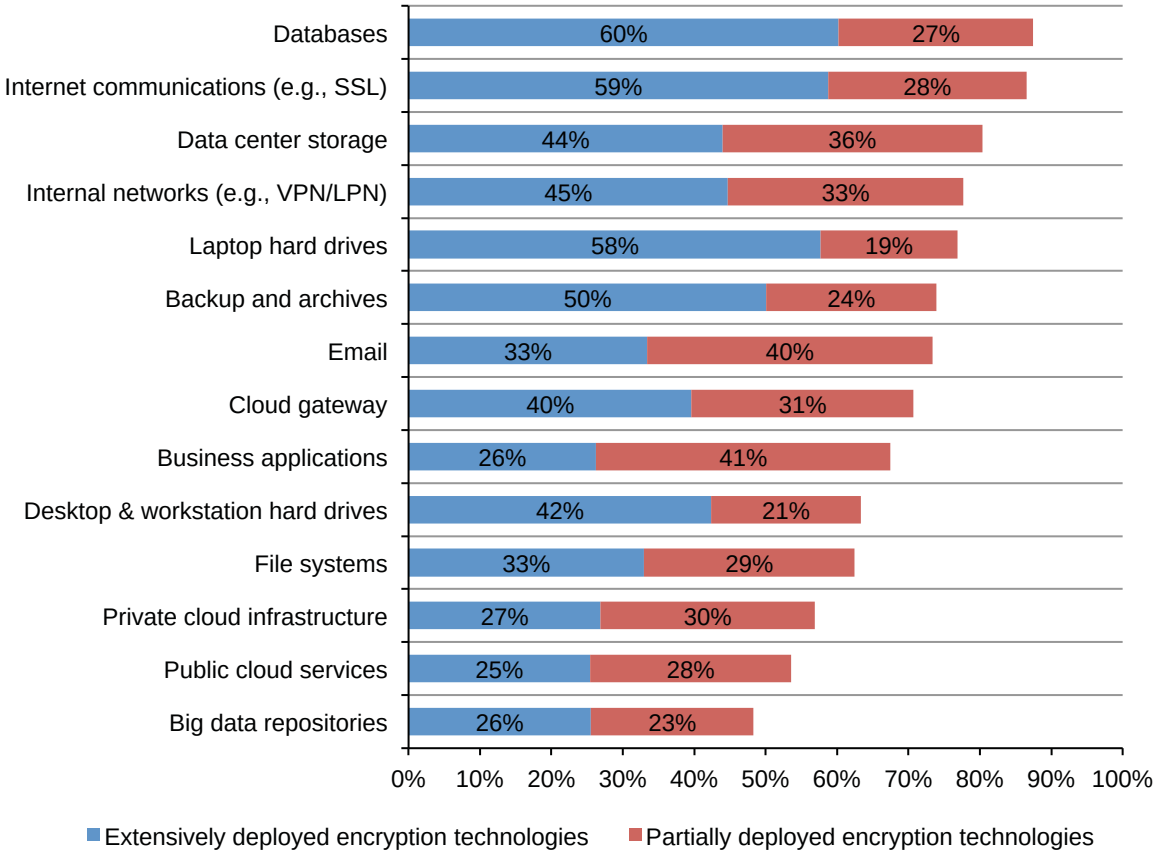


Deployment choices

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 and private cloud infrastructure -- have a lower deployment rate but are all demonstrating year on year growth.

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

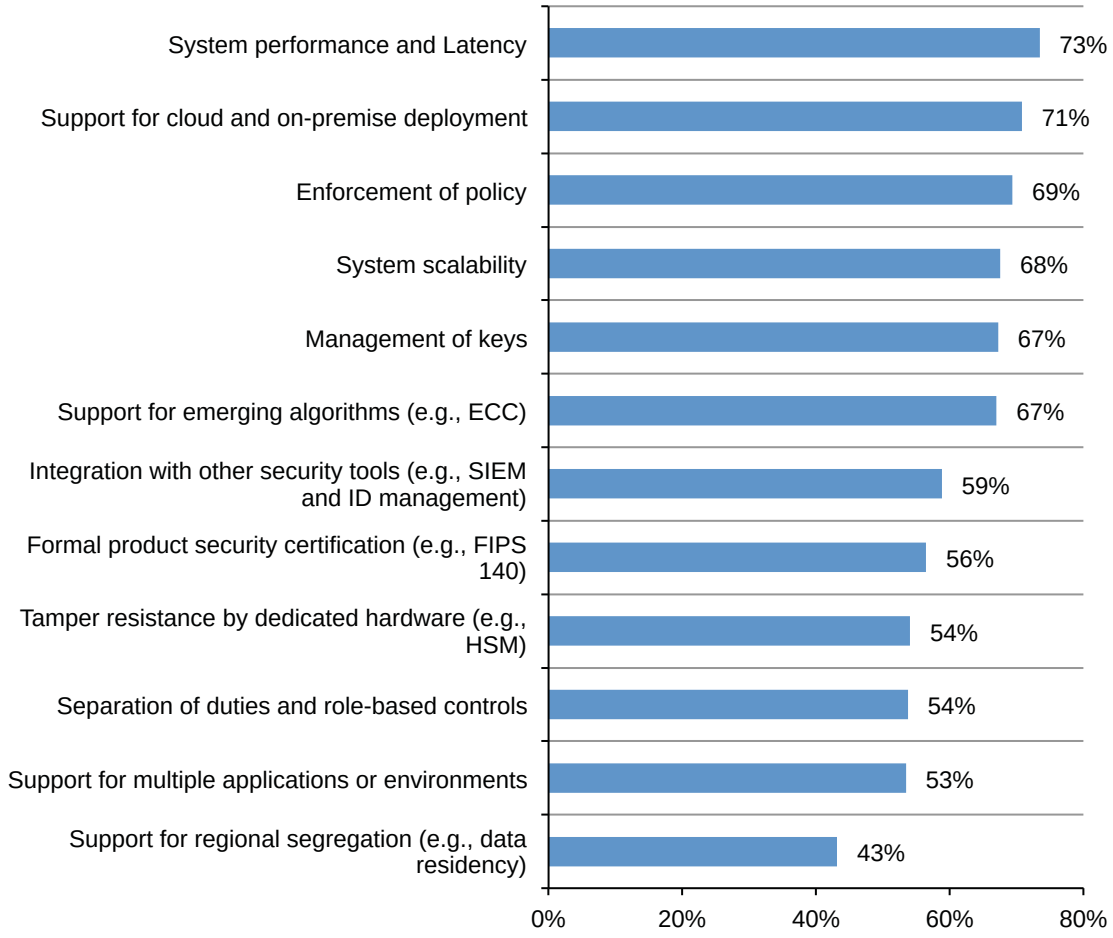


Encryption features considered most important

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.

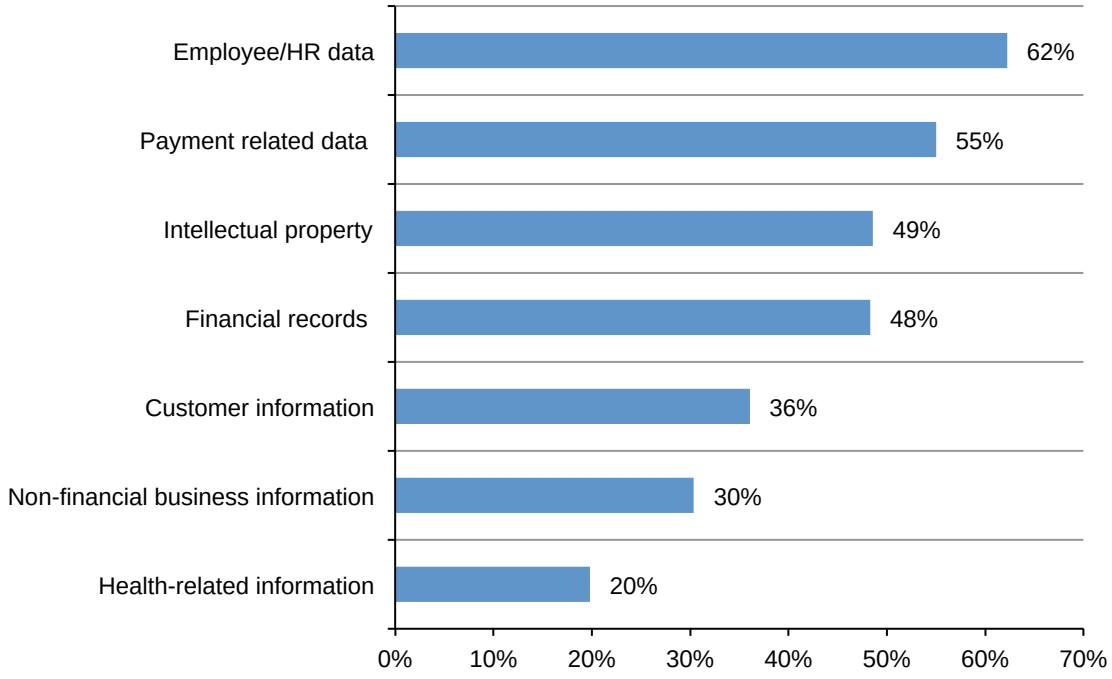
According to consolidated findings, system performance and latency, support for cloud and on-premise deployment and enforcement of policy are the three most important features. The performance finding is not surprising given that SSL/TLS is a top use case and the importance of speed in networking. Support 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 important for cloud 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. The least likely data type is health-related information, which is a surprising result given the sensitivity of health information and recent high profile healthcare data breaches.

