THALES

Ponemon INSTITUTE

2012 Global Encryption Trends Study

Organizations continue to increase their deployment of encryption across the enterprise in response to diverse threats and commercial imperatives

Sponsored by Thales e-Security

Independently conducted by Ponemon Institute LLC

Publication Date: February 2013

2012 Global Encryption Trends Study

2012 Global Encryption Trends Study[1]

Ponemon Institute, February 2013

Part 1. Executive Summary

Ponemon Institute is pleased to present the findings of *the 2012 Global Encryption Trends Study,* sponsored by Thales e-Security. We surveyed 4,205 individuals across multiple industry sectors in seven countries - the United States, United Kingdom, Germany, France, Australia, Japan and Brazil.[2] The purpose of this research is to examine how the use of encryption has evolved over the last eight 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 seven countries in various regions of the globe.

In our research we consider the threats organizations face and how encryption is being used to reduce these risks. In this year's study we asked questions about the types of encryption technologies deployed, the most salient threats to sensitive and confidential information, data protection priorities, and budgeted expenditures for encryption and key management activities.

Following are big encryption trends over eight years:

- Increase in the use of encryption as an enterprise rather than a point solution.
- More influence at the business unit level in choosing and deploying encryption technologies.
- Decrease in the importance of compliance as a main driver to encryption adoption.
- Increase in spending on encryption and key management as a percentage of the IT budget.

Following is a summary of our most salient 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. As shown in this research, organizations with a strong security posture are more likely to invest in encryption and key management to meet their security missions. Characteristics that we believe indicate a favorable orientation to encryption solutions include:

- Have a formal encryption strategy that spans the entire enterprise.
- Place a high level of importance on data protection activities as an integral part of their risk management efforts.
- Attach a high level of importance to the role of key management in the context of encryption of sensitive data.
- Dedicate a larger proportion or share of their IT security budget to encryption and key management solutions.
- Deploy encryption in a wide variety of scenarios or use cases across the entire enterprise.
- Are aware of the role of key management standards such as the key management interoperability protocol (KMIP).
- Deploy hardware security modules (HSMs) as part of the organizations' encryption and key management strategies.

[1]The reporting date of the trends series pertains to the year of completion, not publication. This year's study was completed in December 2012 for seven 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) and Brazil (BZ).
[3]The trend analysis shown in this study was performed on combined country samples spanning eight years (since 2005).

Summary of key findings:

More organizations are adopting an enterprise encryption plan or strategy rather than relying on ad hoc requirements or informal policies. Over the past eight years of conducting this research, organizations in Germany, US and Japan have become more mature in executing their encryption strategies. Australian, French and Brazilian organizations remain less mature.

Business unit leaders are gaining influence over their company's use of encryption solutions. IT leaders are still most influential in determining the use of encryption. However, non-IT business managers are becoming more influential. For the first time, US non-IT managers have become most important for determining their company's encryption strategies. This could indicate that business unit leaders are taking a greater role in determining the technologies their organizations need to ensure data security and privacy.

Encryption usage is an indicator of a strong security posture. Organizations that deploy encryption extensively throughout the enterprise as opposed to limiting its use to a specific purpose (i.e., point solutions) appear to be more aware of threats to sensitive and confidential information and spend more on IT security. In other words, encryption use makes a strong contribution to an organization's overall security posture.

Employee mistakes, e-discovery and other accidental disclosures are considered the main threats to sensitive and confidential data. In fact, concerns over accidental leakage outweigh fears of direct attack by insiders or hackers by more than a ratio of two to one.

Main drivers for using encryption are protecting brand or reputation and reducing the impact of data breaches. However, in the UK and France the main reason for encryption is to comply with privacy or data security regulations and requirements.

Identity and access management followed by the discovery of data at risk are the top two data protection priorities. New additions to this year's study are application level protection of data and the need for data protection in the cloud computing environment. Least important in our list of potential priorities is the protection of data transmitted over internal and external networks.

The use of encryption as an enterprise security solution is growing. The encryption of backup files, internal networks, external communications, cloud services and databases are most likely to be extensively deployed. In contrast, email encryption and encryption of data on smart phones and tablets are the least likely to see enterprise-wide deployment. Nearly half of the organizations surveyed report they are deploying between four and six different types of encryption.

Financial service companies are most likely to use encryption technologies throughout the enterprise. In contrast, manufacturing and retail organizations are less likely to have extensive encryption usage.

Most important features of encryption technology solutions are system performance and latency, automated management of keys and automated enforcement of policies. The least important features are support for longer encryption keys and support for formal preserving encryption.

Formal key management strategies are becoming more common. These strategies tend to focus on increasing business efficiency and reducing operational cost. Germany and Japan have the highest percentage of companies that have key management strategies independent of the various uses of cryptography within the organization.

