2015 Global Encryption & Key Management Trends Study

Sponsored by Thales e-Security

Independently conducted by Ponemon Institute LLC

Publication Date: April 2015

2015 Global Encryption Trends & Key Management Study

2015 Global Encryption & Key Management Trends Study[1]

Ponemon Institute, April 2015

Part 1. Executive Summary

Ponemon Institute is pleased to present the findings of *the 2015 Global Encryption & Key Management Trends Study,* sponsored by Thales e-Security. We surveyed 4,714 individuals across multiple industry sectors in 10 countries - the United States, United Kingdom, Germany, France, Australia, Japan, Brazil, the Russian Federation and for the first time Mexico and India.[2] The purpose of this research is to examine how the use of encryption has evolved over the past ten 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—especially in healthcare and retail industries. However, they still struggle with the "pain" of managing keys or certificates.

Following is a summary of our key findings. More details are provided for each key finding listed below in the next section of this paper. We believe the findings are important because they demonstrate the relationship between encryption and a strong security posture.

Following are key takeaways from this study:

- More companies embrace an encryption strategy that is applied consistently across the enterprise.
- Business units continue to gain influence in choosing and deploying encryption technologies.
- Healthcare and retail companies increased encryption usage more than other industries.
- The biggest challenge in planning and executing a data encryption strategy is discovering where sensitive data resides in the organization.
- Support for cloud and on-premise deployment is one of the most important features of an encryption solution.
- Management of keys and certificates is painful because of no clear ownership and systems are isolated and fragmented.

Summary of key findings:

Most companies in this research have an overall, enterprise-wide encryption plan or strategy. Thirty-six percent of respondents say they have an overall encryption plan or strategy that is applied consistently across the entire enterprise and 26 percent say their enterprise encryption plan is adjusted to fit different applications and data types. Only 15 percent of respondents say they have no strategy.

German companies continue to dominate in the strategic use of encryption. Companies in the US and Japan follow in applying encryption strategies consistently across the entire enterprise**.** In contrast, Brazil and Mexico are least likely to use encryption as a strategically important security tool.

[1] This year's study was completed in December 2014 for 10 country samples.

[2] In the figures, countries are abbreviated as follows: Germany (DE), Japan (JP), United States (US), United Kingdom (UK), Australia (AU), France (FR), Brazil (BZ), Russia (RF), Mexico (MX) and India (IN).

[3] The trend analysis shown in this study was performed on combined country samples spanning 10 years (since 2005).

IT operations are losing influence over determining their companies' encryption strategy. While IT continues to have the most responsibility for defining the company's encryption strategy, lines of business are becoming more important. This could be due in part to companies permitting greater use of employee-owned devices and an increase in the consumerization of IT.

Healthcare and retail companies have had the greatest increases in encryption usage. Most industries continue to increase their use of encryption. However, possibly because of the Anthem data breach in healthcare and numerous mega retail data breaches these industries had the highest increase in encryption deployment.

Companies take a tactical approach to encryption mainly to comply with external privacy or data security regulations and requirements. Sixty-seven percent of respondents say their approach to using encryption is driven by individual requirements and not so much strategic goals (33 percent of respondents).

What are the main drivers for using encryption technology solutions? When asked why their organization encrypts sensitive and confidential data, 64 percent of respondents say compliance is most important, followed by protection of information against specific, identified threats (42 percent of respondents), reduction in the scope of compliance audits (41 percent of respondents) and general improvement in their security posture (25 percent of respondents). Only 19 percent of respondents say it is to comply with internal policies and 9 percent say it is to avoid public disclosure after a data breach occurs.

Only 22 percent of respondents believe encrypted data that was lost or stolen would require customers to be notified if a data breach occurred. Data most often encrypted is employee/HR data (61 percent of respondents), payment-related data (56 percent of respondents) and financial records (51 percent of respondents) are most often encrypted. Employee mistakes (53 percent of respondents) are by far the biggest threat to the exposure of sensitive or confidential data. Only 19 percent say malicious insiders are a main threat.

The biggest challenge in planning and executing a data encryption strategy is discovering where sensitive data resides in the organization. Fifty-six percent of respondents say it is finding the location of their organizations' sensitive data followed by 48 percent of respondents who say it is initially deploying encryption technology that is the hardest part of an encryption strategy.

A concern for many is classifying which data to encrypt (34 percent of respondents) and ongoing management of encryption and keys (33 percent of respondents). The human factor (training users to use encryption appropriately) is only an issue for 15 percent of respondents.

Support for cloud and on-premise deployment is the most important feature of an encryption solution. The ability to integrate encryption solutions on premise and in the cloud is key for companies, according to 62 percent of respondents. Fifty-three percent of respondents say system performance and latency is important. Management of keys (51 percent of respondents) and integration with other security tools and management keys is important (51 percent of respondents).

Encryption and tokenization are considered alternative approaches to safeguarding sensitive data, according to 40 percent of respondents. Thirty-five percent of respondents believe encryption and tokenization are alternative approaches in a few specific scenarios. Only 8 percent say the use of tokenization and encryption are unrelated—each has its own clear areas for usage.

Managing keys or certificates is painful. Fifty-six percent of respondents rate the overall "pain" associated with managing keys or certificates within their organizations as severe (7+ on a scale of 1 = minimal impact to 10 = severe impact). The top reasons for the difficulty are no clear ownership (58 percent), systems are isolated and fragmented (50 percent) and lack of skilled personnel (47 percent). The most painful are SSH keys (63 percent), keys for external services (cloud or hosted services) (61 percent) and application level keys and certificates (e.g. signing, authentication and encryption) (51 percent).

Fifty-one percent say they use manual processes (e.g. spreadsheet, paper-based), followed by external certificate authority and removable media (e.g. thumb drive, CDROM) are the key management systems their organizations mostly use. Respondents are directly involved in these key management systems: hardware security modules (56 percent of respondents), internal certificate authority (54 percent of respondents) and central key management system/server (43 percent of respondents).

Hardware security modules (HSMs) are deployed by 33 percent of the organizations and growing in importance. Forty-four percent of respondents rate HSMs as important to their key management strategy. In the next 12 months, 55 percent of respondents say their deployment will become more important to their organizations.

The main reasons for using HSMs are authentication (52 percent of respondents), followed by SSL (48 percent of respondents) and database encryption (47 percent of respondents). In the next 12 months, HSMs will be deployed mostly for authentication (58 percent), database encryption (51 percent) and SSL (46 percent).

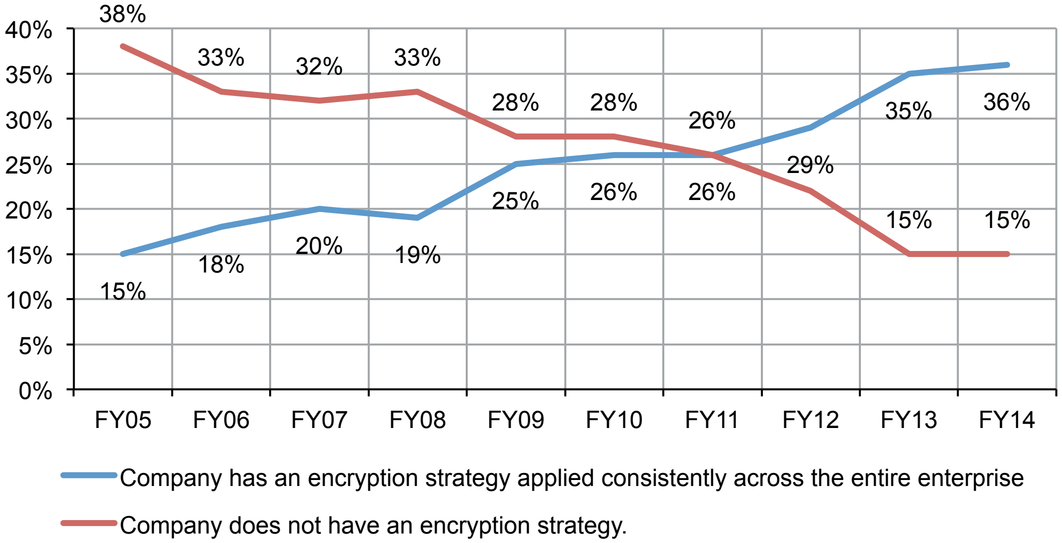
For the first time in 10 years, budget allocated to encryption decreased. Between 2005 and 2013, encryption spending relative to the total IT security budget increased from a low of 9.7 percent to 18.2 percent. However, this year's budget decreased to 15.7 percent.

Part 2. Key Findings

Strategy and adoption of encryption

Since conducting this study, 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. Figure 1 shows these changes over the past 10 years.

Figure 1. Trends in encryption strategy



According to Figure 2, 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 and Brazil report the lowest adoption of an enterprise encryption strategy.

Figure 2. Differences in enterprise encryption strategies by country

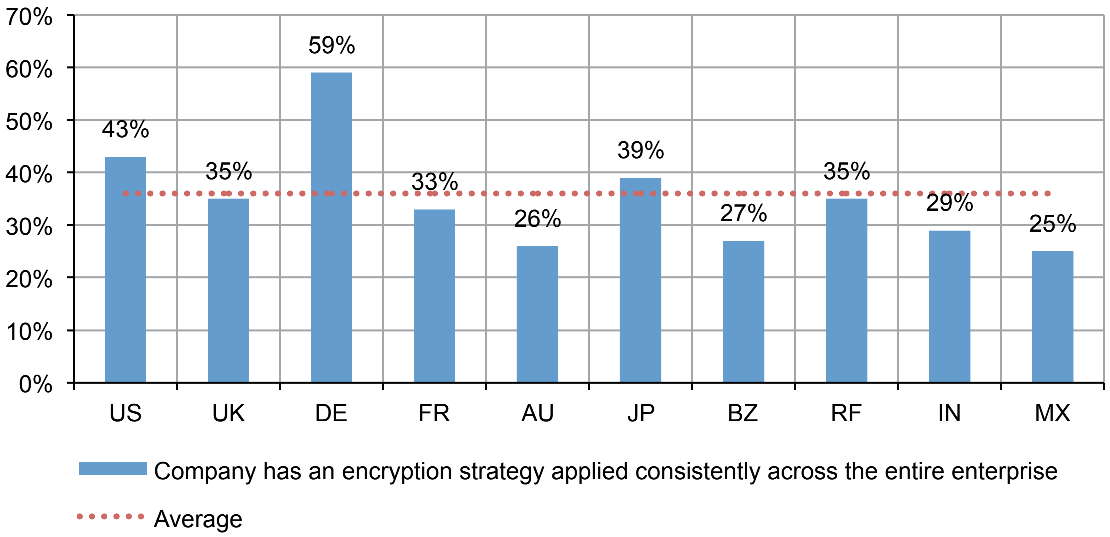


Figure 3 shows the most influential functional areas for defining the company's encryption strategy. The figure shows that IT operations are deemed most influential in determining the organization's enterprise encryption strategy. In this study, "lines of business" are defined as those with commercial or executive responsibility within the organization.

Figure 3. Most influential for determining the company's encryption strategy

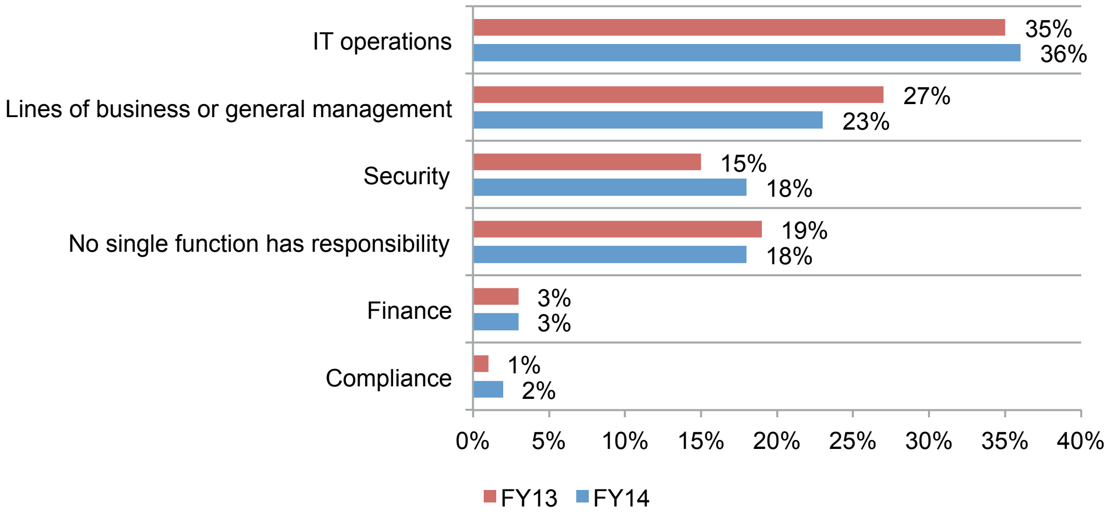


Figure 4 shows that the IT operations function has consistently been most influential in framing the organization's encryption strategy over 10 years. However, that picture is steadily changing with business unit leaders gaining influence over their company's encryption strategy.

We posit that the rising influence of business leaders reflects a general increase in consumer concerns over data privacy and the importance of demonstrating compliance to 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 been relatively constant (flat line) over a 10-year period.