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 53 (23+30) percent of respondents in FY15 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 or certificates.
Country samples are consolidated

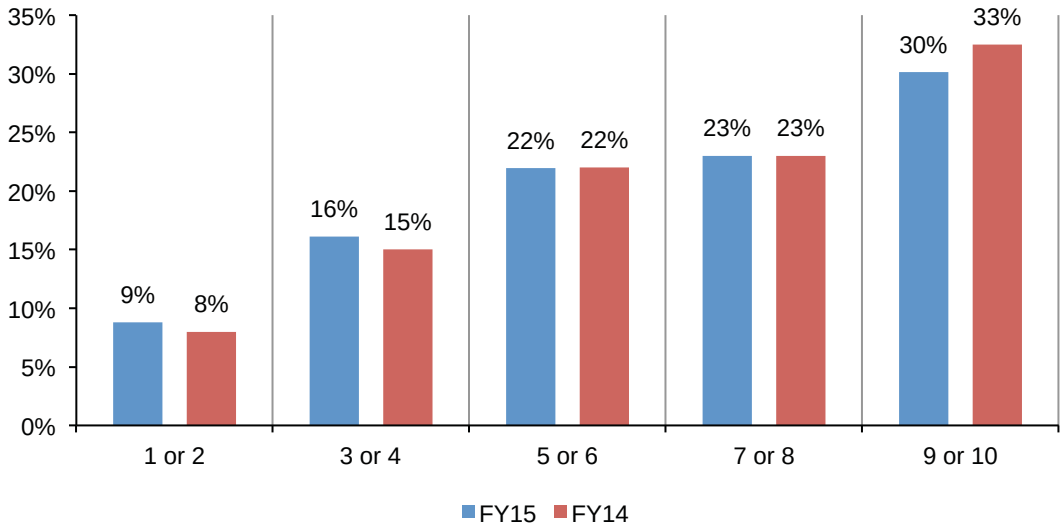
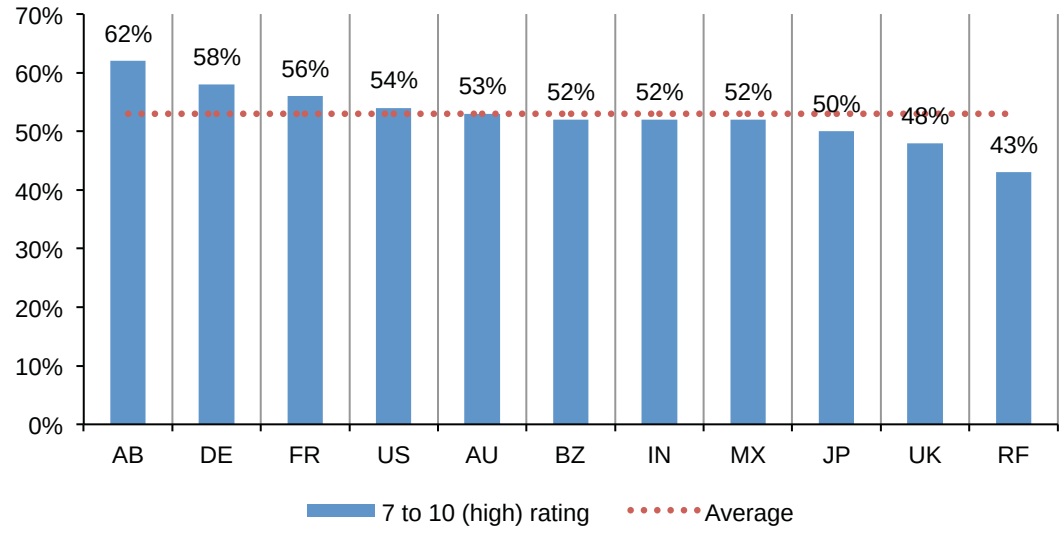


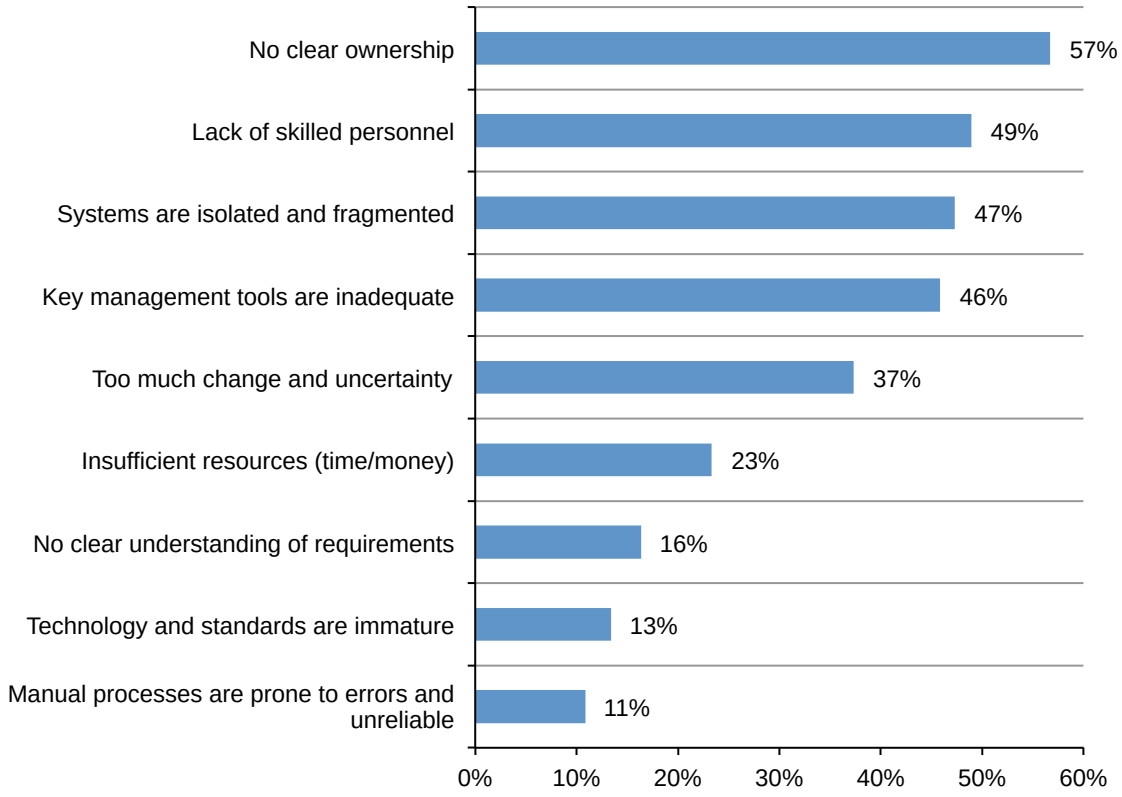
Figure 15 shows the 7+ ratings on a 10-point scale for each country. As can be seen, the average percentage in all country samples is 53 percent, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 62 percent occurs in Arabia. At 43 percent, the lowest pain level occurs in Russia.