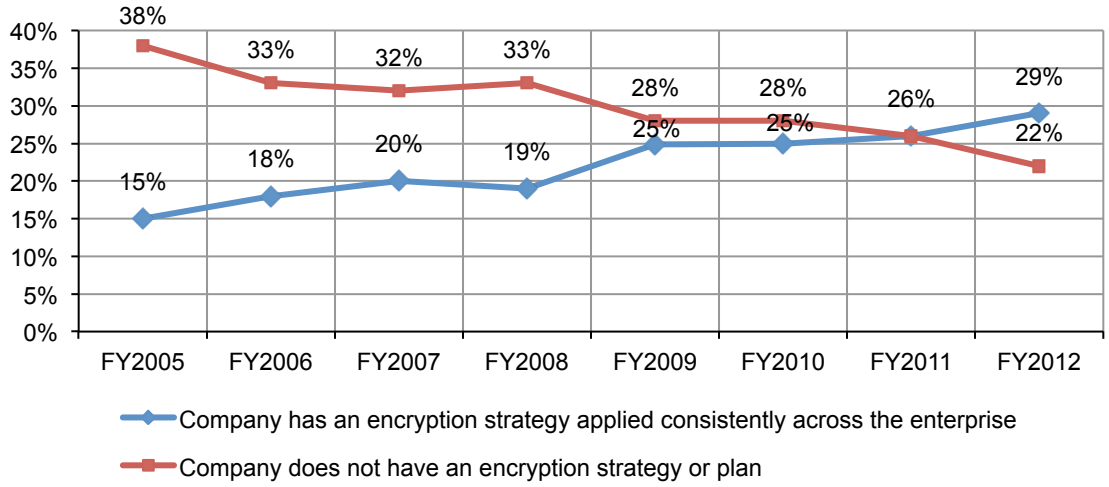
Key management standards and hardware security modules (HSM) are projected to become more important. Key management interoperable protocol (KMIP) and HSMs provide mechanisms for unifying and automating key management activities and reducing the risk of key management processes being subverted as a way to gain illicit access to encrypted data.

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 in the past eight 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 France and Brazil report the lowest adoption of an enterprise strategy.

Figure 2. Differences in enterprise encryption strategies by country samples

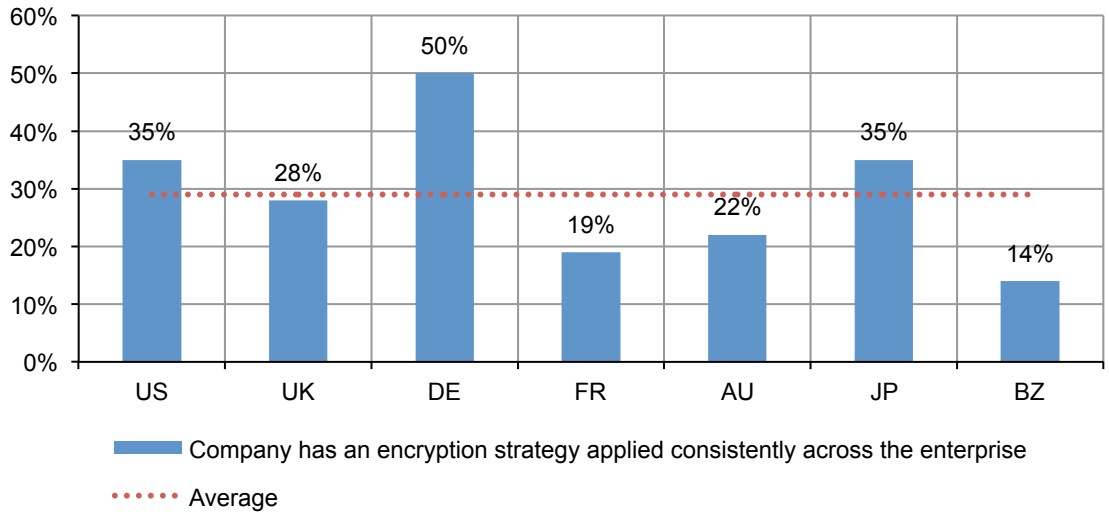


Figure 3 shows the most influential functional areas for defining the company's encryption strategy. The figure shows that IT operations are deemed most influential in determining the organization's enterprise encryption strategy. In this study, "lines of business" are defined as those with commercial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

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

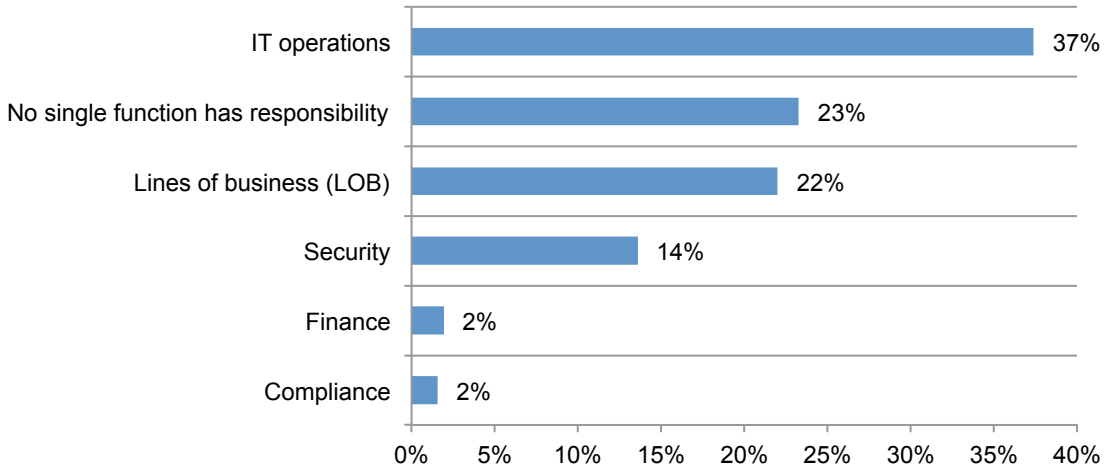


Figure 4 shows that the IT operations function has consistently been most influential in framing the organization's encryption strategy. However, that picture is steadily changing with business unit leaders gaining influence over their company's encryption strategy.