Figure 4. Influence of IT operations, lines of business and security

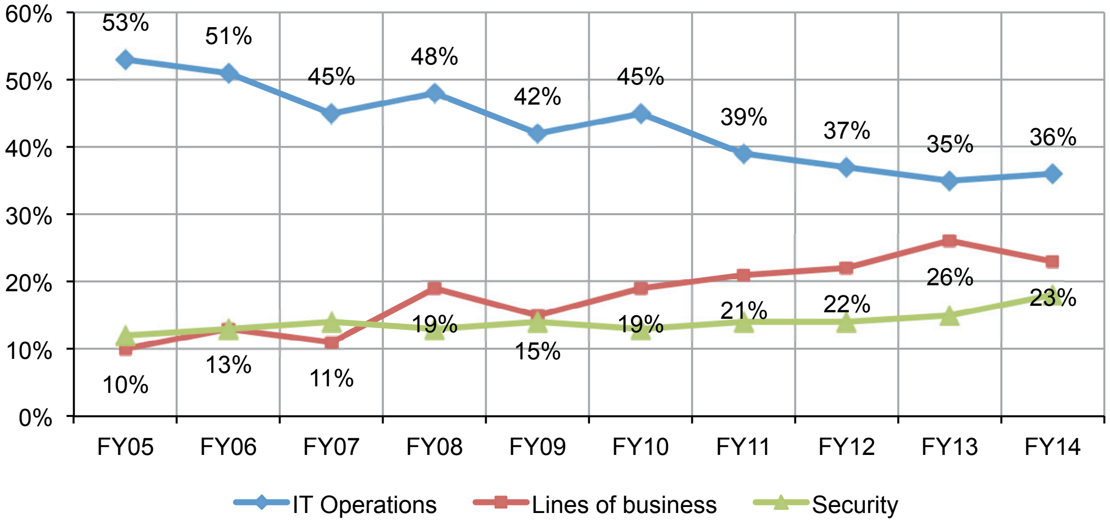
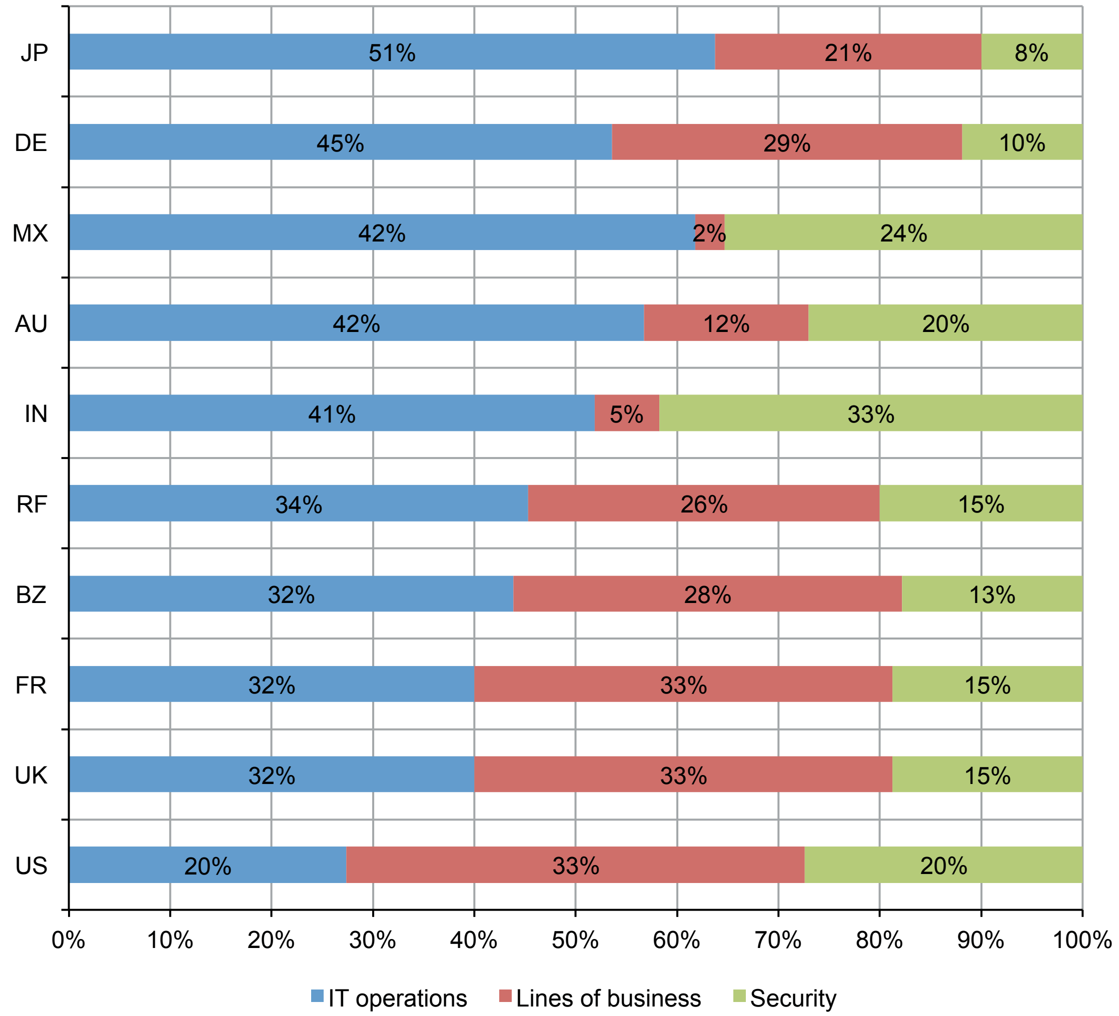


Figure 5 shows the percentage distribution of respondents who rate IT operations, LOB and security as most influential in determining their organization's encryption strategy. This chart shows IT operations as most influential in seven of 10 countries. In contrast, the US, UK and France see business managers as most influential in determining the company's encryption strategy.

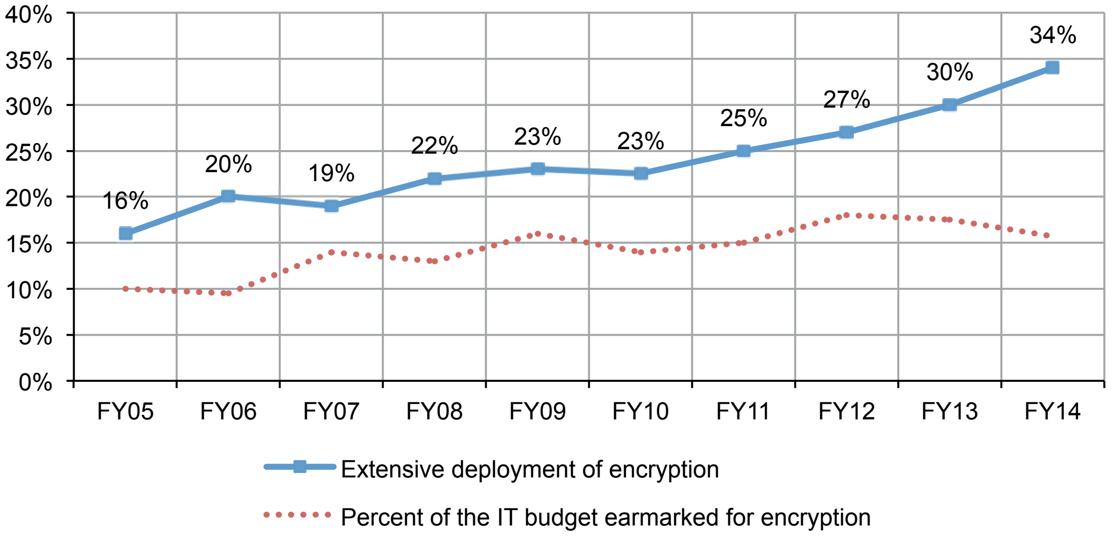
Figure 5. Influence of IT operations, LOB and security by country



Trends in adoption of encryption

Since we began tracking the enterprise-wide use of encryption in 2005, there has been a steady increase in the encryption solutions used by organizations.[4] Figure 6 summarizes enterprise-wide usage consolidated for various encryption technologies over 10 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 modest correlation.

Figure 6. Trend on the extensive use of encryption technologies



[4] The combined sample used to analyze trends is explained in Part 3. Methods.

Figure 7 shows a positive relationship between encryption strategy and the deployment of encryption. German, US and Japanese organizations have the highest percentage of companies with an enterprise encryption strategy and they are the most extensive users of encryption technologies. In contrast, Mexico has the lowest percentage of companies with an enterprise strategy for encryption and has the lowest extensive use rate.

Figure 7. Extensive use and prevalence of an enterprise encryption strategy by country

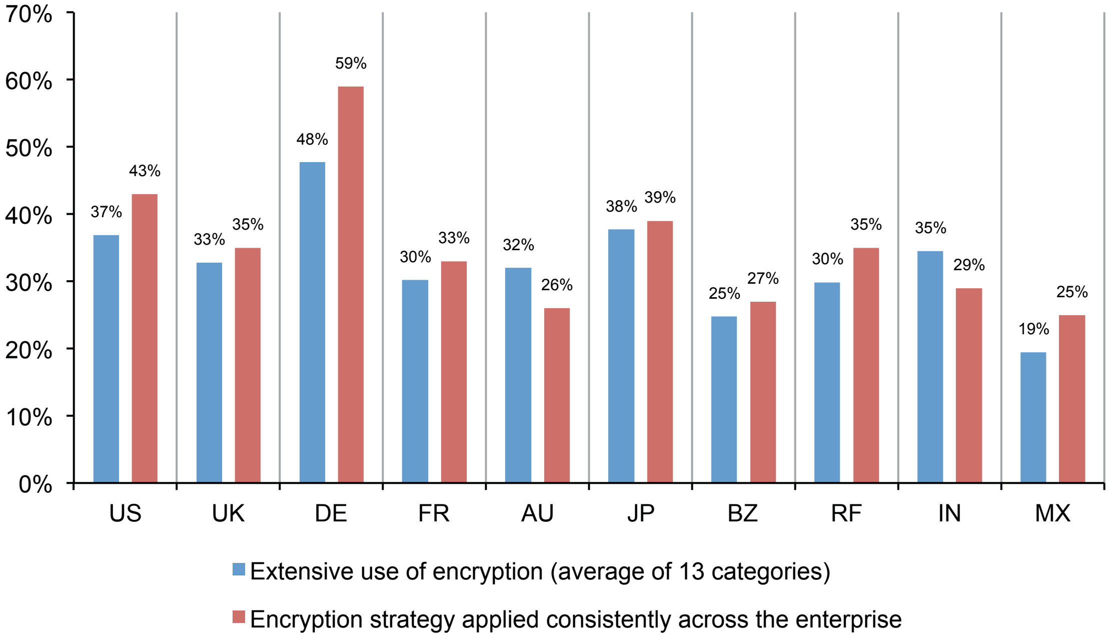
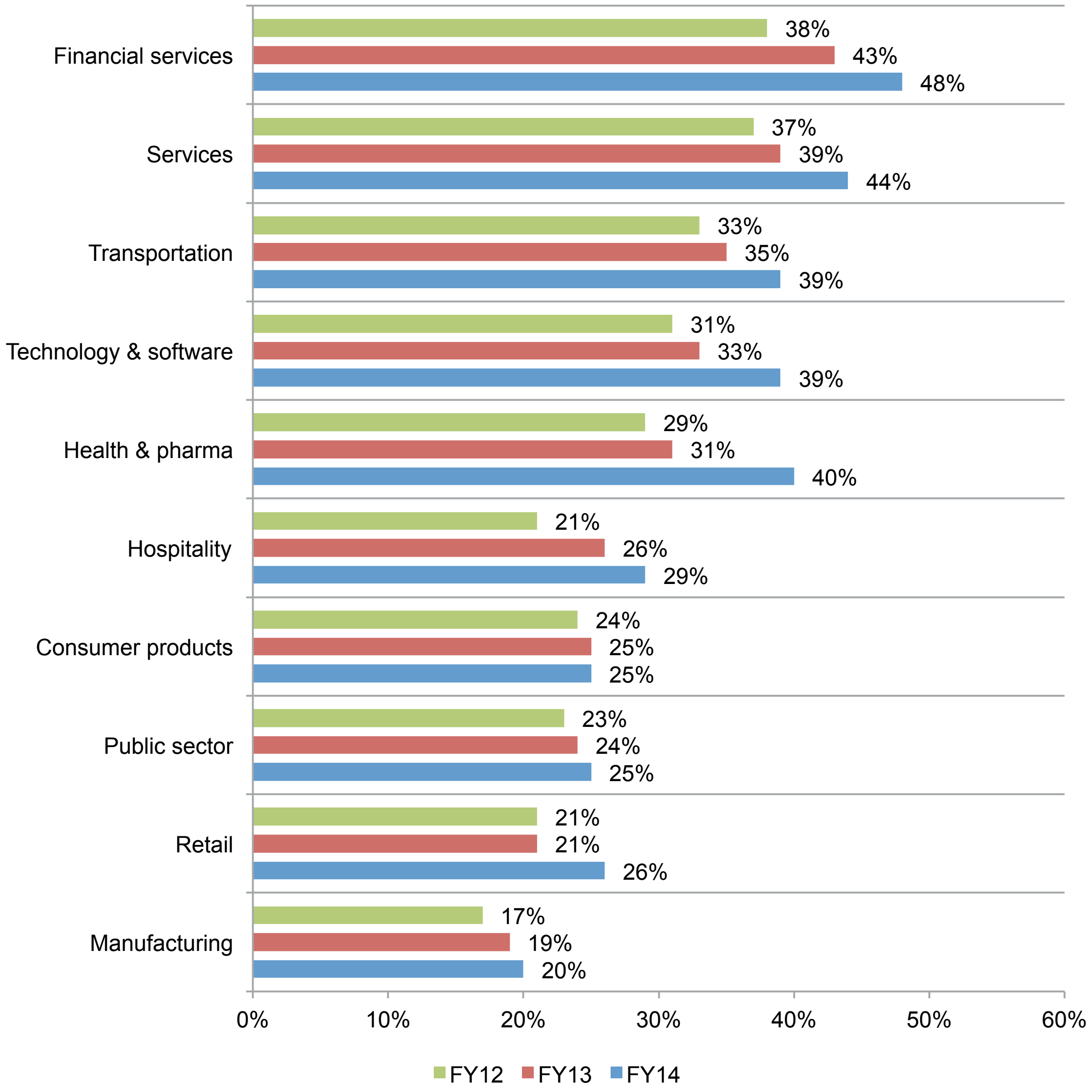


Figure 8 shows the extensive usage of encryption solutions for 10 industry sectors over three years. Results suggest a steady increase in all industry sections. The most significant increases in encryption usage occur in health and pharmaceutical and retail.