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



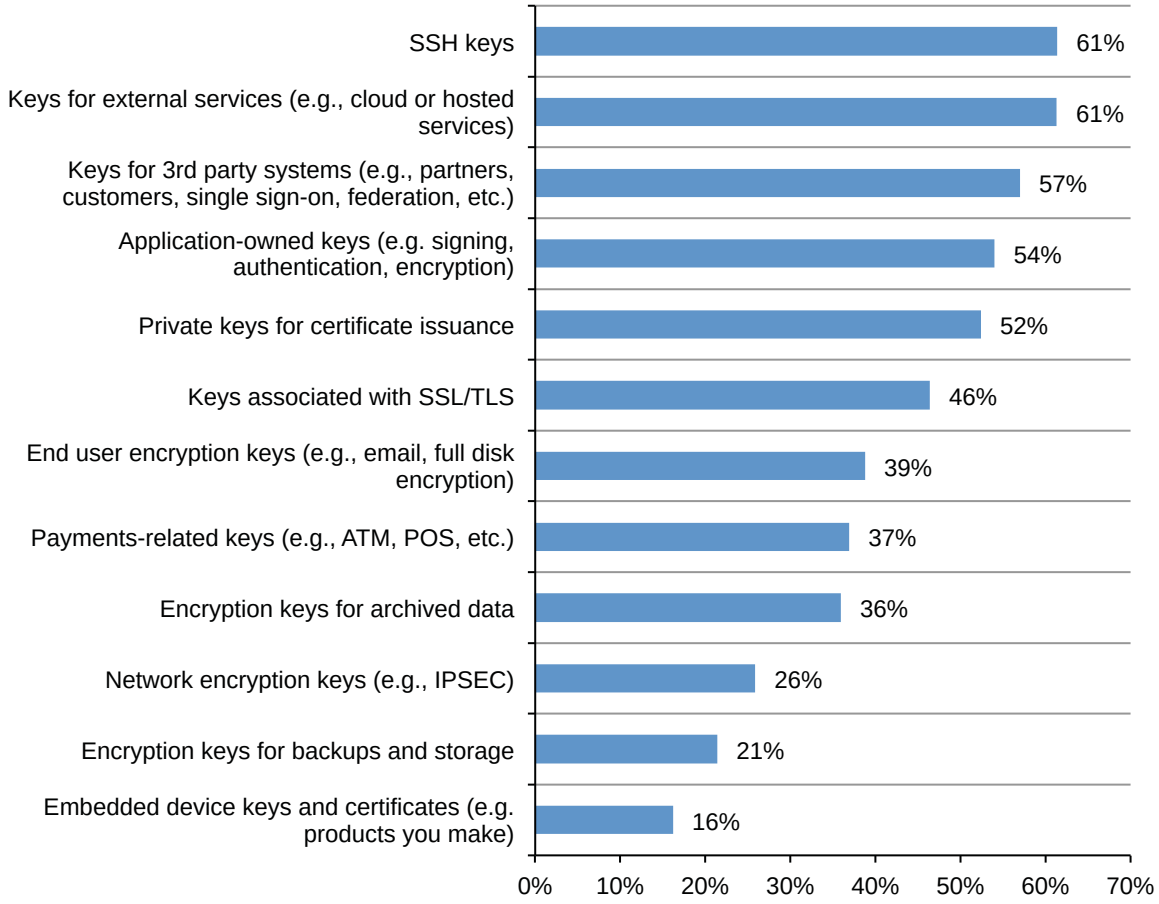
Why is key management painful? Figure 16 shows the reasons why the management of keys is so difficult. The top three reasons are: (1) no clear ownership of the key management function, (2) lack of skilled personnel and (3) isolated or fragmented key management systems.

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



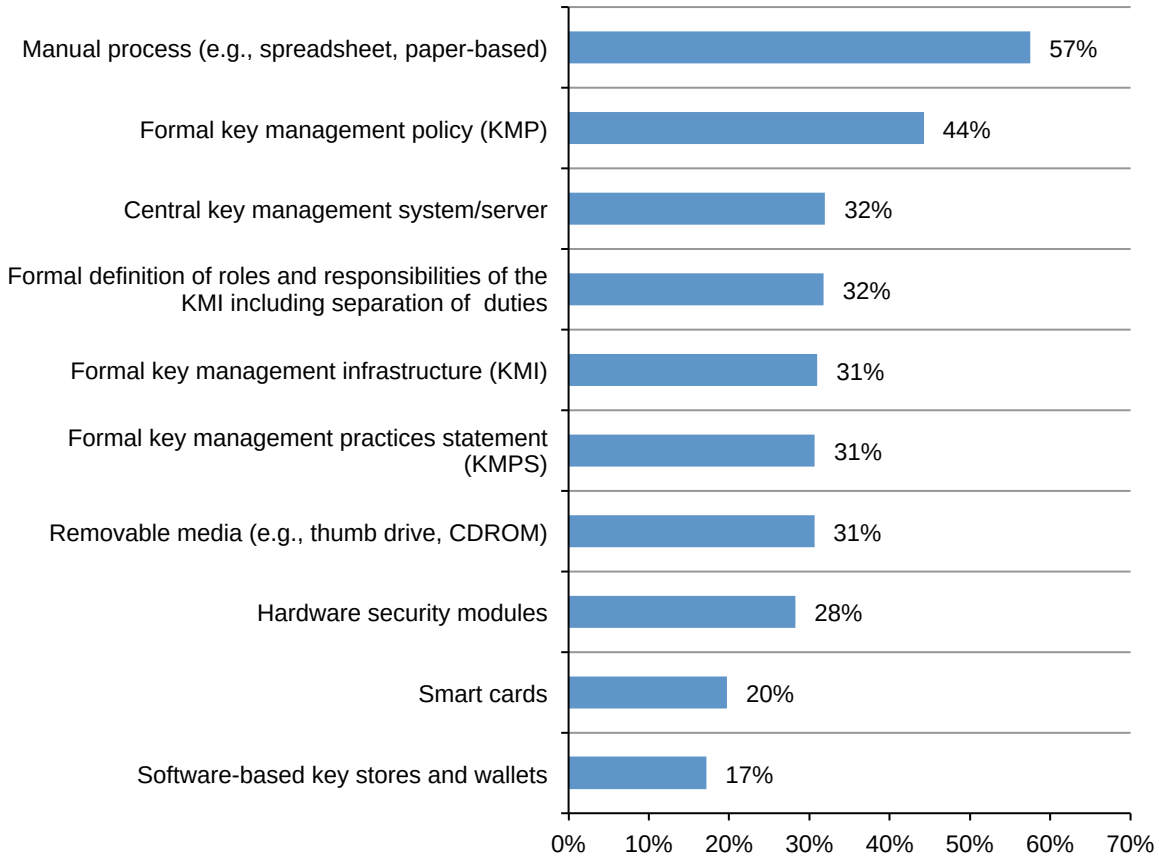
Which keys are most difficult to manage? According to Figure 17, the types of keys that are viewed as most difficult to manage include: (1) SSH keys, (2) keys for external services and (3) keys for third-party systems. The least difficult include: (1) network encryption keys, (2) encryption keys for 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) central key management system/server.

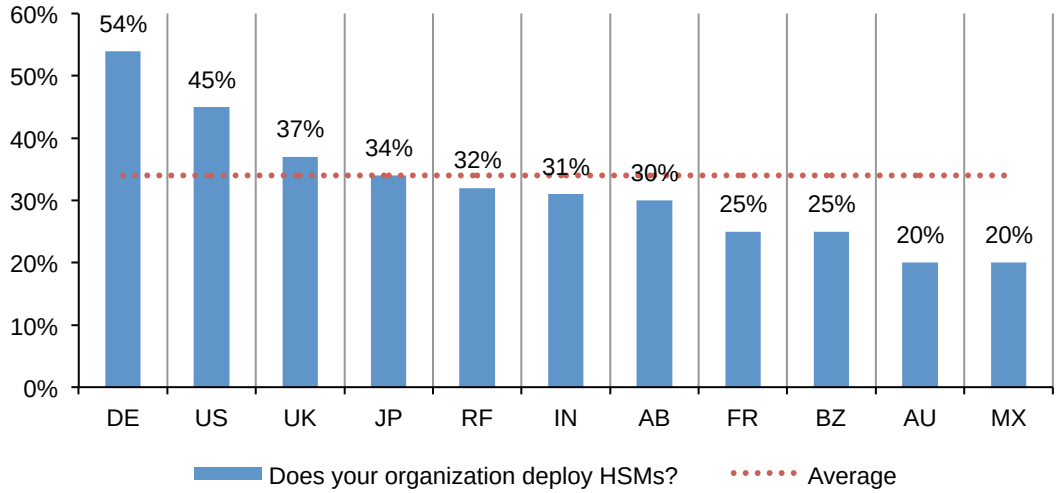
Figure 18. What key management systems does your organization presently use?
Country samples are consolidated
More than one choice permitted



Importance of hardware security modules (HSMs)[5]