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 has 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 the past year years.

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

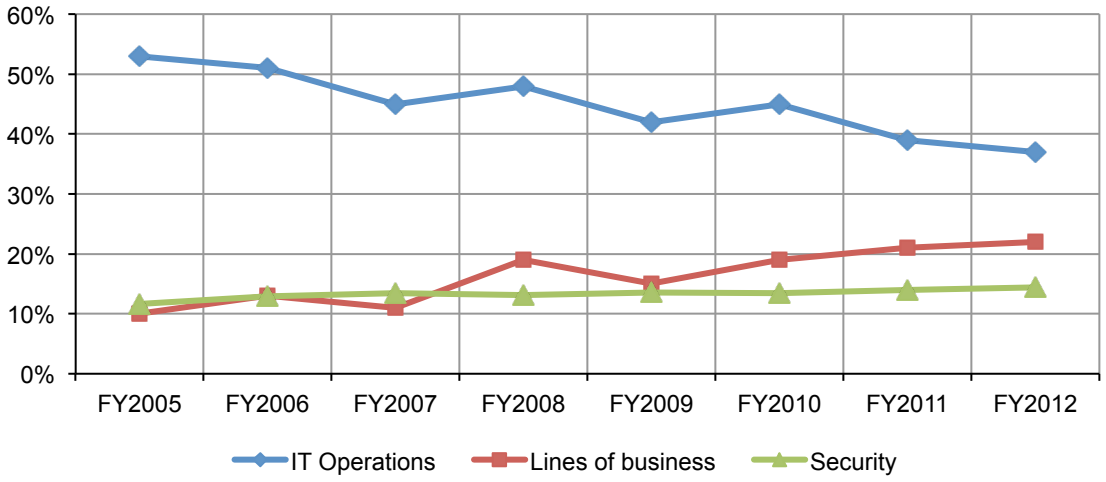
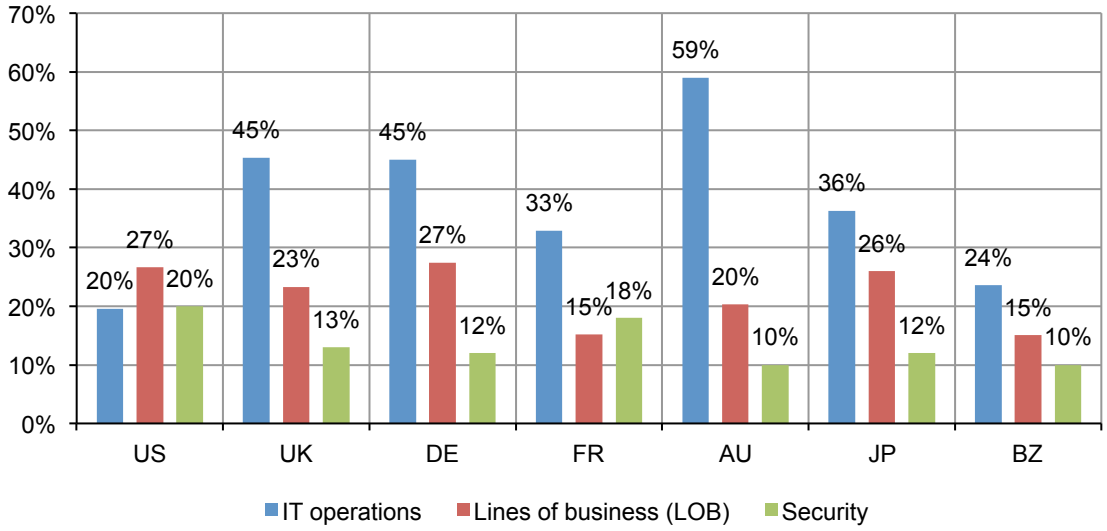


Figure 5 shows the distribution of respondents who rate IT operations, LOB and security as most influential in determining their organization's encryption strategy. This chart shows IT operations as most influential followed by business managers in six of seven countries. For the first time, business managers are more influential than IT, according to US respondents. In addition, respondents in the US and France rate security as having a higher level of influence on setting their organization's encryption strategy than in the other countries.