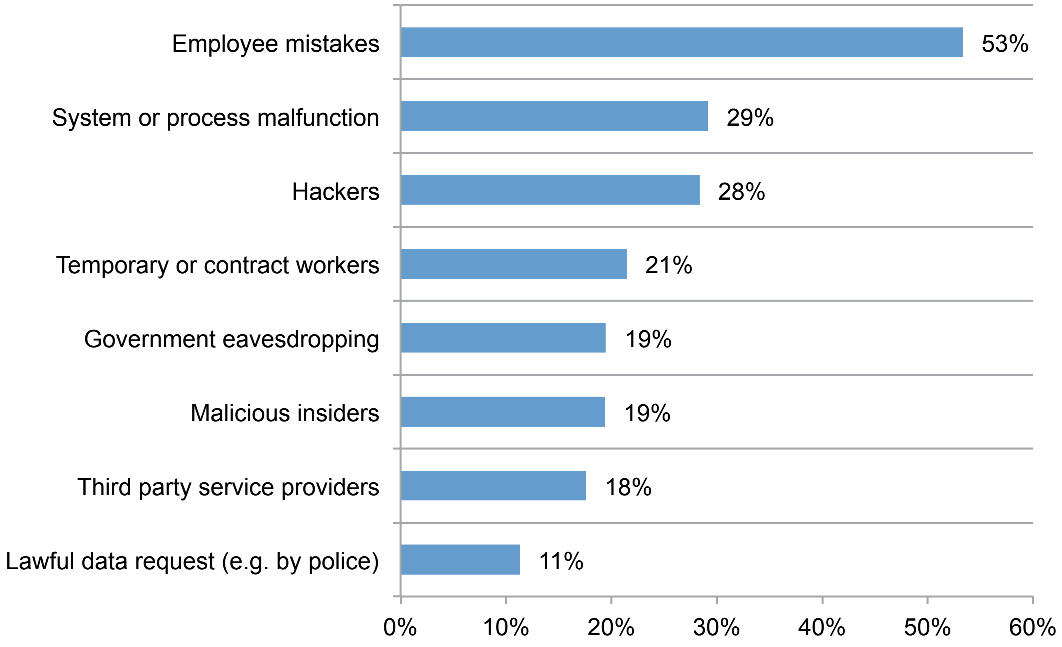
Figure 8. The extensive use of encryption by industry
Average of 13 encryption categories



Threats, main drivers and priorities

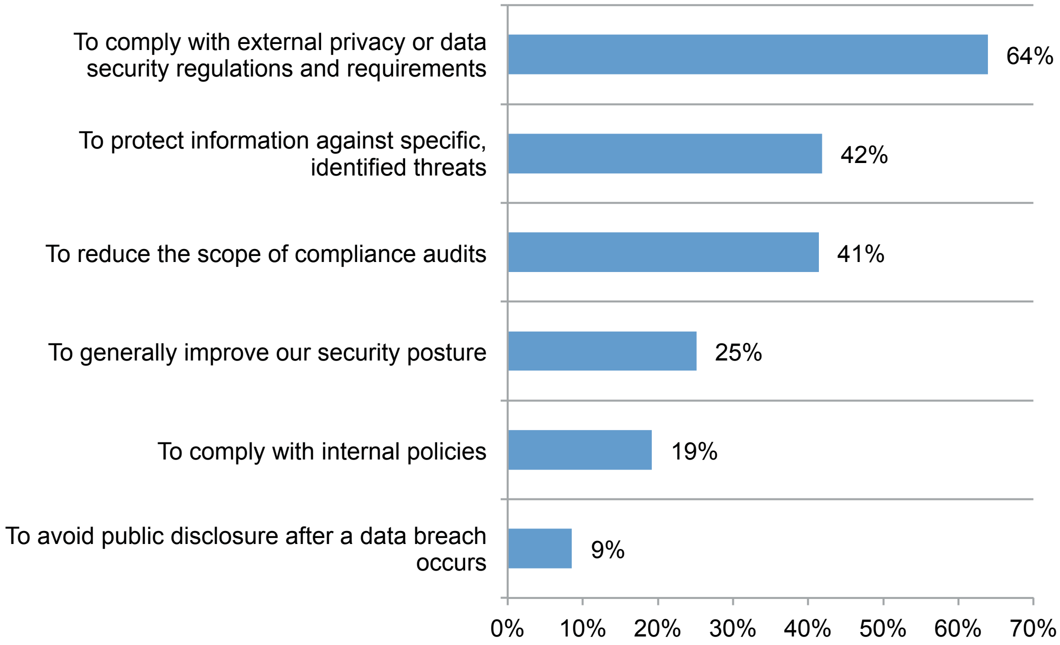
Figure 9 shows the most significant threats to the exposure of sensitive or confidential data are employee mistakes, system process malfunctions and hackers. In contrast, the least significant threats to the exposure of sensitive or confidential data include third-party service providers and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) outweigh concerns over actual attacks by hackers and malicious insiders.

Figure 9. The most salient threats to sensitive or confidential data
More than one choice permitted



Sixty-four percent see compliance with privacy and data security requirements as the main driver to using encryption technologies. Six drivers for deploying encryption are presented in Figure 10. Respondents report compliance with regulations and protecting the organization against specific threats are the two top reasons for using encryption technologies. The least significant drivers include avoiding data breach disclosures and compliance with internal policies.

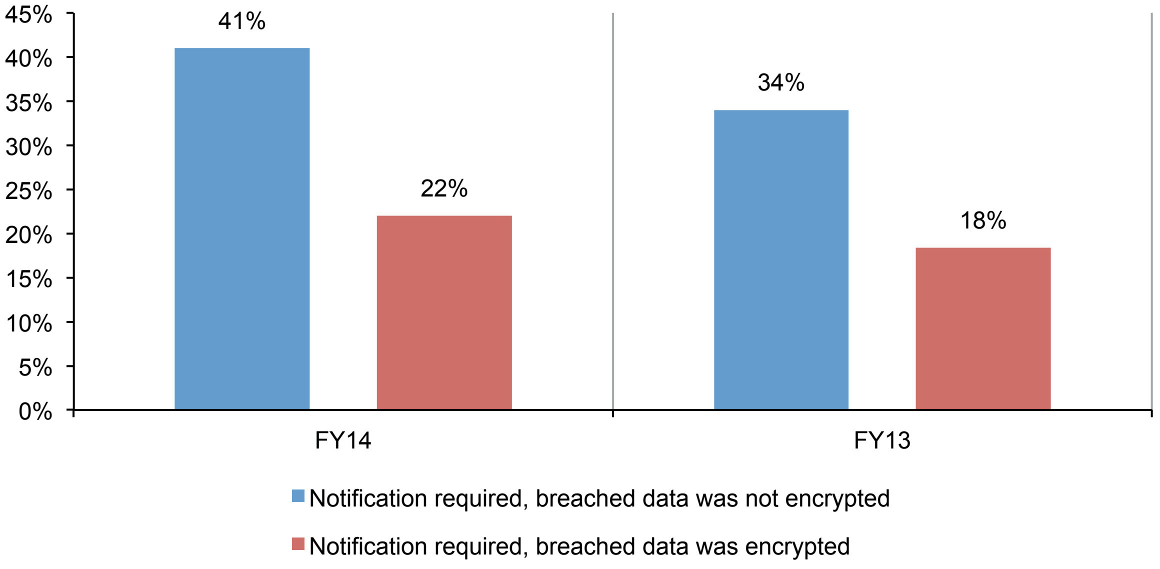
Figure 10. The main drivers for using encryption technology solutions
More than one choice permitted



Respondents believe data encryption reduces their organization's obligation to notify individuals in the event of data loss or theft. Figure 11 shows the results from a question asking respondents "Would your organization be required to notify customers after the data breach involving the loss or theft of their personal information?"

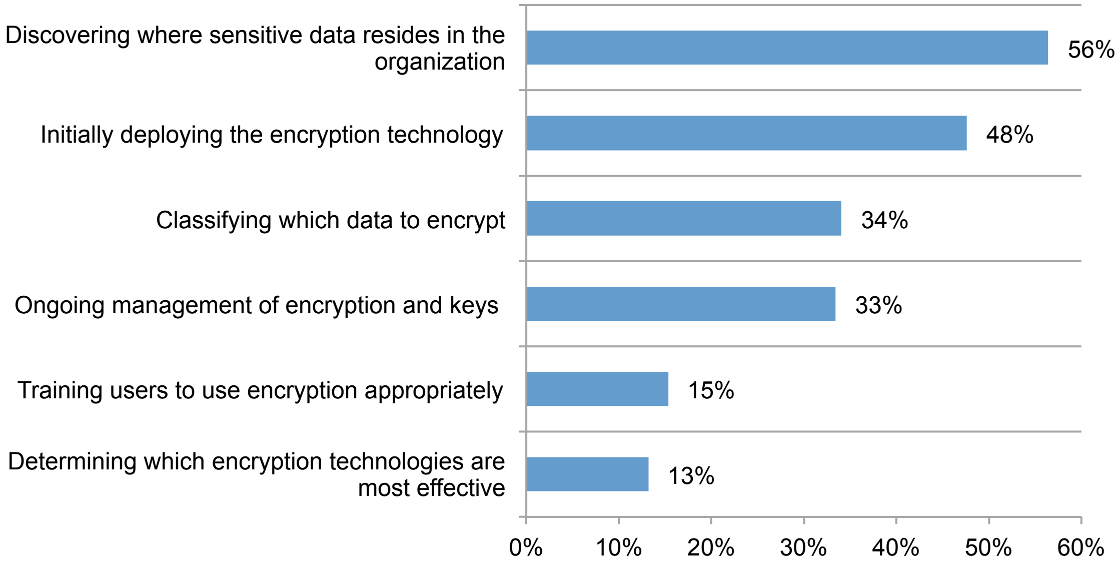
This question presented two separate conditions: (1) breached data is encrypted and (2) breach data is not encrypted. As can be seen, respondents recognize that data encryption minimizes notification requirements to breach victims. The overall average response to notification in the case of unencrypted data loss is 22 percent in 2014 and 18 percent in 2013.

Figure 11. Would a data breach of customers' personal data require notification?



Discovering where sensitive data resides in the organization is the biggest challenge. Figure 12 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-six percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 48 percent of all respondents cite deploying encryption technology as a significant challenge.