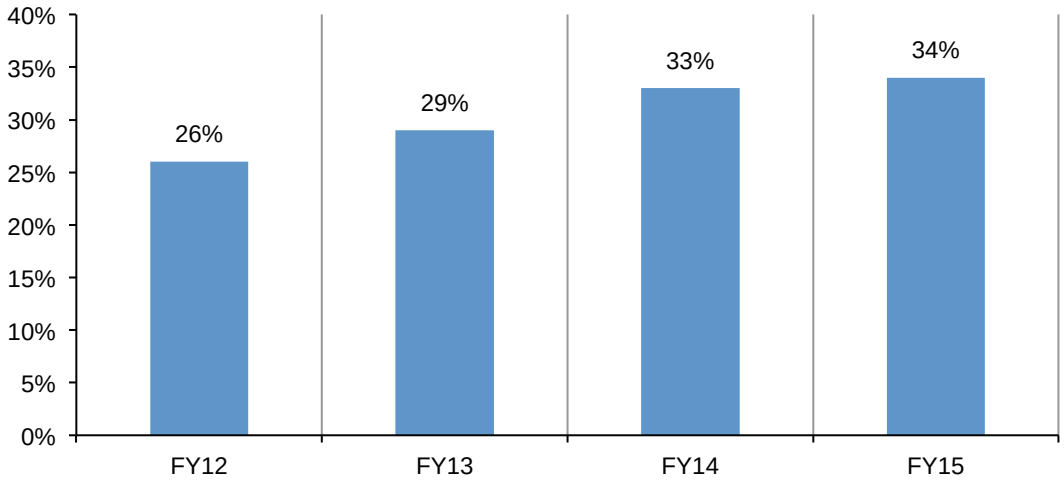
Germany, US and UK organizations are more likely to deploy HSMs. Figure 19 summarizes the percentage of respondents that deploy HSMs as part of their organization's key management program or activities. Germany, US and UK are more likely to deploy HSMs to their organization's key management activities than other countries. The overall average deployment rate for HSMs as part of key management activities is 34 percent.

Figure 19. Deployment HSMs as part of key management



Deployment of HSMs increases steadily. Figure 20 shows a four-year trend for HSMs. As can be seen, the rate of global HSM deployment as part of key management activities has steadily increased.

Figure 20. HSM deployment rate as part of key management over four 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 associated with server based applications 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.

Figure 21 summarizes the percentage of respondents in 11 countries that rate HSM as either very important or important to their organization's key management program or activities. The overall average importance rating in the current year is 49 percent. The pattern of responses suggests Germany, US and Japan are most likely to assign importance to HSMs as part of their organization's key management activities.

Figure 21. Perceived importance of HSMs as part of key management
Important & very important response

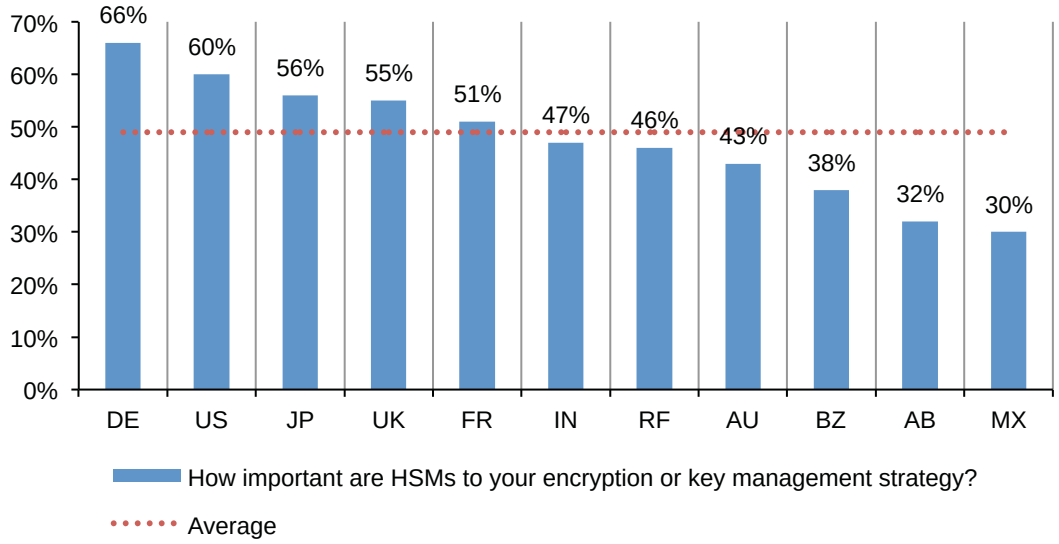
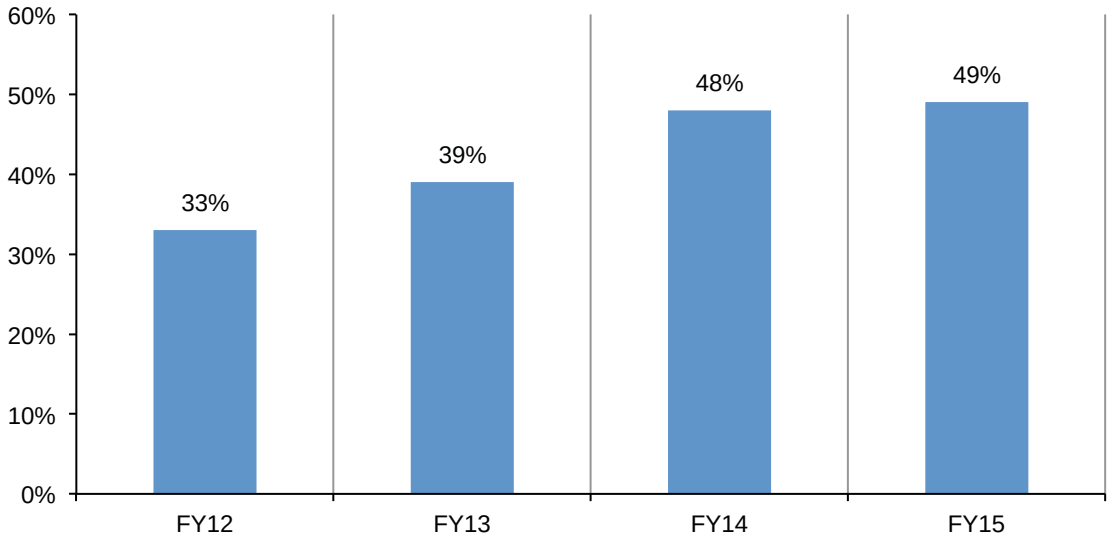


Figure 22 shows a four-year trend. As can be seen, the level of HSM importance has steadily increased over time.

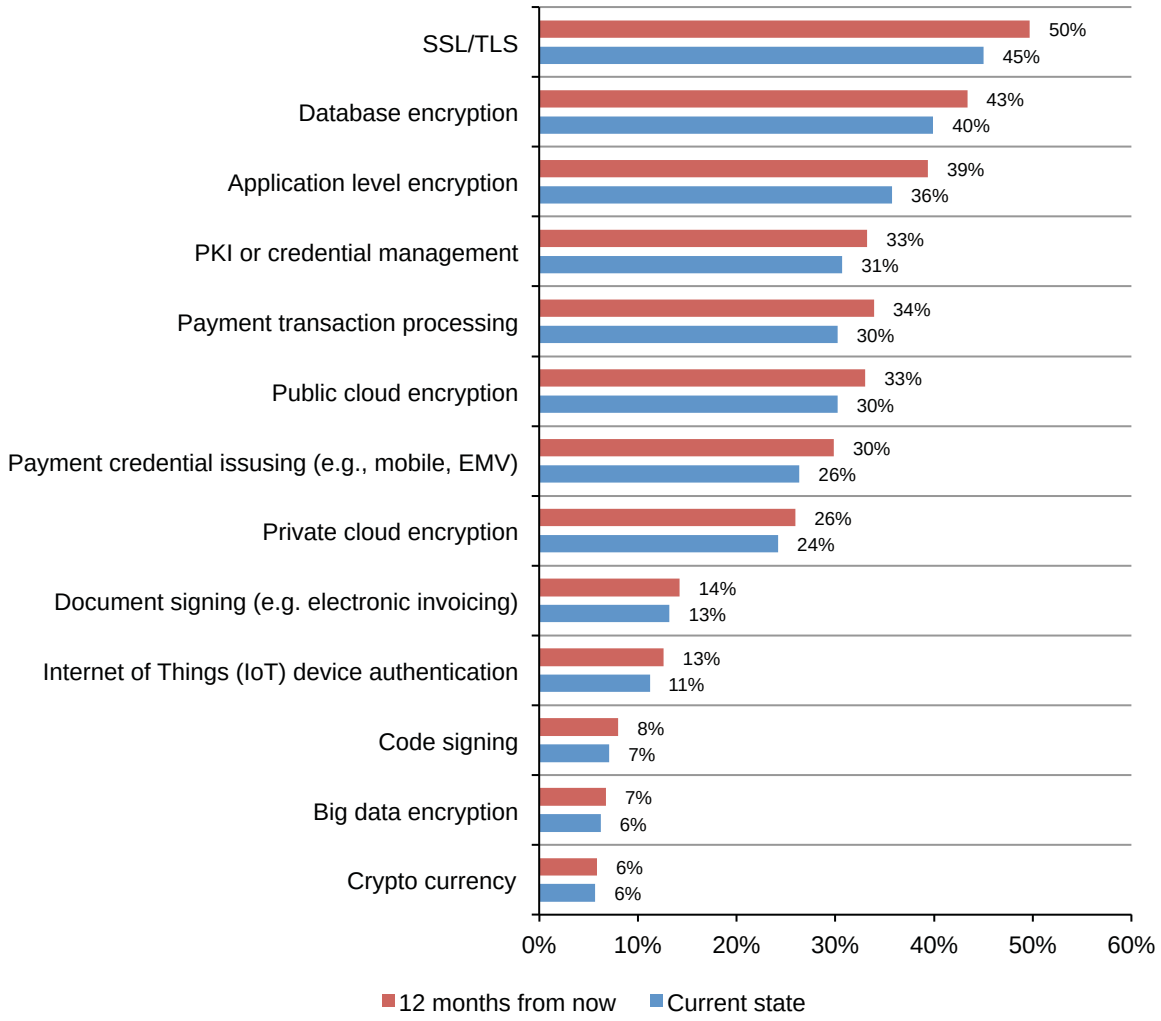
Figure 22. Perceived importance of HSMs as part of key management over four years
Country samples are consolidated