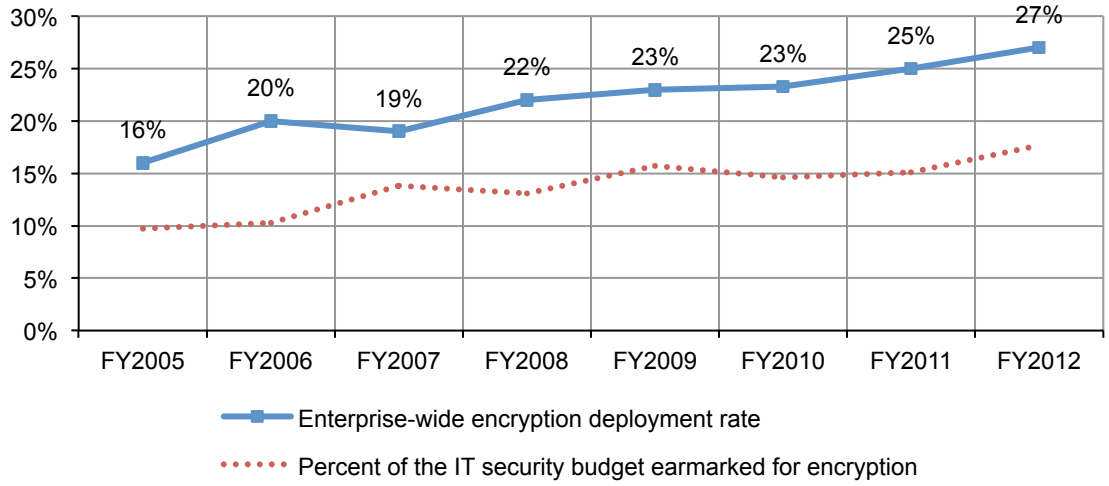
Figure 5. Influence of IT operations, LOB and security by country samples



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 (i.e., a compound increase of 11 percent computed over eight years.[4] Figure 6 summarizes enterprise-wide usage consolidated for various encryption technologies over eight 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. As expected, the patterns for deployment and budget show a strong 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 organizations have the highest percentage of companies with an enterprise encryption strategy and they are the most extensive users of encryption technologies. In contrast, Brazil has the lowest percentage of companies with an enterprise strategy and encryption use.

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

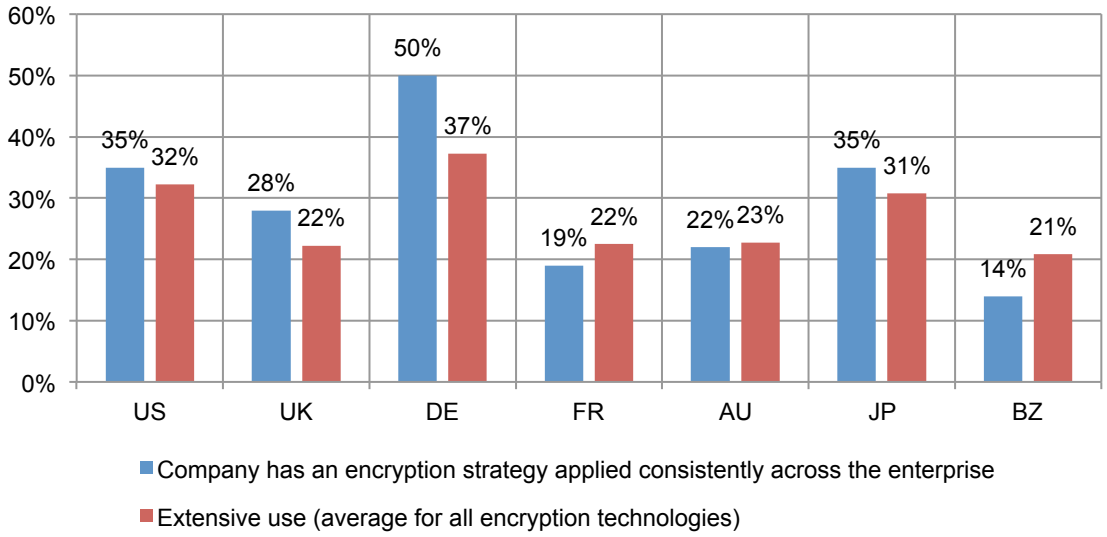
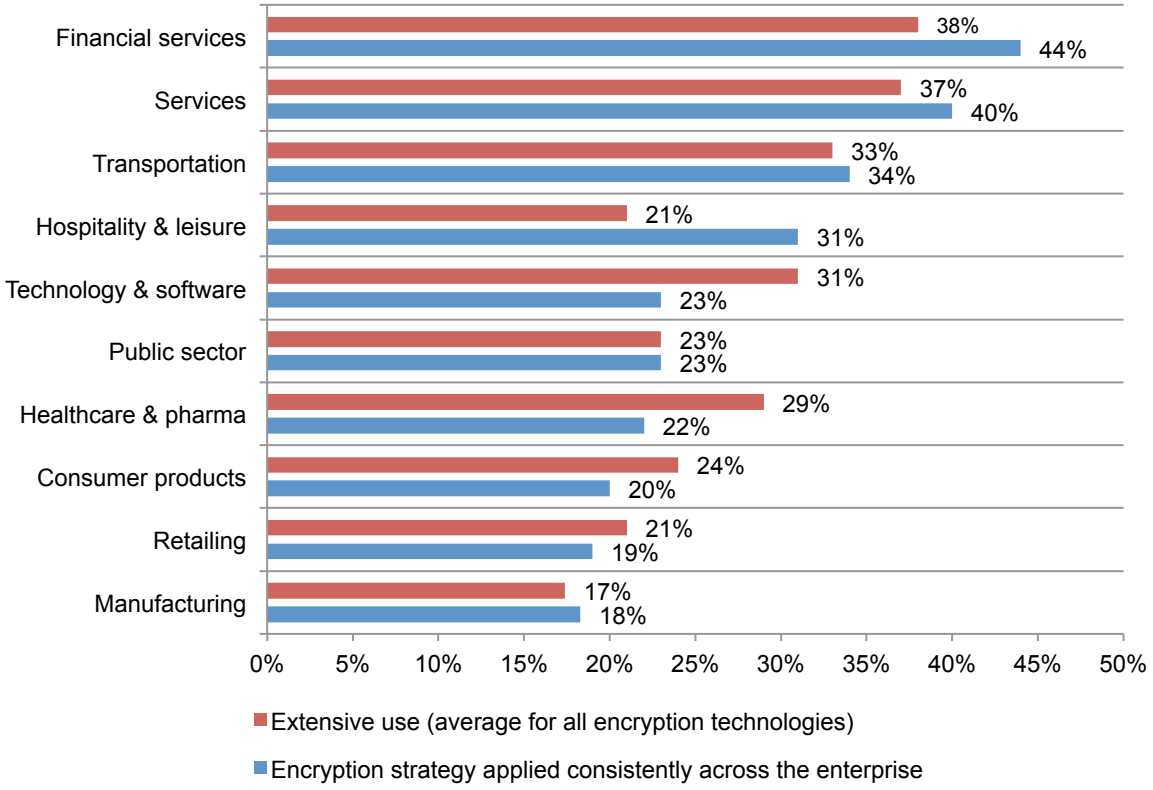