Figure 12. Biggest challenges in planning and executing a data encryption strategy
Two choices permitted

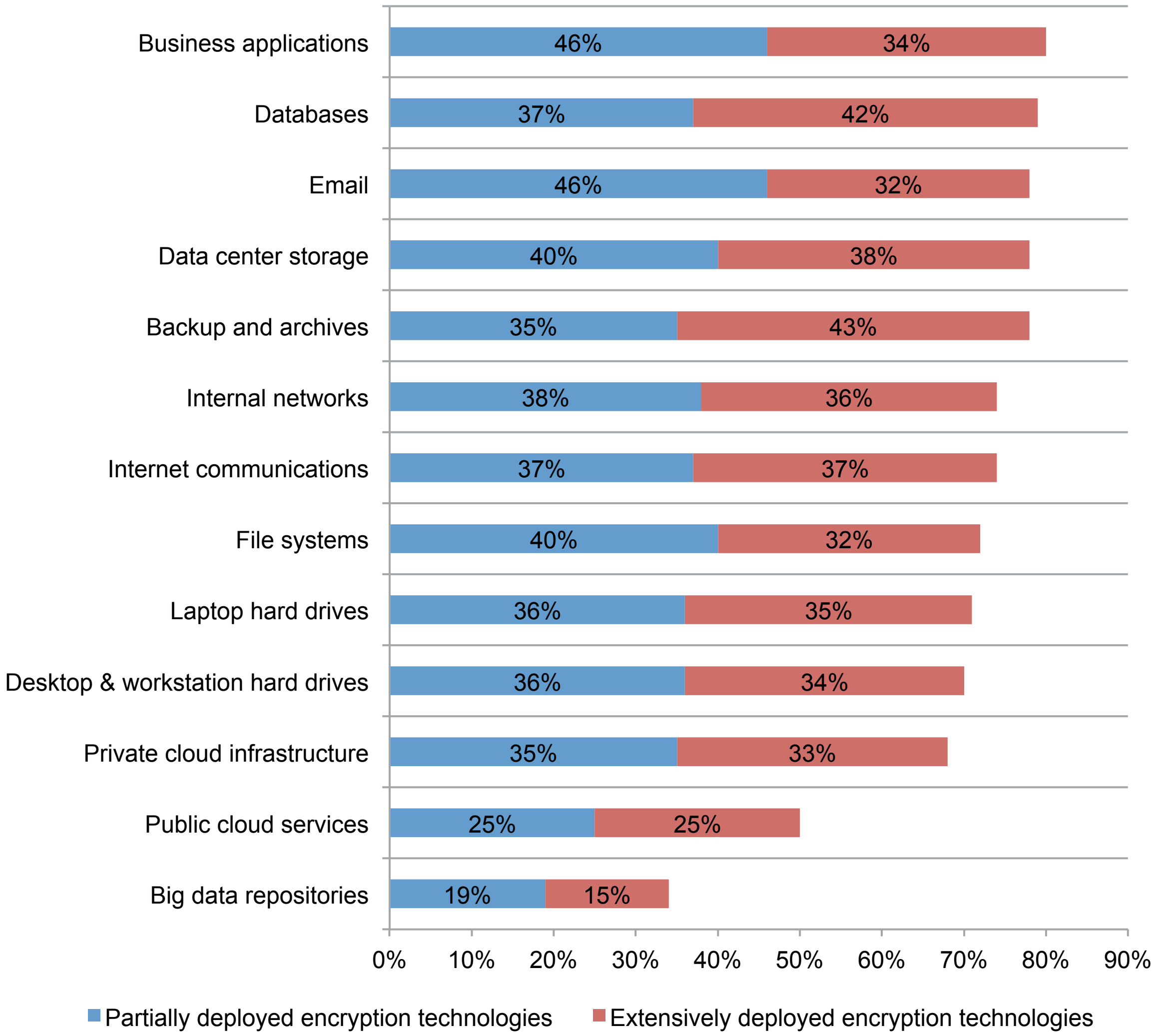


Deployment choices and decision criteria

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 13, no single technology dominates because organizations have very diverse deployments. Encryption of business applications, databases, email and data center storage are the most likely to be deployed. In contrast, encryption of big data repositories, public cloud services and private cloud infrastructure are the least likely to be deployed.

Figure 13. Consolidated view on the use of encryption technologies



The use of encryption varies among countries. Figure 14 reports the extensive and partial deployment of 13 encryption technologies for 10 countries. As shown, respondents in Germany Japan and the US have the highest deployment rates. Mexico and Brazil have the lowest deployment rates.

Figure 14. Extensive and partial deployment of data encryption technologies

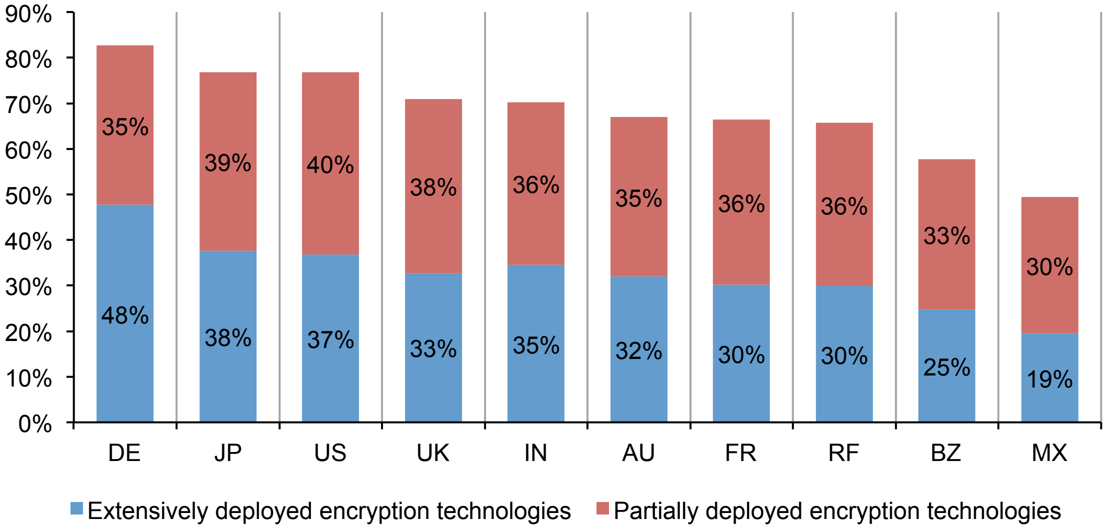
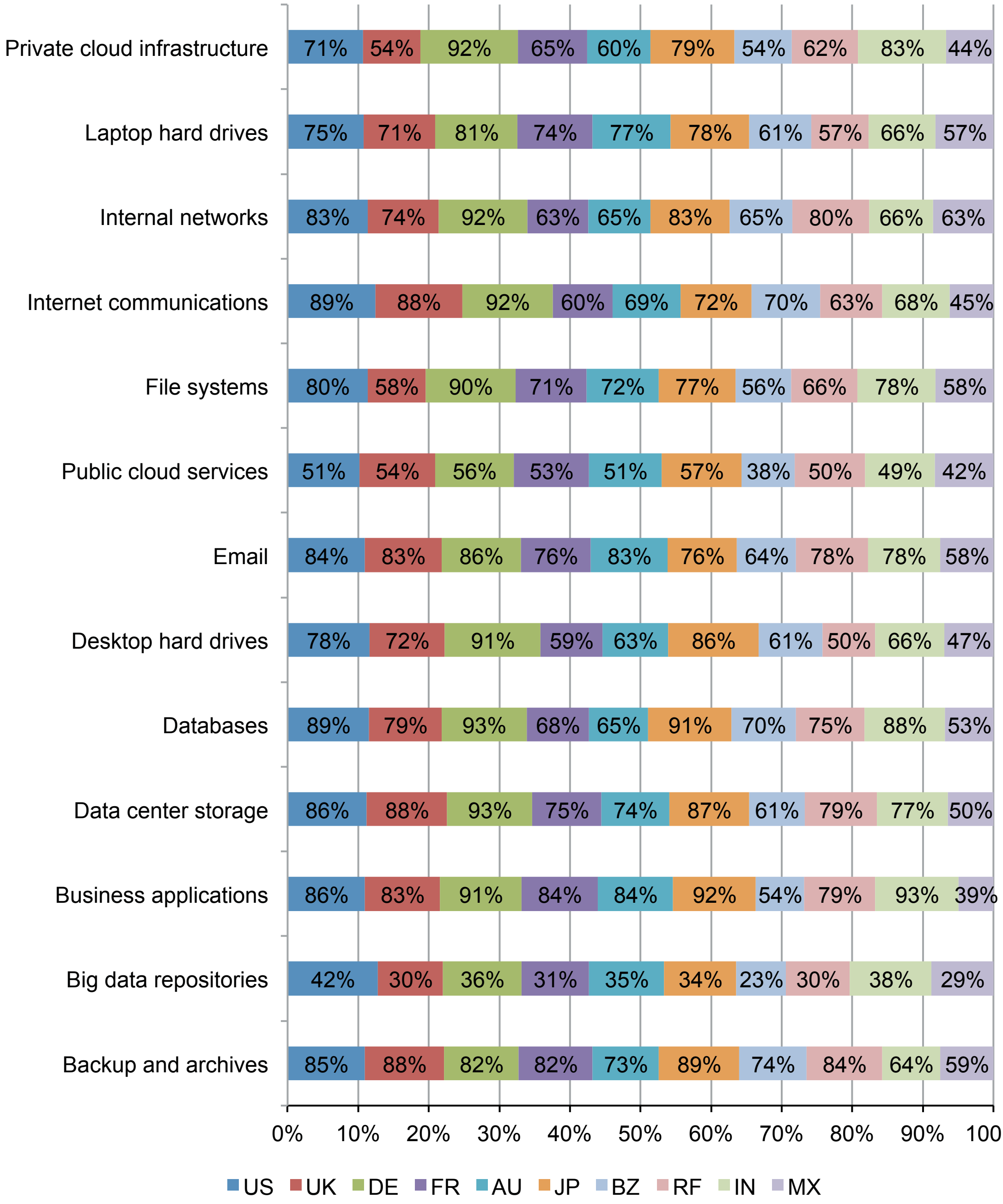


Figure 15 presents a proportional analysis of 13 encryption technologies both extensively and partially deployed within 10 country samples. Please note that the percentage shown in each cell represents the total usage rate.

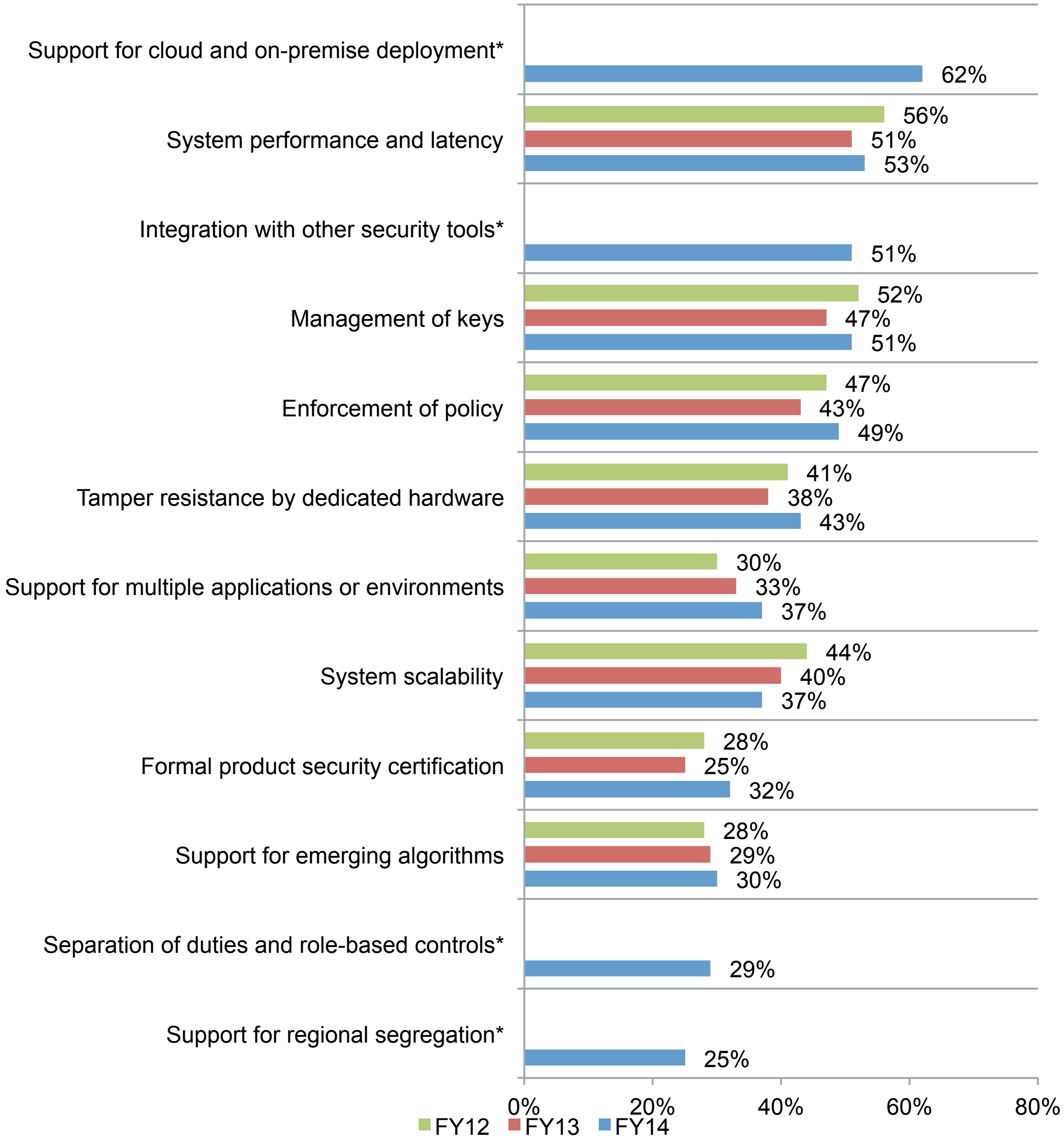
Figure 15. The use of 13 encryption technologies by country



Encryption features considered most important

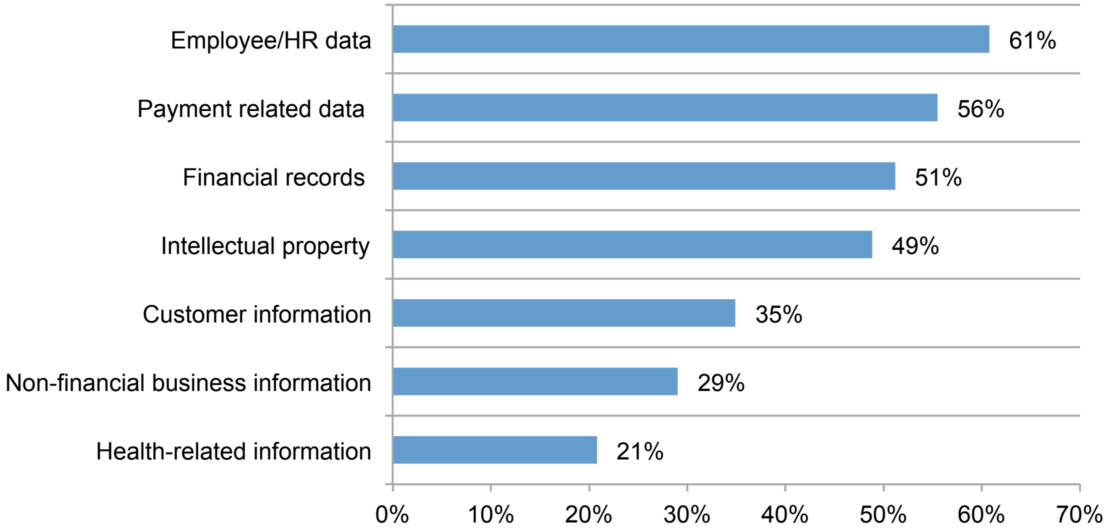
Figure 16 lists 12 encryption technology features. Each percentage defines the very important response. Respondents were asked to rate encryption technology features considered most important to their organization's security posture. According to consolidated findings, support for cloud and on-premise deployment, system performance and latency and integration with other security tools are the three most important features.