What are the primary purposes or uses for HSMs? Figure 23 summarizes the primary purpose or use cases for deploying HSMs. As can be seen, the two top choices are SSL/TLS and database encryption. This chart shows small differences between today's HSM use and deployment in 12 months.

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

Figure 23. 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 24 reports the average percentage of IT security spending relative to total IT spending over the last 11 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 24. Trend in the percent of IT security spending relative to the total IT budget
Country samples are consolidated

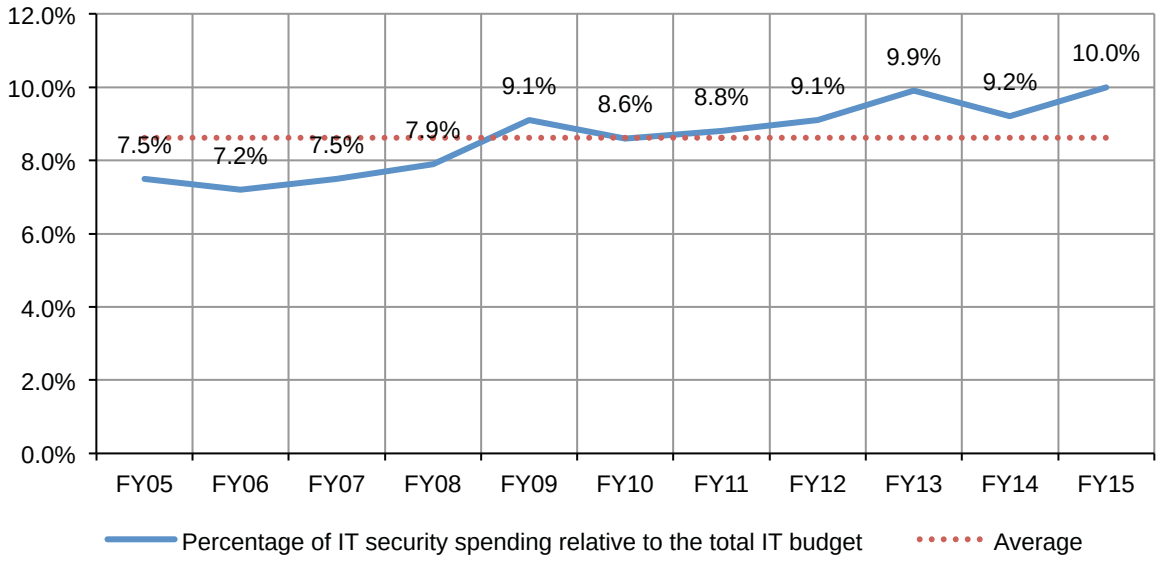
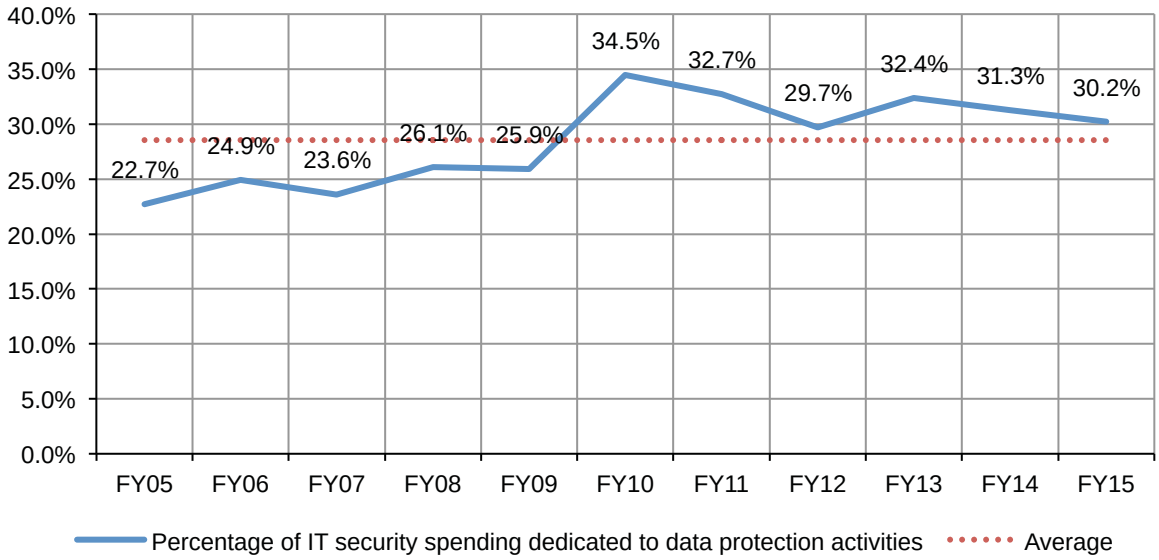


Figure 25 reports the percentage of data protection spending relative to the total IT security budget over 11 years. This trend appears to be slightly upward sloping, which suggests data protection spending as a proportion of total IT security is on the rise.

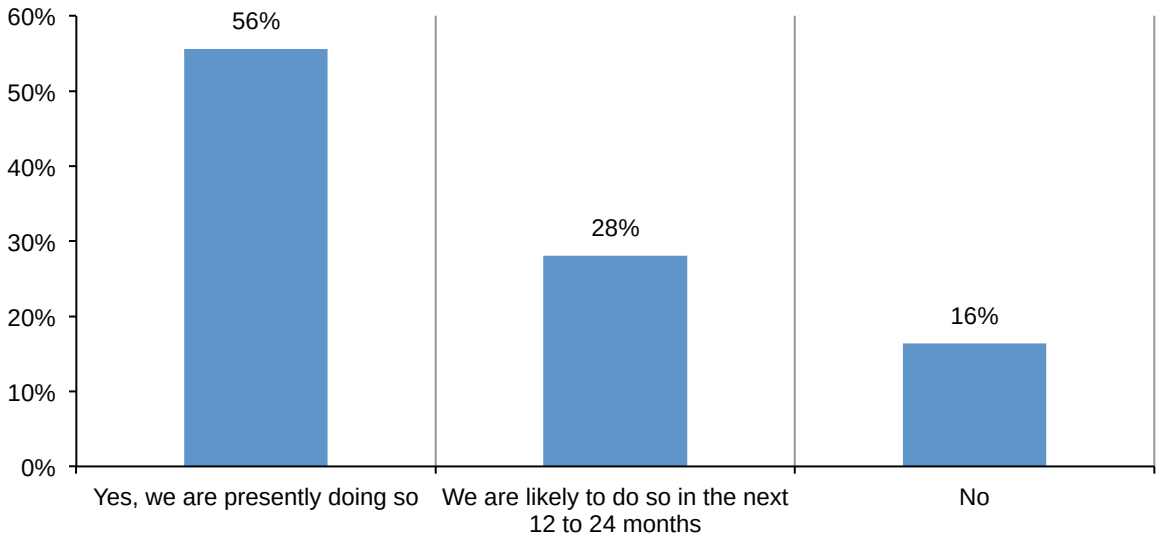
Figure 25. Trend in the percent of IT security spending dedicated to data protection activities
Country samples are consolidated



Cloud encryption

According to Figure 26, 56 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 28 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.

Figure 26. Do you currently transfer sensitive or confidential data to the cloud?
Country samples are consolidated



According to Figure 27, with respect to the transfer of sensitive or confidential data to the cloud, India, Brazil, US and Germany – a mix of both developing and mature countries from an encryption adoption perspective – have higher rates than other countries. Russia has the lowest transfer rate.