Figure 8 shows the relationship between encryption strategy and use of encryption for 10 industry sectors. Here again, the findings suggest a positive relationship between strategy and use.

Financial services have the highest percentage of companies with an enterprise encryption strategy and are the most extensive users of encryption technologies. In contrast, manufacturing companies have the lowest deployment rate and are the least likely to have an enterprise encryption strategy. It is interesting to note that there are three sectors where a gap exists between strategy and deployment. In the case of the technology and healthcare sector, the rate of deployment appears to be ahead of strategy. In hospitality and leisure deployment appears to lag.

Figure 8. The extensive use and availability of an enterprise strategy by industry



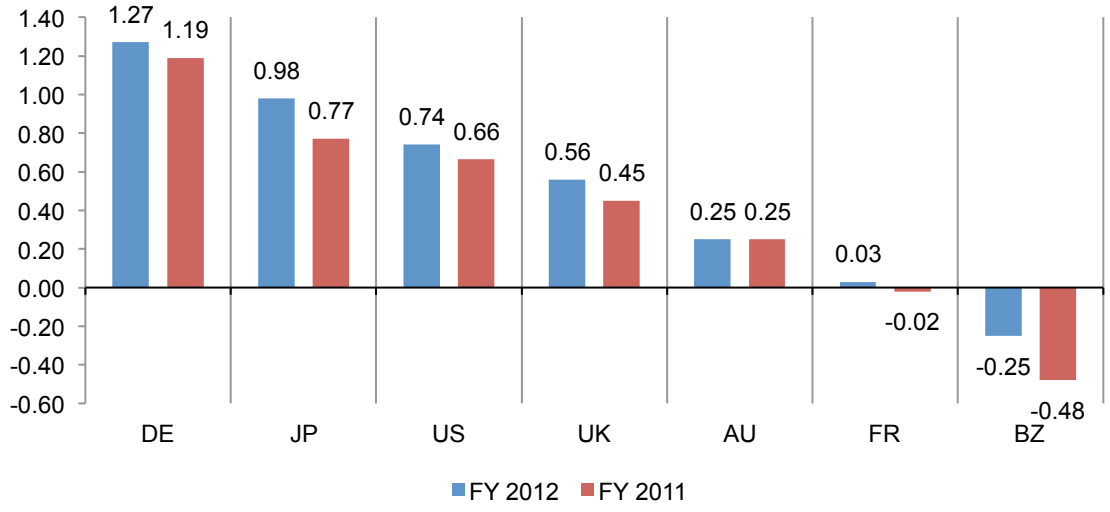
Encryption and Security Effectiveness (SES)

To estimate the security posture of organizations, we used the Security Effectiveness Score or SES as part of the survey process.[5] The SES range of possible scores is +2 (most favorable) to -2 (least favorable). We define an organization's security effectiveness as being able to achieve the right balance between efficiency and effectiveness across a wide variety of security issues and technologies.

A favorable score indicates that the organization's investment in people and technologies is both effective in achieving its security mission and is also efficient. In other words, they are not squandering resources and are still being effective in achieving their security goals.

Following is a summary of the average SES for each country sample for two years. Germany achieves the highest score, while Brazil has the lowest score in both the 2011 and 2012 encryption trends studies.