Figure 16. Most important features of encryption technology solutions
Very important response
More than one choice permitted
*Historic data is not available



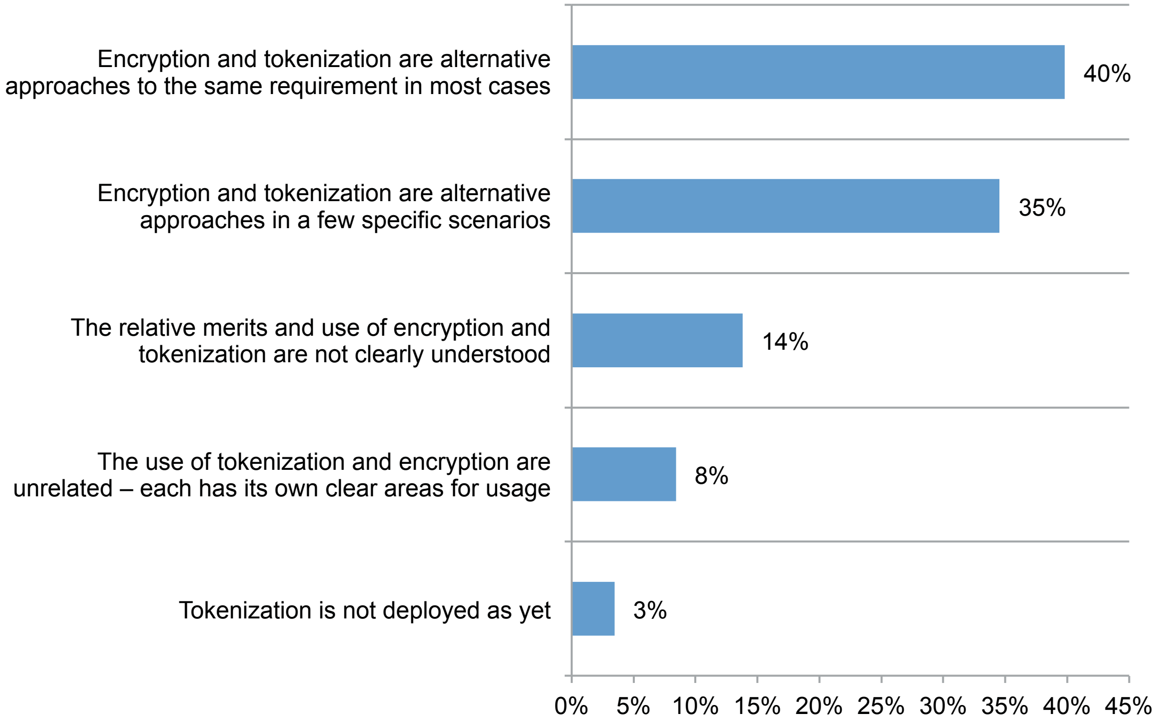
Encryption of data types. Figure 17 provides a list of 7 data types that are routinely encrypted by respondents' organizations. As can be seen, human resource data is the most likely data type to be encrypted. The least likely data type is health-related information, which is a surprising result given the sensitivity of health information and recent high profile healthcare data breaches.

Figure 17. Data types routinely encrypted.
More than one choice permitted



Perceptions about tokenization. Figure 18 compares how respondents view tokenization versus the use of encryption. Forty percent see encryption and tokenization as alternative approaches in most cases. Only 8 percent of respondents see the use of tokenization and encryption as unrelated – each having its own clear areas of usage.

Figure 18. How do you compare the use of tokenization by your organization to the use of encryption?



Attitudes about key management

Using a 10-point scale, respondents were asked to rate the overall "pain" associated with managing keys or certificates within their organization, where 1 = minimal impact to 10 = severe impact. Figure 24 clearly shows that 56 (23+33) percent of respondents chose ratings at or above seven – suggesting a fairly high pain threshold.

Figure 19. Rating on the overall impact, risk and cost associated with managing keys or certificates.

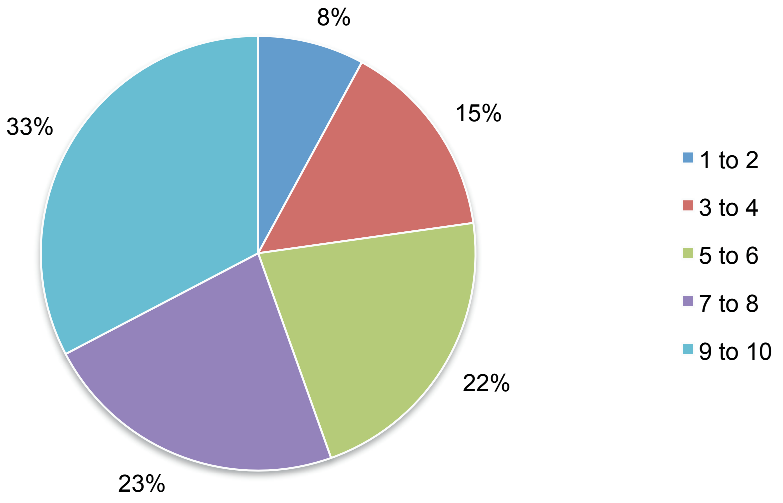
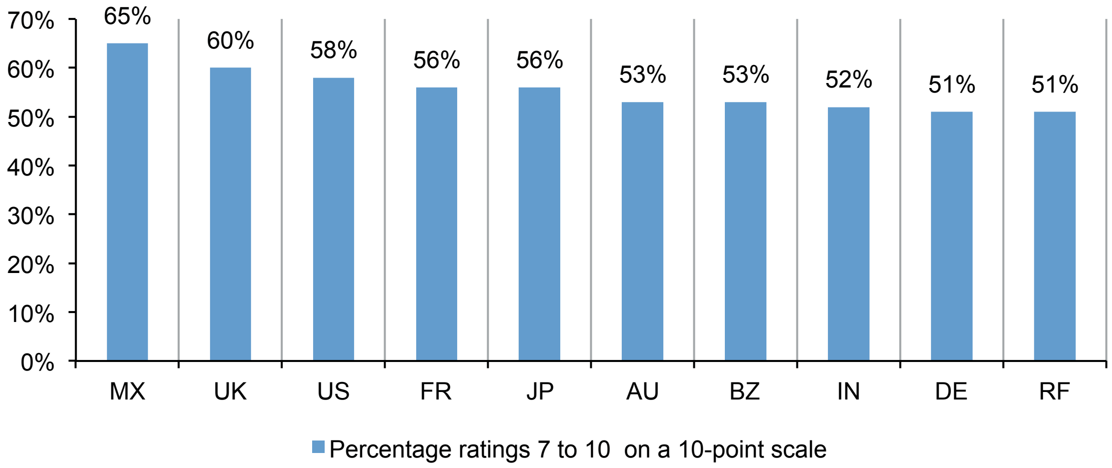


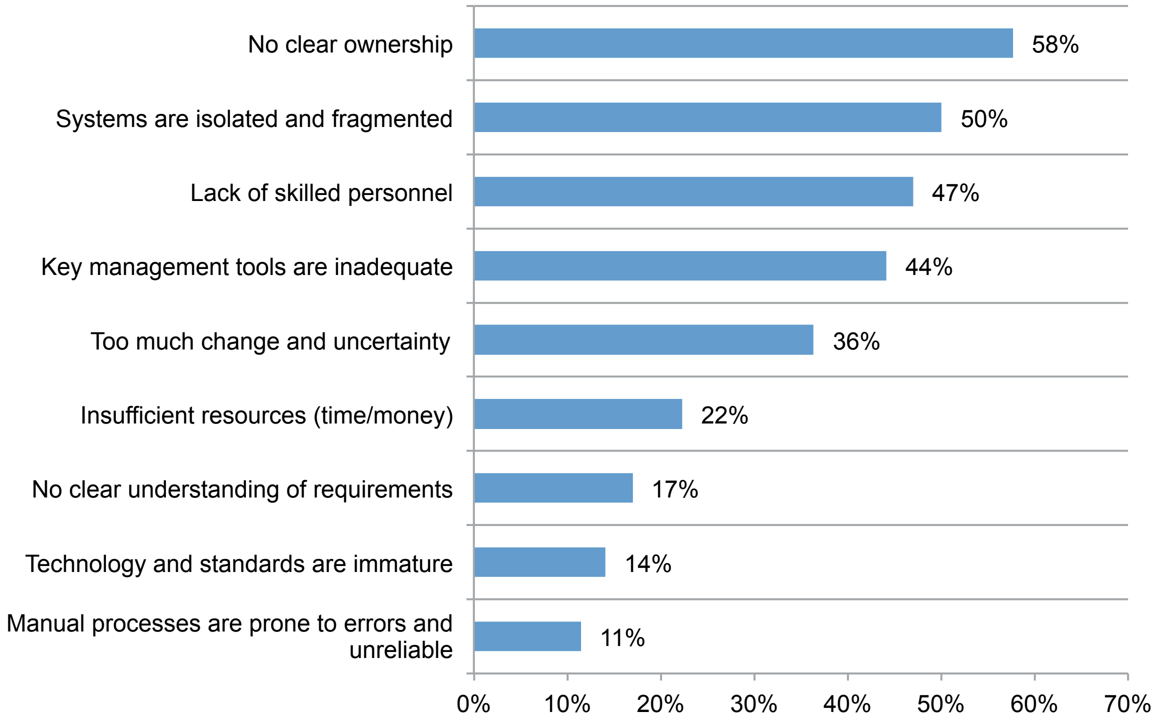
Figure 20 shows the so-called "pain threshold" – *which is defined as the percentage of 7 to 10 ratings* on a 10-point scale for each country. As can be seen, the average percentage in all country samples is above 50 percent, which suggests respondents view managing keys and certificates as a very challenging activity. The highest percentage pain threshold of 65 percent occurs in Mexico. At 51 percent, the lowest pain threshold occurs in Russia and Germany.