Figure 27. Organizations that transfer sensitive or confidential data to the cloud by country

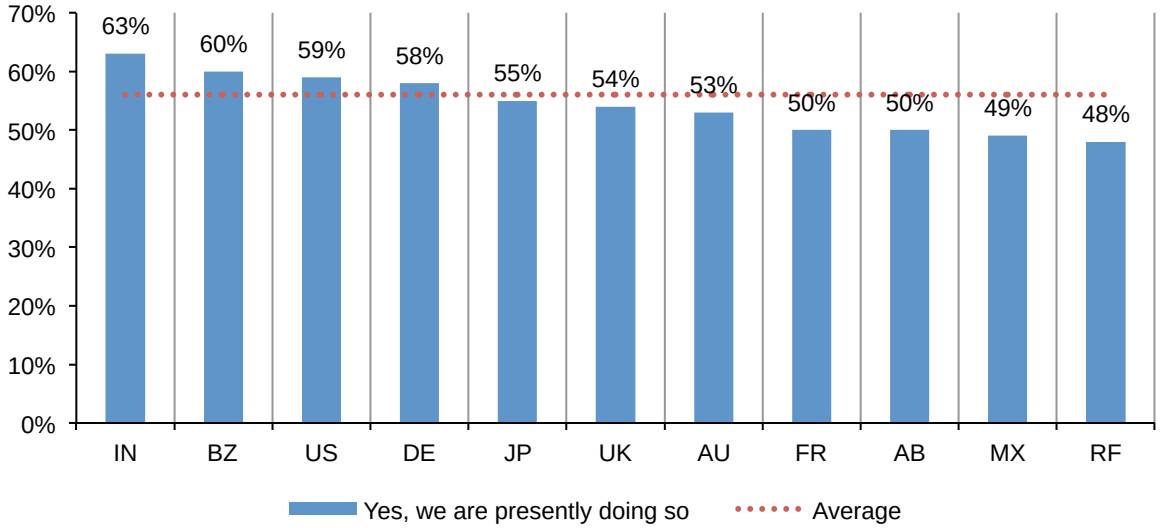
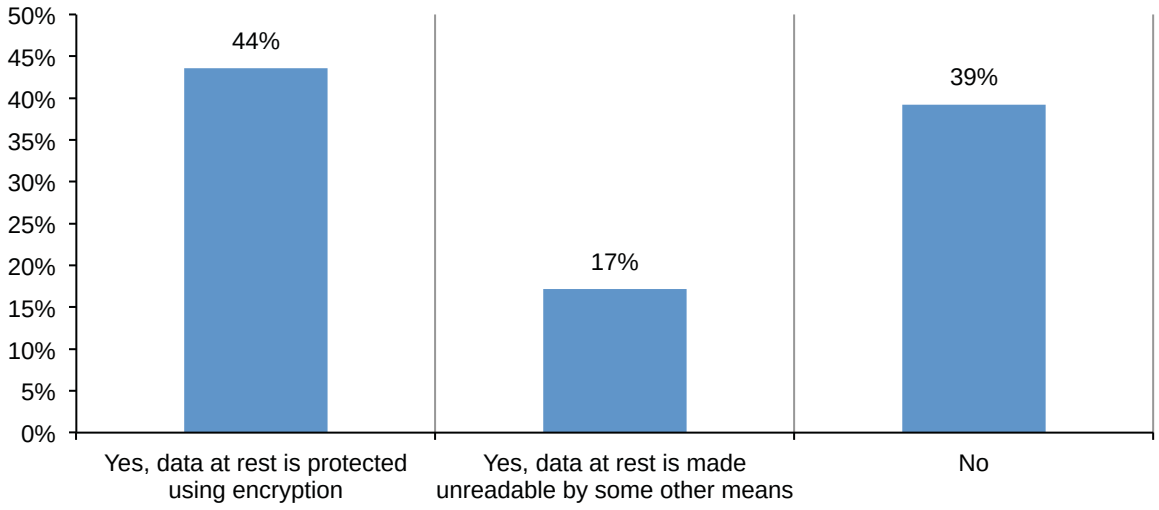


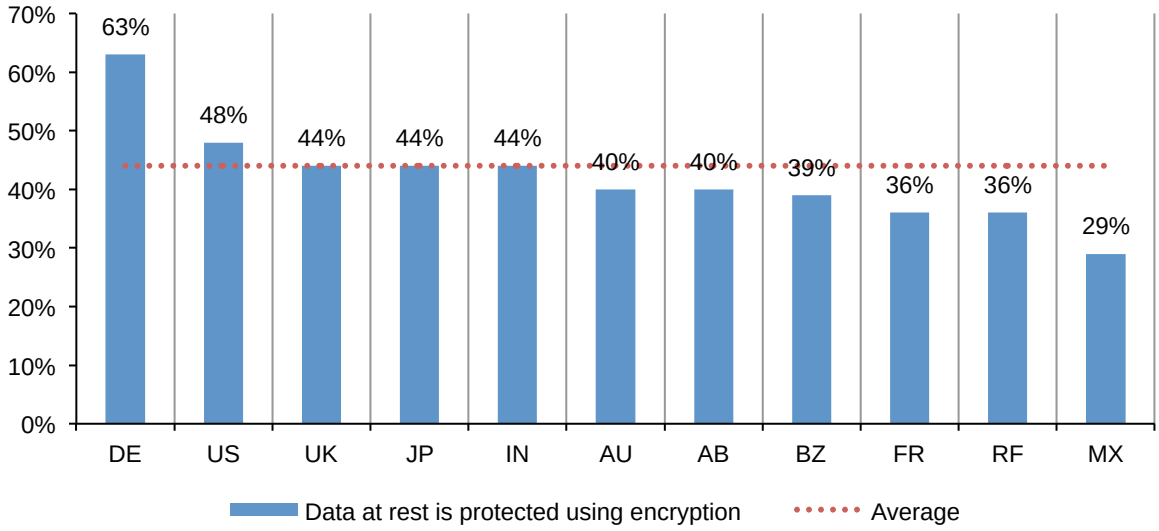
Figure 28 shows 44 percent of respondents say their organizations protect sensitive or confidential data at rest in the cloud using encryption. Another 17 percent say data at rest is made unreadable using some other mechanism such as tokenization or data masking. Although both of these figures grew from the previous year, it is significant to note that almost 40% of cloud data at rest is unprotected.

Figure 28. Do you protect data at rest in the cloud through encryption or some other measure that renders data unreadable?
Country samples are consolidated



As shown in Figure 29, German organizations are most likely to deploy encryption to protect sensitive or confidential data at rest in the cloud environment. In contrast, Mexican organizations are least likely to use encryption to secure data in the cloud.

Figure 29. Organizations that use encryption to protect data at rest in the cloud by country



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 February 2016. Our consolidated sampling frame of practitioners in all countries consisted of 131,453 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 5,605 returns of which 596 were rejected for reliability issues. Our final consolidated 2015 sample was 5,009, thus resulting in an overall 3.8% response rate.

The first encryption trends study was conducted in the US 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 cluster sample (AB) (composed of Saudi Arabia and United Arab Emirates) to this 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	9,882	368	3.7%
AU	Australia	7,565	334	4.4%
BZ	Brazil	13,577	460	3.4%
DE	Germany	15,009	563	3.8%
FR	France	13,210	344	2.6%
IN	India	17,010	578	3.4%
JP	Japan	12,892	487	3.8%
MX	Mexico	10,430	429	4.1%
RF	Russian Federation	5,770	201	3.5%
UK	United Kingdom	13,481	487	3.6%
US	United States	22,509	758	3.4%

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

Table 2. Sample history over 11 years

Legend	FY15	FY14	FY13	FY12	FY11	FY10	FY09	FY08	FY07	FY06	FY05
AB	368	0	0	0	0	0	0	0	0	0	0
AU	334	359	414	938	471	477	482	405	0	0	0
BZ	460	472	530	637	525	0	0	0	0	0	0
DE	563	564	602	499	526	465	490	453	449	0	0
FR	344	375	478	584	511	419	414	0	0	0	0
IN	578	532	0	0	0	0	0	0	0	0	0
JP	487	476	521	466	544	0	0	0	0	0	0
MX	429	445	0	0	0	0	0	0	0	0	0
RF	201	193	201	0	0	0	0	0	0	0	0
UK	487	509	637	550	651	622	615	638	541	489	0
US	758	789	892	531	912	964	997	975	768	918	791
Total	5,009	4,714	4,275	4,205	4,140	2,947	2,998	2,471	1,758	1,407	791

[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.