Figure 9. Average security effectiveness score (SES) in ascending order by country



[5]The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). Hence, a result greater than zero is viewed as net favorable.

Figure 10 reports the SES results compiled from encryption trend studies conducted over eight years. The trend line shown below is increasing, which suggests the security posture of participating companies has increased over the eight-year time period.

Figure 10. Trend in average Security Effectiveness Score (SES)

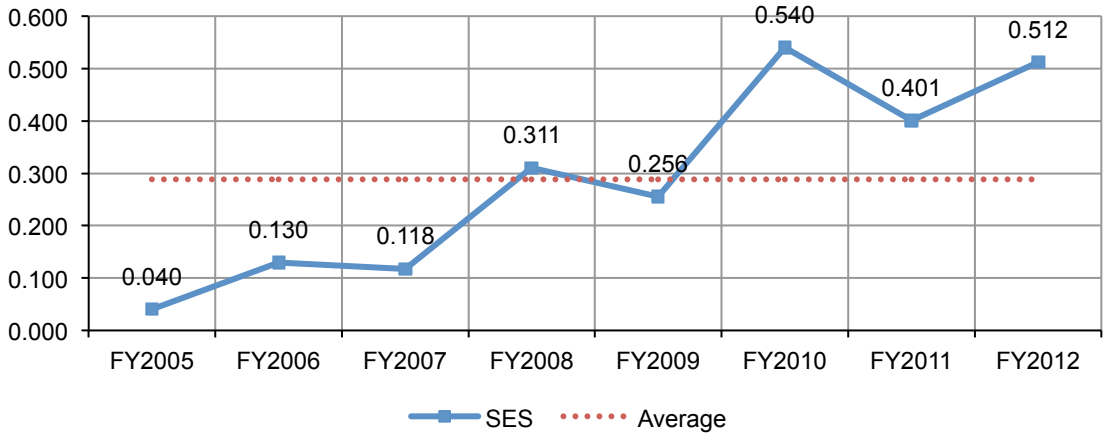


Figure 11 summarizes a cross-tab analysis of SES and the percentage of organizations that have an enterprise-wide encryption strategy and the percentage that have an extensive deployment of encryption. We divide the overall sample into four quartiles based on SES. We see that organizations in the highest SES quartile sub-sample are nearly three times more likely to deploy a holistic encryption strategy than companies in the lowest SES quartile sub-sample (41 percent versus 16 percent).

This figure also shows organizations in the highest SES quartile sub-sample are more than two times more likely to be extensive users of encryption technologies than companies in the lowest SES quartile sub-sample (38 percent versus 15 percent). The pattern of quartile averages in Figure 11 provides strong evidence that both encryption strategy and the use of encryption make an important contribution to organizations' security posture.

Figure 11. Analysis of encryption strategy and use by SES quartile (security posture)

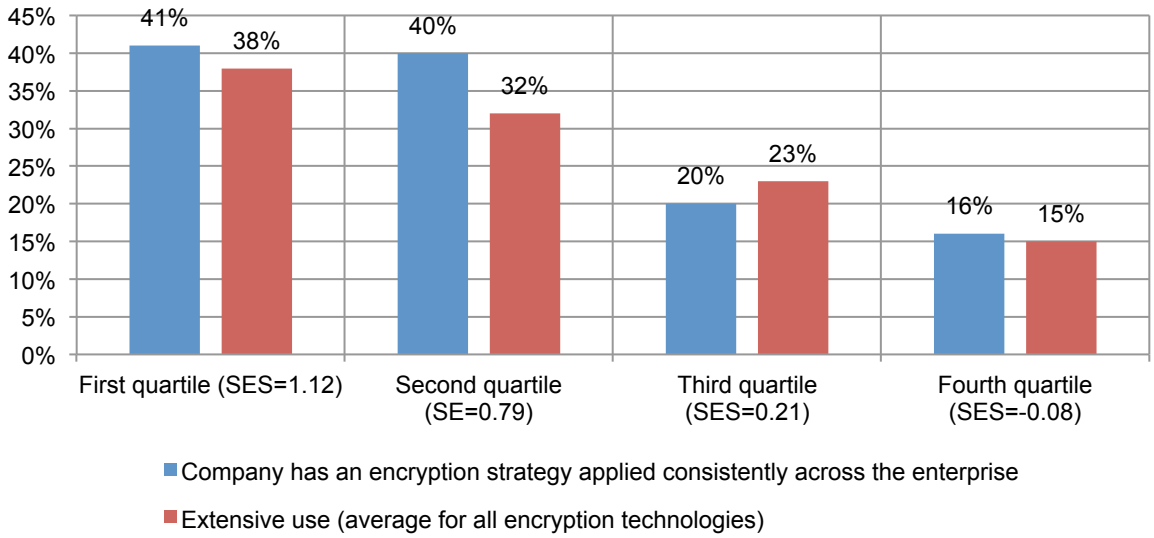
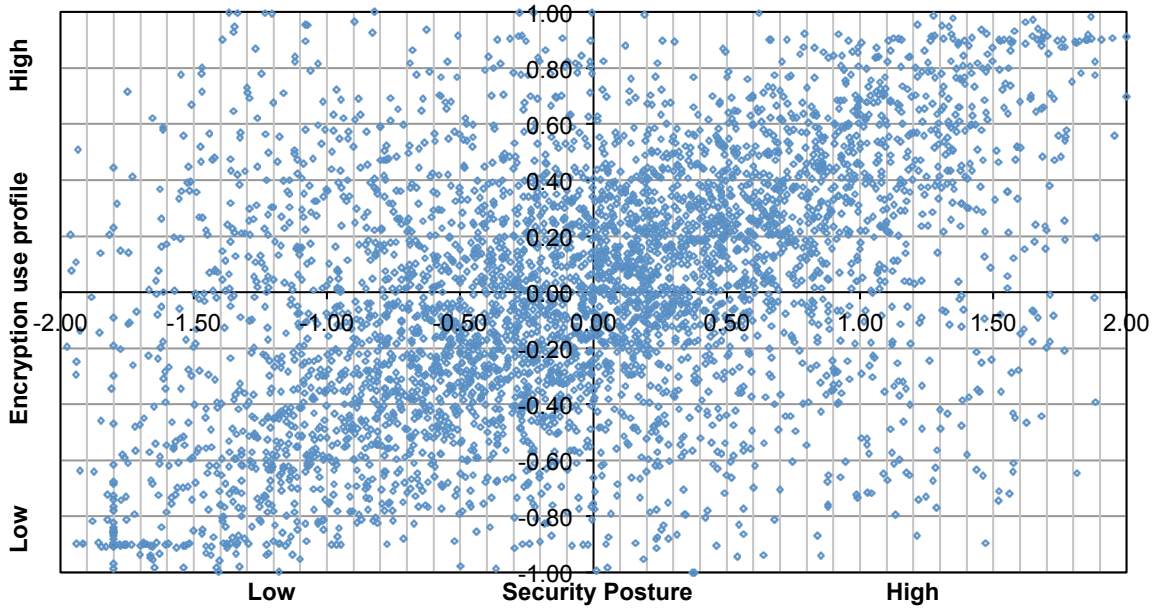