Figure 20. Percentage "pain threshold" by country
Percentage 7 to 10 rating on a 10-point scale



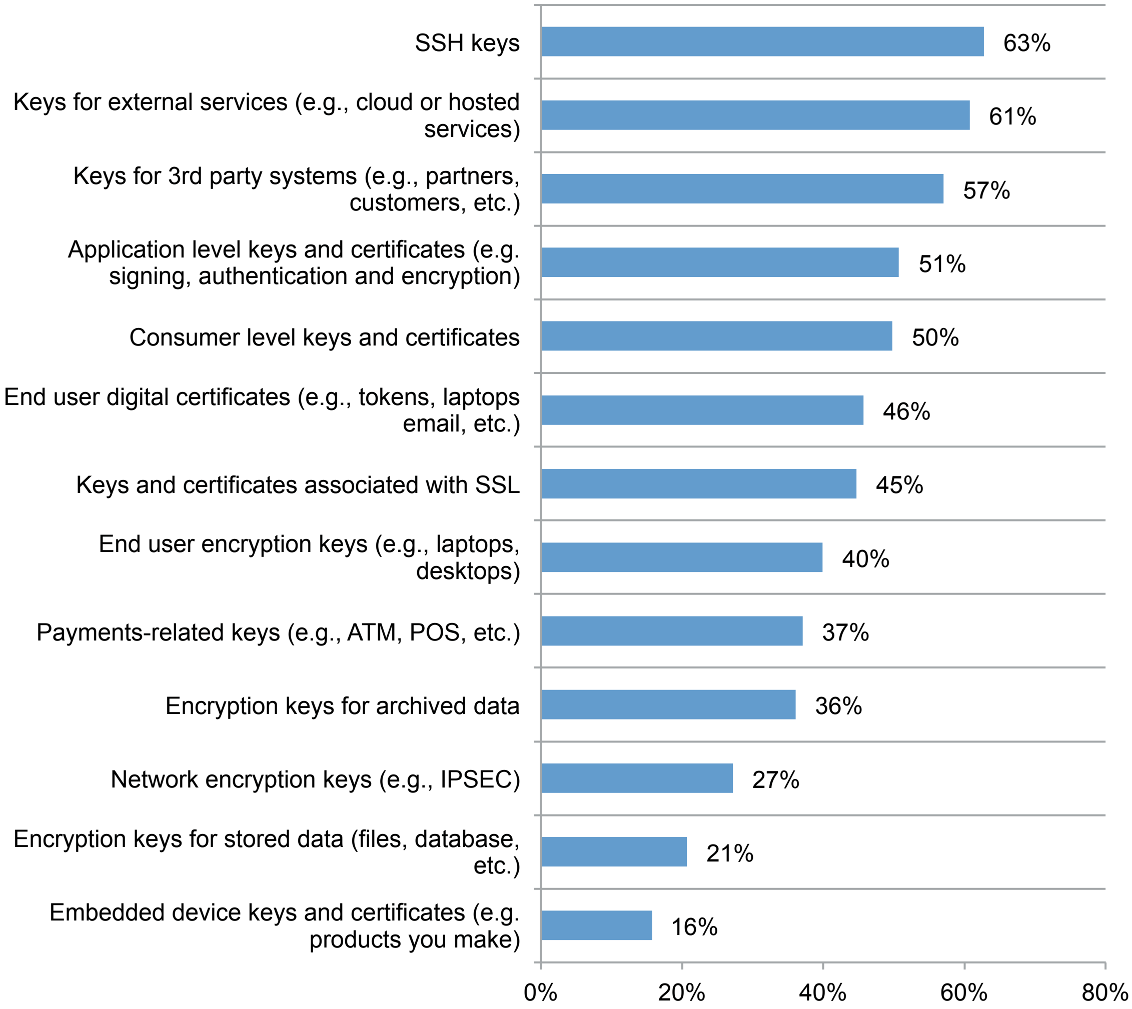
According to Figure 21, the top three reasons why the management of keys and certificates is so difficult includes (1) no clear ownership of the key management function, (2) isolated or fragmented key management systems and (3) lack of skilled personnel.

Figure 21. What makes the management of keys and certificates so painful?
More than one choice permitted



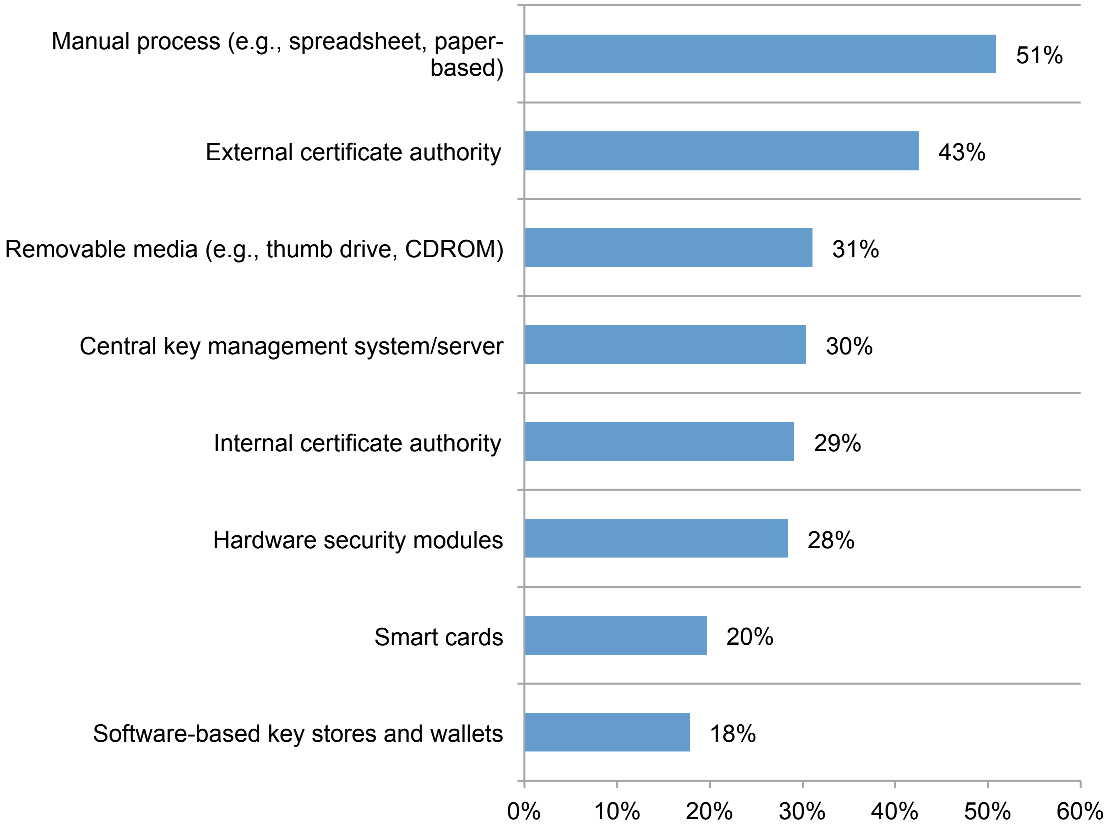
According to Figure 22, the types of keys that are viewed as most difficult to manage include: (1) SSH keys, (2) keys for external services and (3) keys for third-party systems. The least difficult include: (1) embedded device keys and certificates, (2) encryption keys for stored data and (3) network encryption keys.

Figure 22. Types of keys most difficult to manage
Very painful and painful response
More than one choice permitted



As shown in Figure 23, respondents' companies use a wide range of key management systems. The most commonly deployed systems include manual processes, external certificate authorities, removable media and central key management systems/servers.

Figure 23. What key management systems does your organization presently use?
More than one response permitted

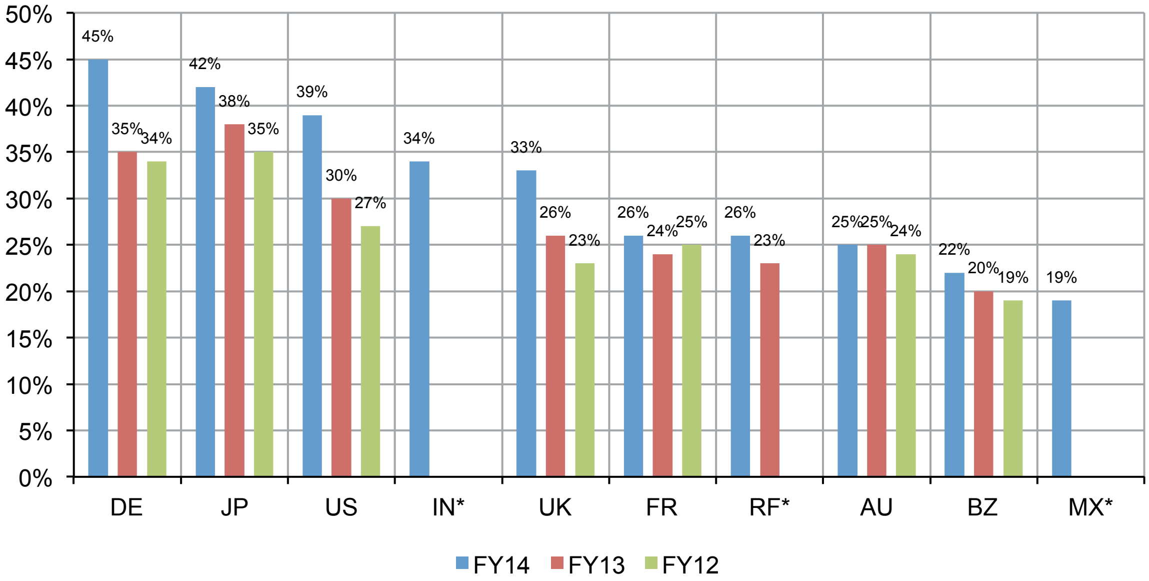


Importance of hardware security modules (HSM)[5]

Figure 24 summarizes the percentage of respondents in 10 countries that deploy HSMs as part of their organization's key management program or activities. As can be seen, the rate of HSM deployment increased in all countries between 2013 and 2014.

Similar to last year, the pattern of responses suggest respondents in Germany, Japan and the US 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 this year is 33 percent – representing a five percent growth from last year's average deployment rate.

Figure 24. Deployment HSMs as part of key management activities
*Historical data is not available



[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 25 summarizes the percentage of respondents in 10 countries that rate HSM as either very important or important to their organization's key management program or activities. It is interesting to note that the importance level appears to be increasing between 2012 and 2014.

Similar to last year, the pattern of responses suggests German, Japanese and US respondents are most likely to assign importance to HSMs as part of their organization's key management activities. The overall average importance rating in the current year is 48 percent. Last year's average importance rating was 45 percent.

Figure 25. Perceived importance of HSM as part of key management activities
Important & very important response
*Historical data is not available

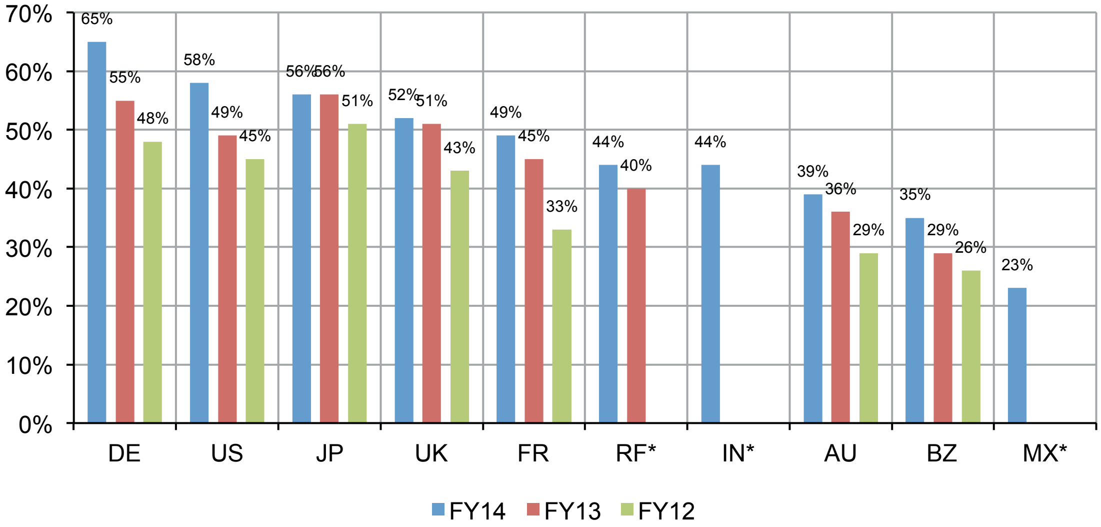
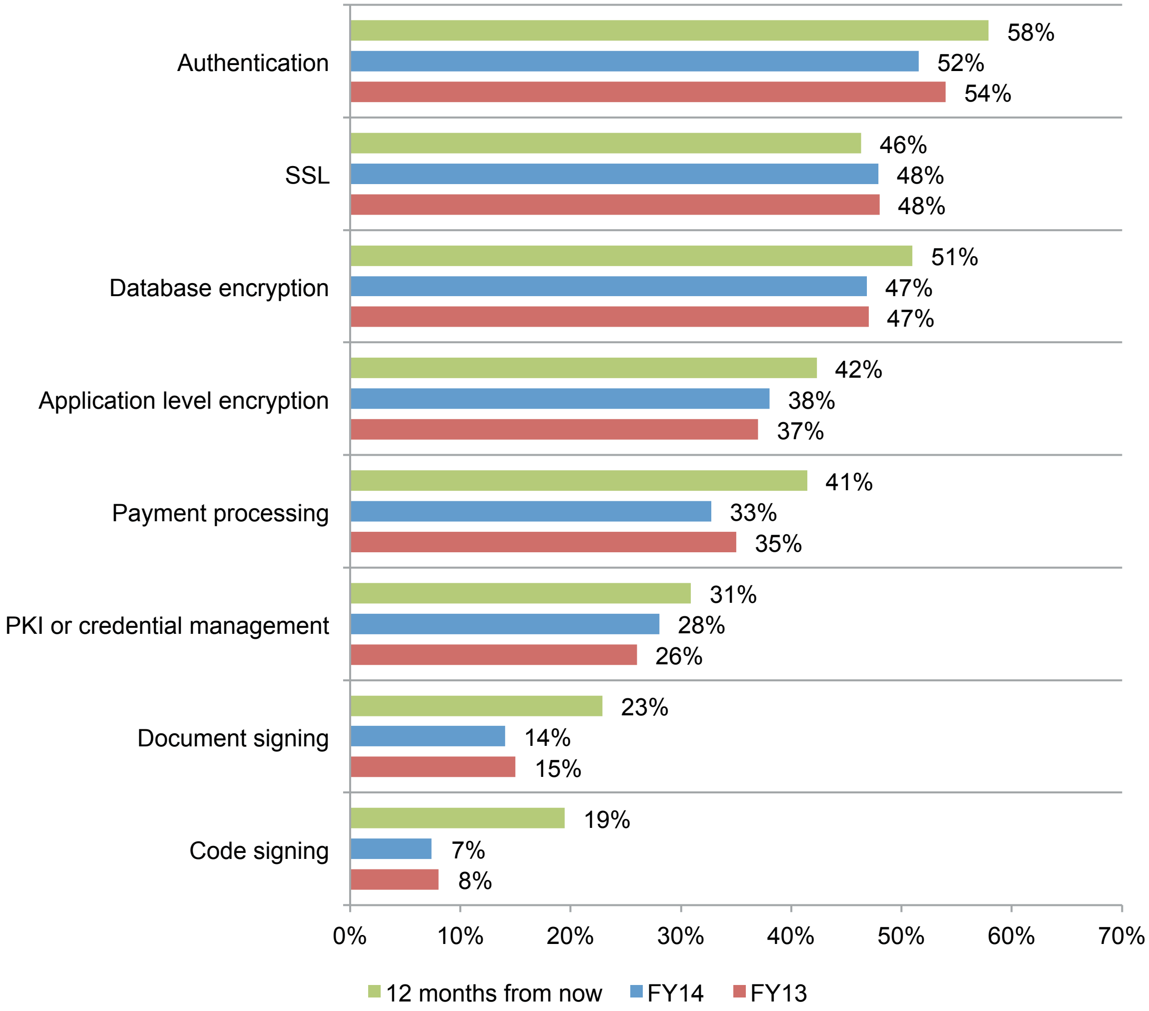


Figure 26 summarizes the primary purpose or use cases for deploying HSMs. As can be seen, the number one purpose is authentication followed by SSL and database encryption. This chart also shows differences between today's HSM use and deployment in 12 months. The most significant increases predicted for the next 12 months, according to respondents, are code signing, document signing and payment processing.