Figure 30 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 30. Distribution of respondents according to position level
Country samples are consolidated

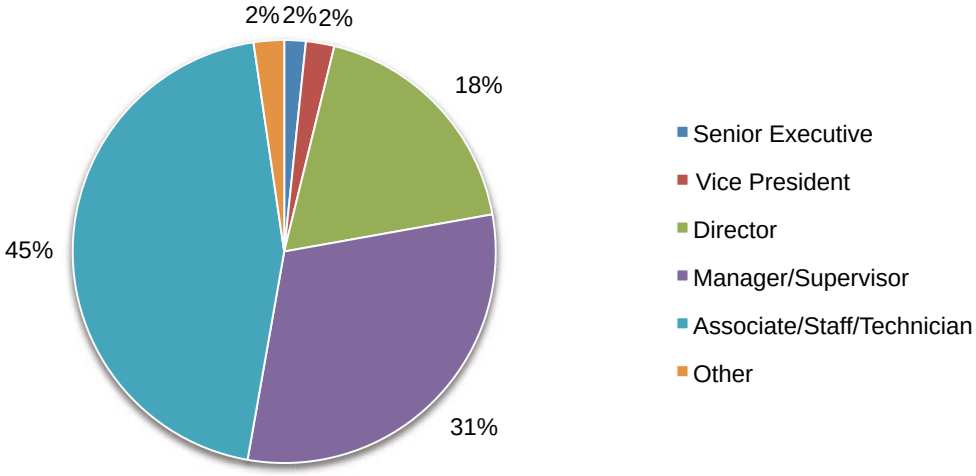
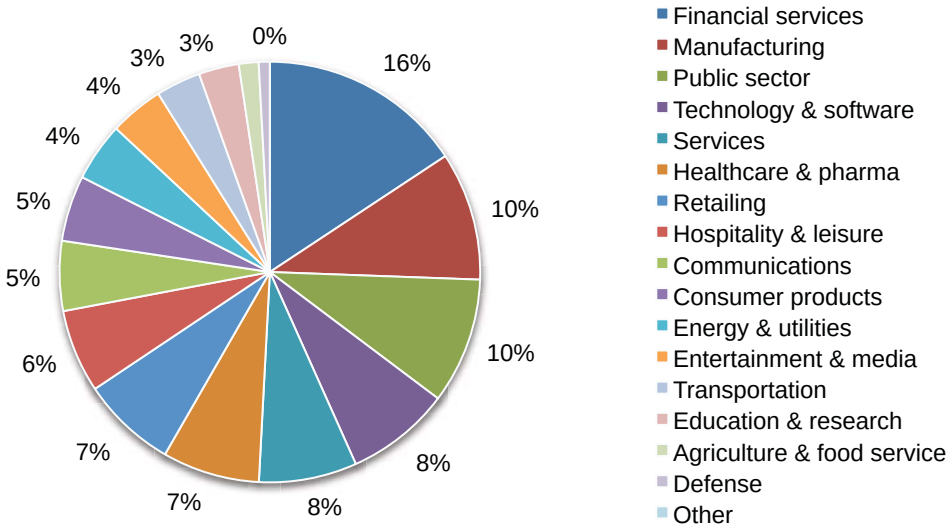


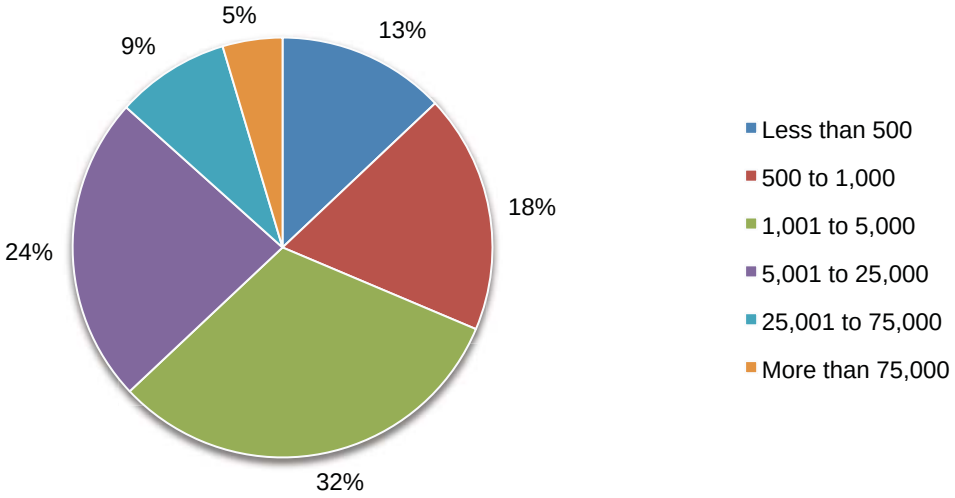
Figure 31 reports the respondents' organizations primary industry segments. As shown, 16 percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Ten percent are located in public sector organizations, including central and local government. Another 10 percent are located in manufacturing companies.

Figure 31. Distribution of respondents according to primary industry classification
Country samples are consolidated



According to Figure 32, the majority of respondent are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 32. 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
Total sampling frame	131,453
Total returns	5,605
Screened or rejected surveys	596
Final sample (consolidated)	5,009
Response rate	3.8%

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	37%
We have an overall encryption plan or strategy that is adjusted to fit different applications and data types	25%
For certain types of sensitive or confidential data such as Social Security numbers or credit card accounts we have a limited encryption plan or strategy	22%
We don't have an encryption plan or strategy	15%
Total	100%

Q2. Following are 14 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. In addition, please check if you are directly involved in the deployment of each area presented.

Q2a-1 Backup and archives	Consolidated
Extensively deployed	50%
Partially deployed	24%
Not deployed	26%
Total	100%

Q2b-1. Big data repositories	Consolidated
Extensively deployed	26%
Partially deployed	23%
Not deployed	52%
Total	100%

Q2c-1. Business applications	Consolidated
Extensively deployed	26%
Partially deployed	41%
Not deployed	33%
Total	100%

Q2d-1. Data center storage	Consolidated
Extensively deployed	44%
Partially deployed	36%
Not deployed	20%
Total	100%

Q2e-1. Databases	Consolidated
Extensively deployed	60%
Partially deployed	27%
Not deployed	13%
Total	100%

Q2f-1. Desktop & workstation hard drives	Consolidated
Extensively deployed	42%
Partially deployed	21%
Not deployed	37%
Total	100%

Q2g-1. Email	Consolidated
Extensively deployed	33%
Partially deployed	40%
Not deployed	27%
Total	100%

Q2h-1. Public cloud services	Consolidated
Extensively deployed	25%
Partially deployed	28%
Not deployed	46%
Total	100%

Q2i-1. File systems	Consolidated
Extensively deployed	33%
Partially deployed	29%
Not deployed	38%
Total	100%

Q2j-1. Internet communications (e.g., SSL)	Consolidated
Extensively deployed	59%
Partially deployed	28%
Not deployed	13%
Total	100%

Q2k-1. Internal networks (e.g., VPN/LPN)	Consolidated
Extensively deployed	45%
Partially deployed	33%
Not deployed	22%
Total	100%

Q2l-1. Laptop hard drives	Consolidated
Extensively deployed	58%
Partially deployed	19%
Not deployed	23%
Total	100%

Q2m-1 Private cloud infrastructure	Consolidated
Extensively deployed	27%
Partially deployed	30%
Not deployed	43%
Total	100%

Q2n-1 Cloud gateway (2016 only)	Consolidated
Extensively deployed	40%
Partially deployed	31%
Not deployed	29%
Total	100%

Q4. In your organization, who has responsibility or is most influential in directing your organization's strategy for using encryption? Please select one best choice.	Consolidated
No single function has responsibility	20%
IT operations	32%
Finance	3%
Lines of business (LOB) or general management	27%
Security	16%
Compliance	2%
Total	100%

Q5. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top three reasons.	Consolidated
To avoid public disclosure after a data breach occurs	8%
To protect information against specific, identified threats	49%
To comply with internal policies	15%
To comply with external privacy or data security regulations and requirement	61%
To reduce the scope of compliance audits	34%
To protect enterprise intellectual property	50%
To protect customer personal information	47%
To limit liability from breaches or inadvertent disclosure	35%
Total	300%

Q7. 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	57%
Classifying which data to encrypt	35%
Determining which encryption technologies are most effective	13%
Initially deploying the encryption technology	49%
Ongoing management of encryption and keys	31%
Training users to use encryption appropriately	15%
Total	200%

Q8. 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	69%
Management of keys	67%
Support for multiple applications or environments	53%
Separation of duties and role-based controls	54%
System scalability	68%
Tamper resistance by dedicated hardware (e.g., HSM)	54%
Integration with other security tools (e.g., SIEM and ID management)	59%
Support for regional segregation (e.g., data residency)	43%
System performance and Latency	73%
Support for emerging algorithms (e.g., ECC)	67%
Support for cloud and on-premise deployment	71%
Formal product security certification (e.g., FIPS 140)	56%

Q9. What types of data does your organization encrypt? Please select all that apply.	Consolidated
Customer information	36%
Non-financial business information	30%
Intellectual property	49%
Financial records	48%
Employee/HR data	62%
Payment related data	55%
Health-related information	20%

Q10. What are the main threats that might result in the exposure of sensitive or confidential data? Please select the top two choices.	Consolidated
Hackers	28%
Malicious insiders	18%
System or process malfunction	30%
Employee mistakes	52%
Temporary or contract workers	22%
Third party service providers	20%
Lawful data request (e.g. by police)	12%
Government eavesdropping	18%
Total	200%

Part 2. Key Management

Q12. Please rate the overall "pain" associated with managing keys within your organization, where 1 = minimal impact to 10 = severe impact?	Consolidated
1 or 2	9%
3 or 4	16%
5 or 6	22%
7 or 8	23%
9 or 10	30%
Total	100%

Q13. What makes the management of keys so painful? Please select the top three reasons.	Consolidated
No clear ownership	57%
Insufficient resources (time/money)	23%
Lack of skilled personnel	49%
No clear understanding of requirements	16%
Too much change and uncertainty	37%
Key management tools are inadequate	46%
Systems are isolated and fragmented	47%
Technology and standards are immature	13%
Manual processes are prone to errors and unreliable	11%
Total	300%

Q14. 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 painfut response combined.	Consolidated
Encryption keys for backups and storage	21%
Encryption keys for archived data	36%
Keys associated with SSL/TLS	46%
SSH keys	61%
End user encryption keys (e.g., email, full disk encryption)	39%
Network encryption keys (e.g., IPSEC)	26%
Application-owned keys (e.g. signing, authentication, encryption)	54%
Payments-related keys (e.g., ATM, POS, etc.)	37%
Embedded device keys and certificates (e.g. products you make)	16%
Keys for external services (e.g., cloud or hosted services)	61%
Keys for 3rd party systems (e.g., partners, customers, single sign-on, federation, etc.)	57%
Private keys for certificate issuance	52%

Q15a. What key management systems does your organization presently use?	Consolidated
Formal key management policy (KMP)	44%
Formal key management practices statement (KMPS)	31%
Formal key management infrastructure (KMI)	31%
Formal definition of roles and responsibilities of the KMI including separation of duties	32%
Manual process (e.g., spreadsheet, paper-based)	57%
Central key management system/server	32%
Hardware security modules	28%
Removable media (e.g., thumb drive, CDROM)	31%
Software-based key stores and wallets	17%
Smart cards	20%
Total	323%

Part 3. Hardware Security Modules

Q16. What best describes your level of knowledge about HSMs?	Consolidated
Very knowledgeable	28%
Knowledgeable	41%
Not knowledgeable (skip to Q19)	31%
Total	100%

Q17a. Does your organization deploy HSMs?	Consolidated
Yes	34%
No (skip to Q19)	66%
Total	100%

Q17b. For what purpose does your organization presently deploy or plan to deploy HSMs? Please select all that apply.	
Q17b-1. HSMs deployed today	Consolidated
Application level encryption	36%
Database encryption	40%
Big data encryption	6%
Public cloud encryption	30%
Private cloud encryption	24%
SSL/TLS	45%
PKI or credential management	31%
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%
Crypto currency	6%
Not planning to use	11%
Total	317%

Q17b-2. HSMs planned to be deployed in the next 12 months	Consolidated
Application level encryption	39%
Database encryption	43%
Big data encryption	7%
Public cloud encryption	33%
Private cloud encryption	26%
SSL/TLS	50%
PKI or credential management	33%
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)	30%
Crypto currency	6%
Not planning to use	12%
Total	348%

Q18. In your opinion, how important are HSMs to your encryption or key management strategy? Very important and important response combined	Consolidated
Q18a. Importance today	49%
Q18b. Importance in the next 12 months	56%

Part 4. Budget Questions

Q19a. Are you responsible for managing all or part of your organization's IT budget this year?	Consolidated
Yes	55%
No (skip to Q20)	45%
Total	100%

Q19b. Approximately, what is the dollar range that best describes your organization's IT budget for 2015?	NA
Extrapolated values shown in millions (billions for JPY, RUB, Rupee and Paso)	

Q19c. Approximately, what percentage of the 2016 IT budget will go to IT security activities?	Consolidated
Extrapolated value	10.0%

Q19d. Approximately, what percentage of the 2016 IT security budget will go to data protection activities?	Consolidated
Extrapolated value	30.2%

Q19e. Approximately, what percentage of the 2016 IT security budget will go to encryption activities?	Consolidated
Extrapolated value	13.6%

Part 6: Cloud encryption: When responding to the following questions, please assume they refer only to public cloud services.	
Q37a. 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	54%
No, but we are likely to do so in the next 12 to 24 months	20%
No (Go to Part 7 if you do not use cloud services for any class of data or application)	26%
Total	100%

Q37b. 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	56%
No, but we are likely to do so in the next 12 to 24 months	28%
No (Go to Part 7 if you do not use or plan to use any cloud services for sensitive or confidential data)	16%
Total	100%

Q37c. In your opinion, who is most responsible for protecting sensitive or confidential data transferred to the cloud?	Consolidated
The cloud provider	58%
The cloud user	20%
Shared responsibility	22%
Total	100%

Q37d. Does your organization protect data at rest in the cloud through the use of encryption or some other measure that renders data unreadable (e.g. tokenization)?	Consolidated
Yes (data at rest is protected using encryption)	44%
Yes (data at rest is made unreadable by some other means)	17%
No	39%
Total	100%

Q37e. If data at rest in the cloud is protected by the use of encryption, how is that protection applied?	Consolidated
Data is encrypted before it is sent to the cloud (please exclude the use of SSL/IPSec or other network encryption when answering)	44%
Data at rest in the cloud is encrypted in the cloud using tools placed there by your organization	21%
Data at rest in the cloud is encrypted in the cloud by the cloud provider	35%
Total	100%

Q37f. For encryption of data at rest in the cloud, my organization's strategy is to . . .	Consolidated
Only use keys controlled by my organization	41%
Only use keys controlled by the cloud provider	21%
Use a combination of keys controlled by my organization and by the cloud provider	38%
Total	100%

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	31%
Associate/Staff/Technician	45%
Other	2%
Total	100%

D2. Check the functional area that best describes your organizational location.	Consolidated
IT operations	57%
Security	16%
Compliance	9%
Finance	3%
Lines of business (LOB)	12%
Other	4%
Total	100%

D3. What industry best describes your organization's industry focus?	**Consolidated**
Agriculture & food service	2%
Communications	5%
Consumer products	5%
Defense	1%
Education & research	3%
Energy & utilities	4%
Entertainment & media	4%
Financial services	16%
Healthcare & pharma	7%
Hospitality & leisure	6%
Manufacturing	10%
Public sector	10%
Retailing	7%
Services	8%
Technology & software	8%
Transportation	3%
Other	0%
Total	100%

D4. What is the worldwide headcount of your organization?	**Consolidated**
Less than 500	13%
500 to 1,000	18%
1,001 to 5,000	32%
5,001 to 25,000	24%
25,001 to 75,000	9%
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 a leading global provider of trust management and data protection solutions that protect the world's most sensitive applications and information. Thales solutions address identity and privacy related challenges with hardware and software-based encryption, digital signature, and management capabilities. In today's increasingly connected world, our solutions help thwart today's targeted attacks and reduce the risk of sensitive data exposure introduced by cloud computing and virtualization, consumer devices in the workplace, increased mobility, big data, and more. www.thales-esecurity.com

About Thales

Thales is a global technology leader for the Aerospace, Transport, Defence and Security markets. With 61,000 employees in 56 countries, Thales reported sales of €13 billion in 2014. With over 20,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its unique international footprint allows it to work closely with its customers all over the world.

Positioned as a value-added systems integrator, equipment supplier and service provider, Thales is one of Europe's leading players in the security market. The Group's security teams work with government agencies, local authorities and enterprise customers to develop and deploy integrated, resilient solutions to protect citizens, sensitive data and critical infrastructure.

Additional Sponsor

About Vormetric

Vormetric's comprehensive high-performance data security platform helps companies move confidently and quickly. Our seamless and scalable platform is the most effective way to protect data wherever it resides—any file, database and application in any server environment. Advanced transparent encryption, powerful access controls and centralized key management let organizations encrypt everything efficiently, with minimal disruption. Regardless of content, database or application—whether physical, virtual or in the cloud —Vormetric Data Security enables confidence, speed and trust by encrypting the data that builds business.