Figure 26. How HSMs are deployed or planned to be deployed in the next 12 months
More than one choice permitted

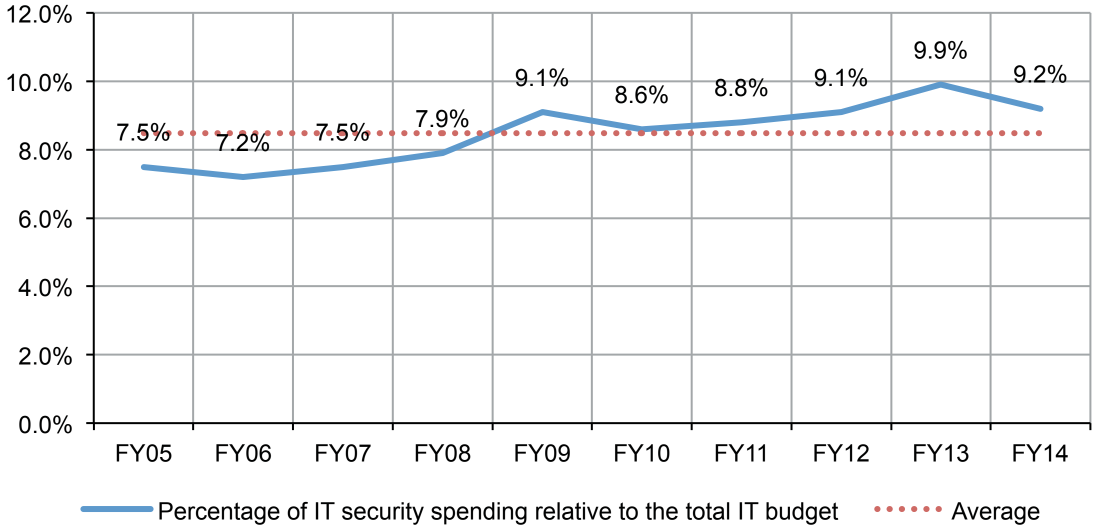


Budget allocations

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.

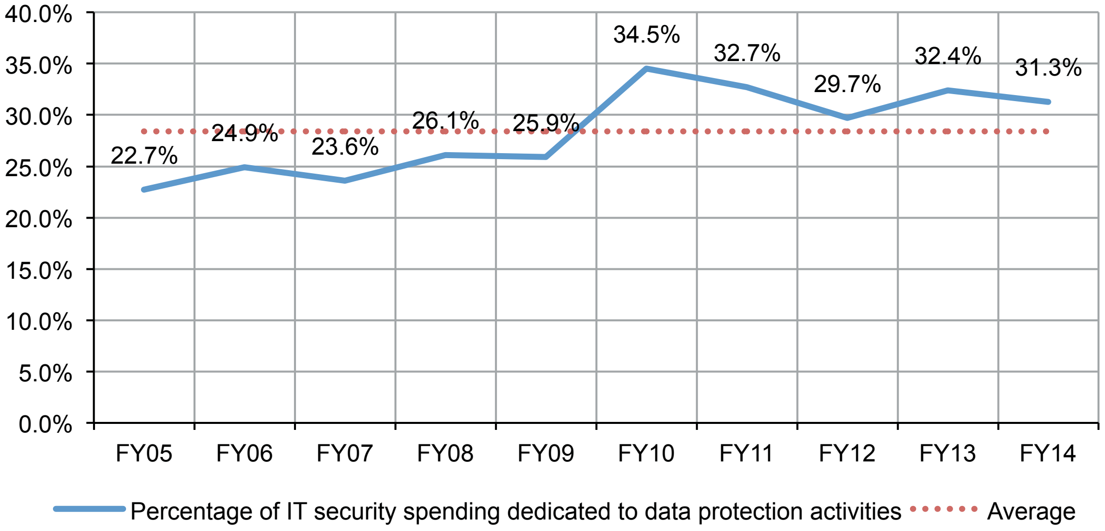
Figure 26 reports the average percentage of IT security spending relative to total IT spending over the last 10 years. As shown, the trend appears to be upper sloping, which suggests the proportion of IT spending dedicated to security activities including encryption is increasing over time.

Figure 26. Trend in the percent of IT security spending relative to the total IT budget



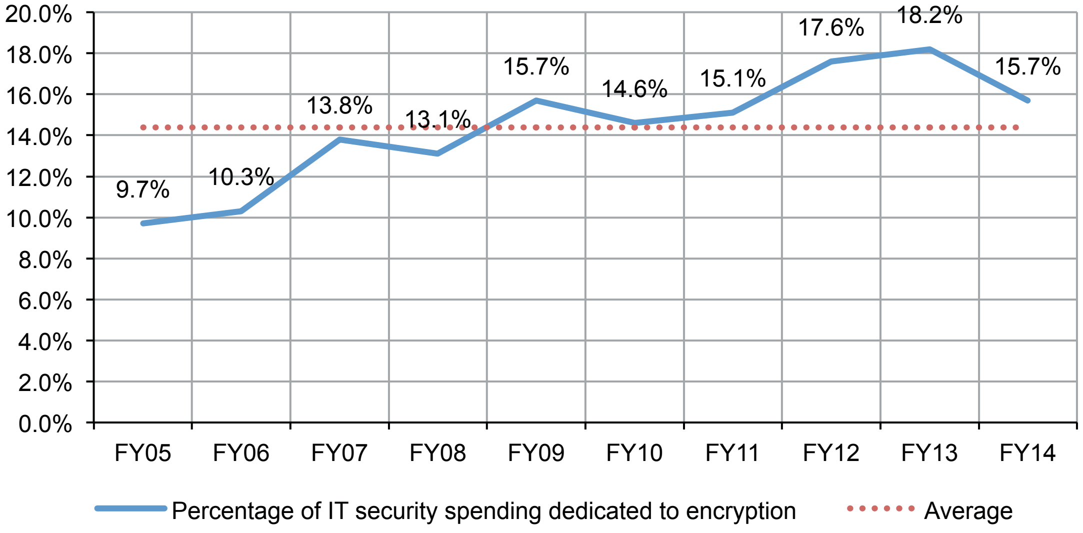
Budget allocated to data protection. Figure 27 reports the percentage of data protection spending relative to the total IT security budget over nine years. This trend appears to be slightly upward sloping, which suggests data protection spending as a proportion of total IT security is on the rise.

Figure 27. Trend in the percent of IT security spending dedicated to data protection activities



Budget allocated to encryption. Figure 28 reports the nine-year trend in the percentage of encryption spending relative to the total IT security budget. Again, the trend appears to be increasing from a low of 9.7 percent in 2005 to 18.2 percent in 2013. Note that this percentage decreased to 15.7 percent in the present year's study.

Figure 28. Trend in the percent of IT security budget dedicated to encryption



Part 3. Methods & Limitations

Table 1 reports the sample response for 10 separate country samples. The sample response for this study was conducted over a 55-day period ending in February 2015. Our consolidated sampling frame of practitioners in all countries consisted of 136,123 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 5,297 returns of which 583 were rejected for reliability issues. Our final consolidated 2014 sample was 4,714, thus resulting in an overall 3.5% 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 10 separate country samples. Trend analysis was performed on combined country samples. As noted before, we added Mexico and India to this year's study.

The respondents' average (mean) experience in IT, IT security or related fields is 8.9 years. Approximately 28 percent of respondents are female and 72 percent male.[6]

Table 1. Survey response in 10 countries

Legend	Survey response	Sampling frame	Final sample	Response rate
US	United States	24,513	789	3.2%
IN	India	16,944	532	3.1%
DE	Germany	14,997	564	3.8%
BZ	Brazil	14,457	472	3.3%
UK	United Kingdom	14,062	509	3.6%
FR	France	13,986	375	2.7%
JP	Japan	13,005	476	3.7%
MX	Mexico	10,560	445	4.2%
AU	Australia	7,980	359	4.5%
RF	Russian Federation	5,619	193	3.4%

Table 2 summarizes the structure of our survey samples for 10 countries over a 10-year period.

Table 2. Sample history over 10 years

Legend	FY14	FY13	FY12	FY11	FY10	FY09	FY08	FY07	FY06	FY05
AU	359	414	938	471	477	482	405	0	0	0
BZ	472	530	637	525	0	0	0	0	0	0
DE	564	602	499	526	465	490	453	449	0	0
FR	375	478	584	511	419	414	0	0	0	0
IN	532	0	0	0	0	0	0	0	0	0
JP	476	521	466	544	0	0	0	0	0	0
MX	445	0	0	0	0	0	0	0	0	0
RF	193	201	0	0	0	0	0	0	0	0
UK	509	637	550	651	622	615	638	541	489	0
US	789	892	531	912	964	997	975	768	918	791
Total	4714	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 10 countries sampled.

Figure 29 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 29. Distribution of respondents according to position level
Consolidated from 10 separate country samples

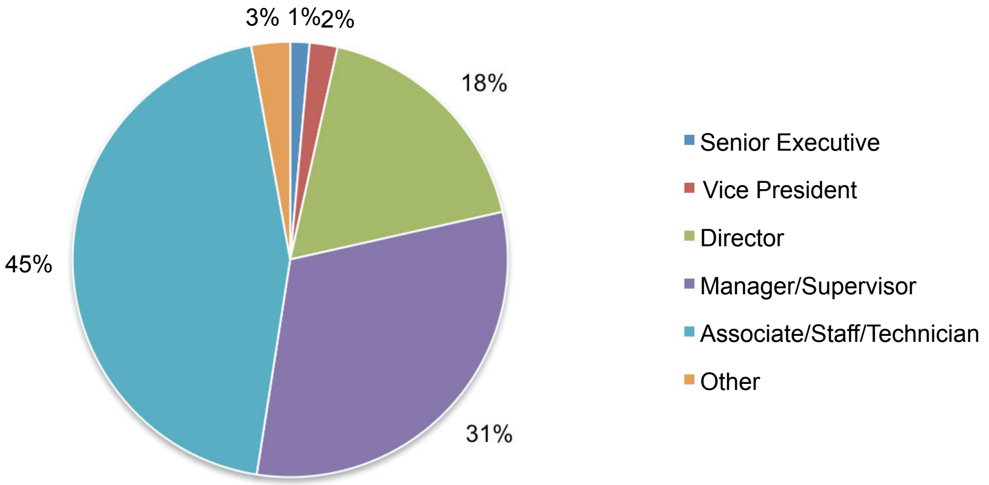
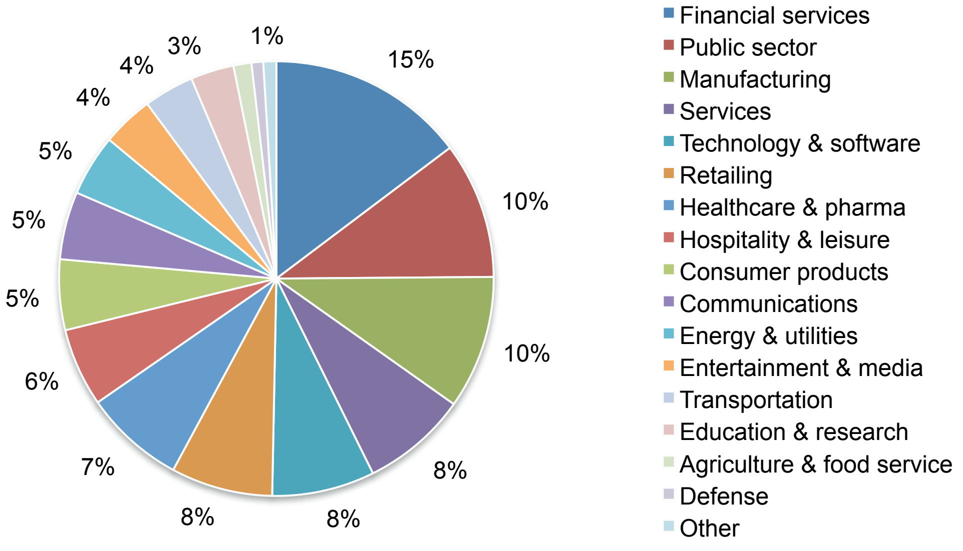


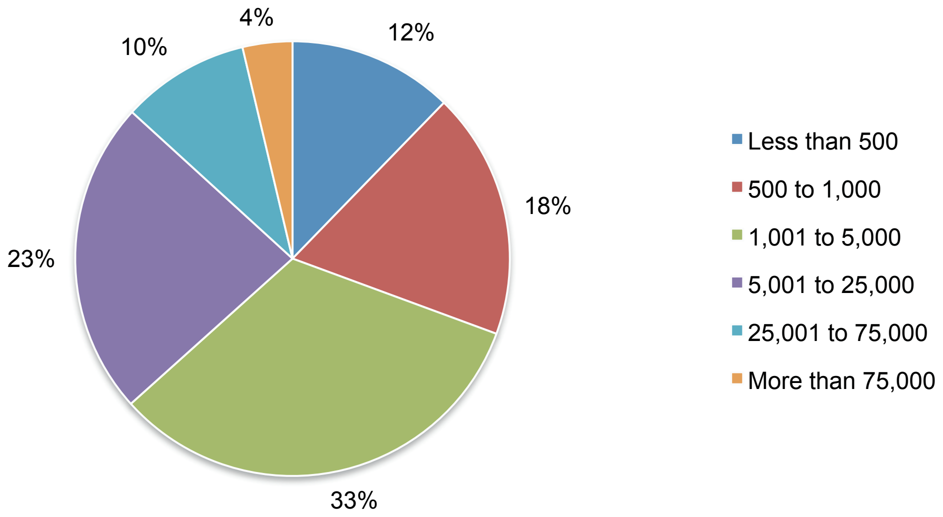
Figure 30 reports the respondents' organizations primary industry segments. As shown, 15 percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 10 percent are located in public sector organizations, including central and local government and manufacturing.

Figure 30. Distribution of respondents according to primary industry classification
Consolidated from ten separate country samples



According to Figure 31, the majority of respondent are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 31. Distribution of respondents according to organizational headcount
Consolidated for ten separate country samples



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 10 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 10 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 1: Survey Data Tables

The following tables provide the consolidated results for 10 country samples.

Survey response	Consolidated
Sampling frame	136,123
Total returns	5,297
Rejected or screened surveys	583
Final sample	4,714
Response rate	3.5%
Sample weights	1.00

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.	36%
We have an overall encryption plan or strategy that is adjusted to fit different applications and data types.	26%
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.	23%
We don't have an encryption plan or strategy.	15%
Total	100%

Extensively deployed encryption technologies	Consolidated
Q2a-1 Backup and archives	43%
Q2b-1. Big data repositories	15%
Q2c-1. Business applications	34%
Q2d-1. Data center storage	38%
Q2e-1. Databases	42%
Q2f-1. Desktop & workstation hard drives	34%
Q2g-1. Email	32%
Q2h-1. Public cloud services	25%
Q2i-1. File systems	32%
Q2j-1. Internet communications (e.g., SSL)	37%
Q2k-1. Internal networks (e.g., VPN/LPN)	36%
Q2l-1. Laptop hard drives	35%
Q2m-1 Private cloud infrastructure	33%
Average	34%

Partially deployed encryption technologies	Consolidated
Q2a-1 Backup and archives	35%
Q2b-1. Big data repositories	19%
Q2c-1. Business applications	46%
Q2d-1. Data center storage	40%
Q2e-1. Databases	37%
Q2f-1. Desktop & workstation hard drives	36%
Q2g-1. Email	46%
Q2h-1. Public cloud services	25%
Q2i-1. File systems	40%
Q2j-1. Internet communications (e.g., SSL)	37%
Q2k-1. Internal networks (e.g., VPN/LPN)	38%
Q2l-1. Laptop hard drives	36%
Q2m-1 Private cloud infrastructure	35%
Average	36%

Total deployment of encryption technologies	**Consolidated**
Q2a-1 Backup and archives	78%
Q2b-1. Big data repositories	34%
Q2c-1. Business applications	80%
Q2d-1. Data center storage	78%
Q2e-1. Databases	79%
Q2f-1. Desktop & workstation hard drives	70%
Q2g-1. Email	77%
Q2h-1. Public cloud services	50%
Q2i-1. File systems	72%
Q2j-1. Internet communications (e.g., SSL)	74%
Q2k-1. Internal networks (e.g., VPN/LPN)	74%
Q2l-1. Laptop hard drives	71%
Q2m-1 Private cloud infrastructure	68%
Average	70%

Are you directly involved in deployment? % Yes response	**Consolidated**
Q2a-1 Backup and archives	48%
Q2b-1. Big data repositories	11%
Q2c-1. Business applications	41%
Q2d-1. Data center storage	60%
Q2e-1. Databases	52%
Q2f-1. Desktop & workstation hard drives	34%
Q2g-1. Email	39%
Q2h-1. Public cloud services	19%
Q2i-1. File systems	32%
Q2j-1. Internet communications (e.g., SSL)	51%
Q2k-1. Internal networks (e.g., VPN/LPN)	39%
Q2l-1. Laptop hard drives	34%
Q2m-1 Private cloud infrastructure	19%

Q3. What best describes your organization’s approach to using encryption? Please select one best choice.	**Consolidated**
Strategic (e.g. centrally defined)	33%
Tactical (e.g. driven by individual requirements)	67%
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	18%
IT operations	36%
Finance	3%
Lines of business (LOB) or general management	23%
Security	18%
Compliance	2%
Total	100%

Q5. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top two reasons.	**Consolidated**
To avoid public disclosure after a data breach occurs	9%
To protect information against specific, identified threats	42%
To generally improve our security posture	25%
To comply with internal policies	19%
To comply with external privacy or data security regulations and requirement	64%
To reduce the scope of compliance audits	41%
Total	200%

Q6. In your opinion, would your organization be required to notify customers after the data breach involving the loss or theft of their personal information?

Q6a. If the data that was lost or stolen was not encrypted	Consolidated
Yes	41%
No	47%
Unsure	11%
Total	100%

Q6b. If the data that was lost or stolen was encrypted	Consolidated
Yes	22%
No	68%
Unsure	11%
Total	100%

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	56%
Classifying which data to encrypt	34%
Determining which encryption technologies are most effective	13%
Initially deploying the encryption technology	48%
Ongoing management of encryption and keys	33%
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	69%
Support for multiple applications or environments	54%
Separation of duties and role-based controls	53%
System scalability	67%
Tamper resistance by dedicated hardware (e.g., HSM)	56%
Integration with other security tools (e.g., SIEM and ID management)	59%
Support for regional segregation (e.g., data residency)	42%
System performance and Latency	73%
Support for emerging algorithms (e.g., ECC)	67%
Support for cloud and on-premise deployment	72%
Formal product security certification (e.g., FIPS 140)	55%

Q9. What types of data does your organization encrypt? Please select all that apply.	Consolidated
Customer information	35%
Non-financial business information	29%
Intellectual property	49%
Financial records	51%
Employee/HR data	61%
Payment related data	56%
Health-related information	21%

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	19%
System or process malfunction	29%
Employee mistakes	53%
Temporary or contract workers	21%
Third party service providers	18%
Lawful data request (e.g. by police)	11%
Government eavesdropping	19%
Total	200%

Q11a. What best describes your level of knowledge about tokenization?	Consolidated
Very knowledgeable	47%
Knowledgeable	27%
Not knowledgeable	18%
No knowledge (skip to Q12)	8%
Total	100%

Q11b. How do you compare the use of tokenization by your organization to the use of encryption?	Consolidated
The use of tokenization and encryption are unrelated – each has its own clear areas for usage	8%
Encryption and tokenization are alternative approaches to the same requirement in most cases	40%
Encryption and tokenization are alternative approaches in a few specific scenarios	35%
The relative merits and use of encryption and tokenization are not clearly understood	14%
Tokenization is not deployed as yet	3%
Total	100%

Part 2. Key Management

Q12. 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	15%
5 or 6	22%
7 or 8	23%
9 or 10	33%
Total	100%

Q13. What makes the management of keys and certificates so painful? Please select the top three reasons.	Consolidated
No clear ownership	58%
Insufficient resources (time/money)	22%
Lack of skilled personnel	47%
No clear understanding of requirements	17%
Too much change and uncertainty	36%
Key management tools are inadequate	44%
Systems are isolated and fragmented	50%
Technology and standards are immature	14%
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 painful response combined.	**Consolidated**
Encryption keys for stored data (files, database, etc.)	21%
Encryption keys for archived data	36%
Keys and certificates associated with SSL	45%
SSH keys	63%
End user encryption keys (e.g., laptops, desktops)	40%
Network encryption keys (e.g., IPSEC)	27%
End user digital certificates (e.g., tokens, laptops email, etc.)	46%
Application level keys and certificates (e.g. signing, authentication and encryption)	51%
Payments-related keys (e.g., ATM, POS, etc.)	37%
Consumer level keys and certificates	50%
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, etc.)	57%

Q15a. What key management systems does your organization presently use? **Percentage use rate**	**Consolidated**
External certificate authority	43%
Internal certificate authority	29%
Manual process (e.g., spreadsheet, paper-based)	51%
Central key management system/server	30%
Hardware security modules	28%
Removable media (e.g., thumb drive, CDROM)	31%
Software-based key stores and wallets	18%
Smart cards	20%
Total	250%

Q15b. What key management systems does your organization presently use? **Directly involved response**	**Consolidated**
External certificate authority	36%
Internal certificate authority	54%
Manual process (e.g., spreadsheet, paper-based)	41%
Central key management system/server	43%
Hardware security modules	56%
Removable media (e.g., thumb drive, CDROM)	34%
Software-based key stores and wallets	18%
Smart cards	29%
Total	312%

Part 3. Hardware Security Modules

Q16. What best describes your level of knowledge about HSMs?	Consolidated
Very knowledgeable	29%
Knowledgeable	43%
Not knowledgeable (skip to Q19)	28%
Total	100%

Q17a. Does your organization deploy HSMs?	**Consolidated**
Yes	33%
No (skip to Q19)	67%
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	38%
Database encryption	47%
SSL	48%
PKI or credential management	28%
Document signing (e.g. electronic invoicing)	14%
Code signing	7%
Authentication	52%
Payment processing	33%
Not planning to use	9%
Total	277%

Q17b-2. HSMs planned to be deployed in the next 12 months	**Consolidated**
Application level encryption	42%
Database encryption	51%
SSL	46%
PKI or credential management	31%
Document signing (e.g. electronic invoicing)	23%
Code signing	19%
Authentication	58%
Payment processing	41%
Not planning to use	3%
Total	315%

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	48%
Q18b. Importance in the next 12 months	55%

Part 4. Budget Questions

Q19a. Are you responsible for managing all or part of your organization's IT budget this year?	**Consolidated**
Yes	57%
No (skip to Q20)	43%
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 2015 IT budget will go to IT security activities?	**Consolidated**
Extrapolated value	9.2%

Q19d. Approximately, what percentage of the 2015 IT security budget will go to data protection activities?	**Consolidated**
Extrapolated value	31.3%

Q19e. Approximately, what percentage of the 2015 IT security budget will go to encryption activities?	**Consolidated**
Extrapolated value	15.7%

Part 6: Role and organizational characteristics

D1. What organizational level best describes your current position?	**Consolidated**
Senior Executive	1%
Vice President	2%
Director	18%
Manager/Supervisor	31%
Associate/Staff/Technician	45%
Other	3%
Total	100%

D2. Check the functional area that best describes your organizational location.	**Consolidated**
IT operations	59%
Security	14%
Compliance	8%
Finance	2%
Lines of business (LOB)	13%
Other	4%
Total	100%

D3. What industry best describes your organization’s industry focus?	**Consolidated**
Agriculture & food service	1%
Communications	5%
Consumer products	5%
Defense	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	4%
Financial services	15%
Healthcare & pharma	7%
Hospitality & leisure	6%
Manufacturing	10%
Public sector	10%
Retailing	8%
Services	8%
Technology & software	8%
Transportation	4%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	**Consolidated**
Less than 500	12%
500 to 1,000	18%
1,001 to 5,000	33%
5,001 to 25,000	23%
25,001 to 75,000	10%
More than 75,000	4%
Total	100%

About the 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 trusted cryptographic solutions with a 40-year track record of protecting the world's most sensitive applications and information. Thales solutions enhance privacy, trusted identities, and secure payments with certified, high performance encryption and digital signature technology for customers in a wide range markets including financial services, high technology, manufacturing, and government. Thales e-Security has a worldwide support capability, with regional headquarters in the United States, United Kingdom, and Hong Kong. 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.

Drawing on its strong cryptographic capabilities, Thales is one of the world leaders in cybersecurity products and solutions for critical state and military infrastructures, satellite networks and industrial and financial companies. With a presence throughout the entire security chain, Thales offers a comprehensive range of services and solutions ranging from security consulting, intrusion detection and architecture design to system certification, development and through-life management of products and services, and security supervision with Security Operation Centres in France and the United Kingdom.