Figure 12 reports a scattergram showing the interrelationship between the respondents' encryption use profile and SES. The encryption use profile is a ratio variable between +1 and -1 compiled from the extensive use of 11 encryption technologies.[6] This diagram clearly shows a clustering of data points that form a positive (upward sloping) relationship, which suggest that encryption use and a strong security posture (high SES) are inextricably linked.

Figure 12. Scattergram depicting the relationship between encryption use ratio and security posture



[6]Each respondent was assigned a profile score based on their organizations' extensive use of encryption technologies. Those respondents who said their organizations extensively deployed all 11 encryption technologies were rated +1. Those respondents who said they did not extensively deploy any one of the 11 encryption technologies were rated -1. Hence, most respondents earned a rating between these two limits.

Threats, main drivers and priorities

As shown in Figure 13, the most significant threat to the exposure of sensitive or confidential data is employee mistakes followed by forced disclosures triggered by e-discovery events such as legal and law enforcement requests and system process malfunctions. In contrast, the least significant threats temporary or contract workers and third-party service providers. Concerns over inadvertent exposure (employee mistakes, e-discovery and system malfunction) outweigh concerns over actual attacks (hackers and malicious insiders) by more than 2 to 1 (57% compared to 25%).

Figure 13. The most salient threats to sensitive or confidential data

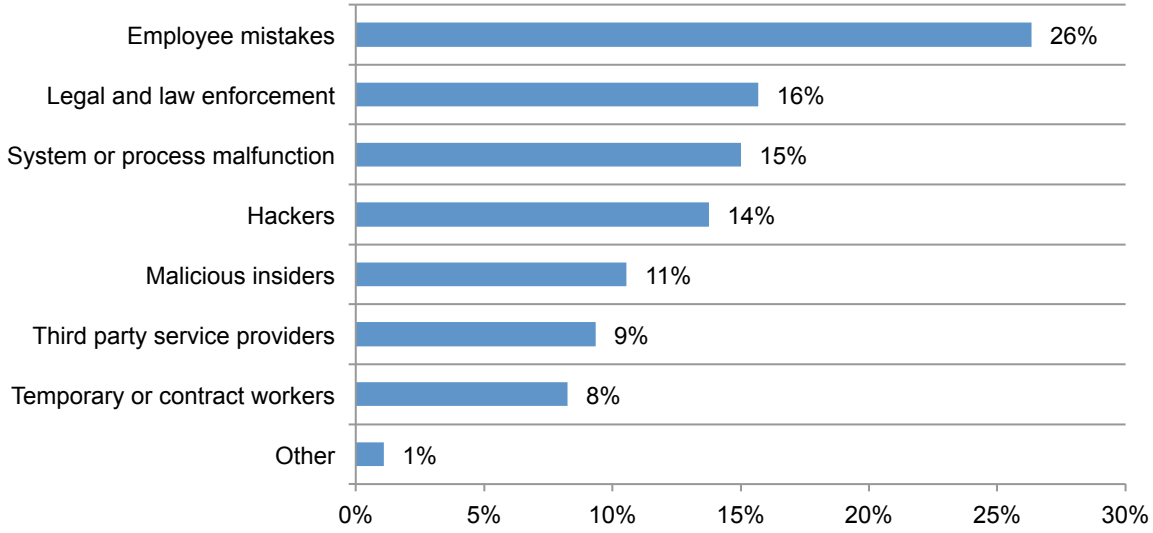
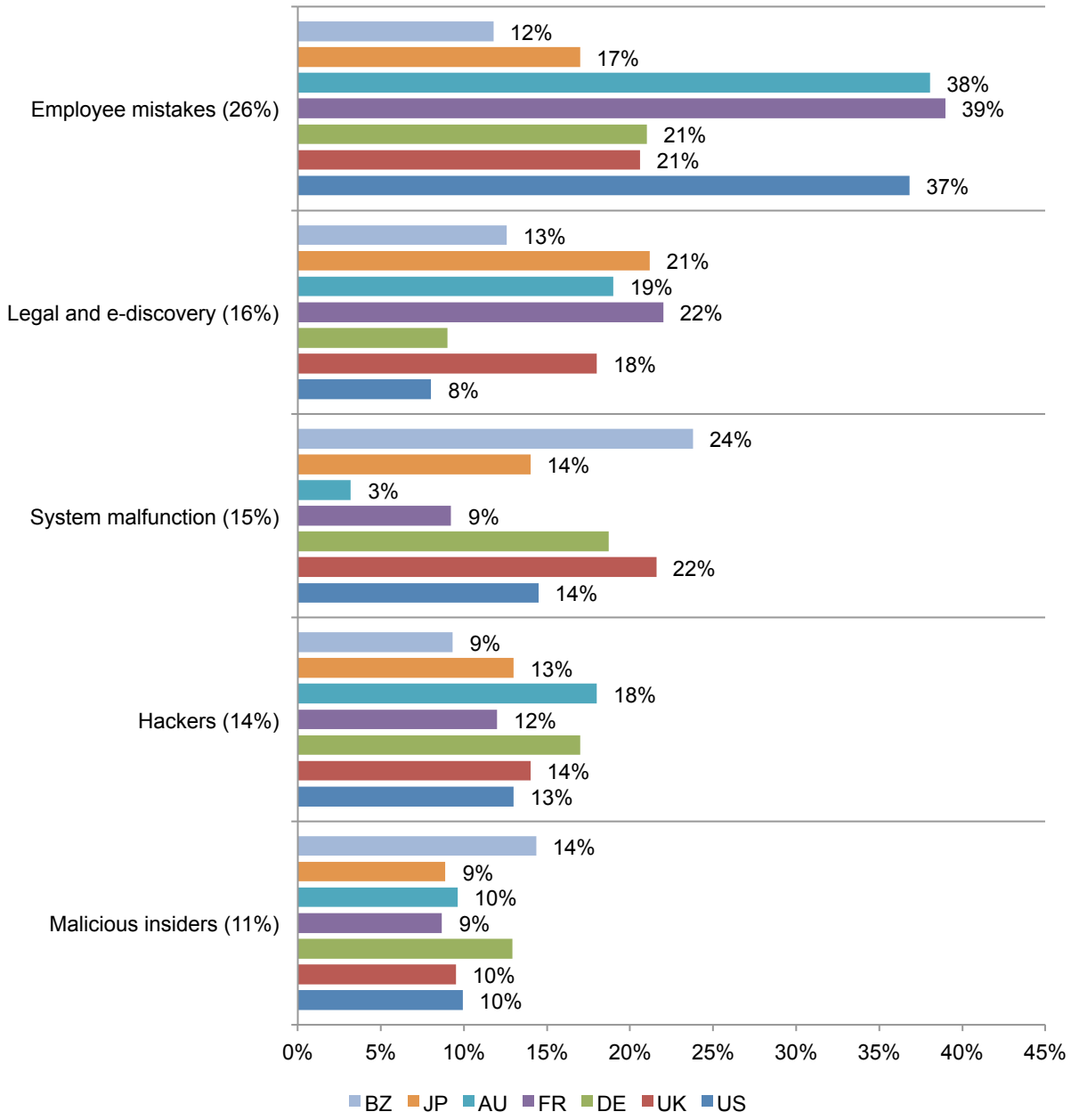


Figure 14 lists in ascending order the top five perceived data threats by country.[7] It shows marked differences among country samples. Accordingly, respondents in France, Australia and the US rate employee mistakes at a much higher level than respondents in Brazil, Japan, Germany and the UK. In contrast, respondents in Brazil rate system malfunction and malicious insiders at much higher levels than all other countries.

Figure 14. Top five perceived threats by country samples



[7]The consolidated average percentage is noted in parenthesis next to each threat category presented.

Main drivers for using encryption are protecting brand or reputation and reducing the impact of data breaches. The top five drivers for deploying encryption are presented in Figure 15. Respondents reported that protecting their organization's brand or reputation if a data breach occurs (44 percent), to reduce the impact of a data breach (42 percent), and to comply with privacy or data security regulations and requirements (38 percent) were the most important drivers.

Figure 15. The main drivers for using encryption technology solutions

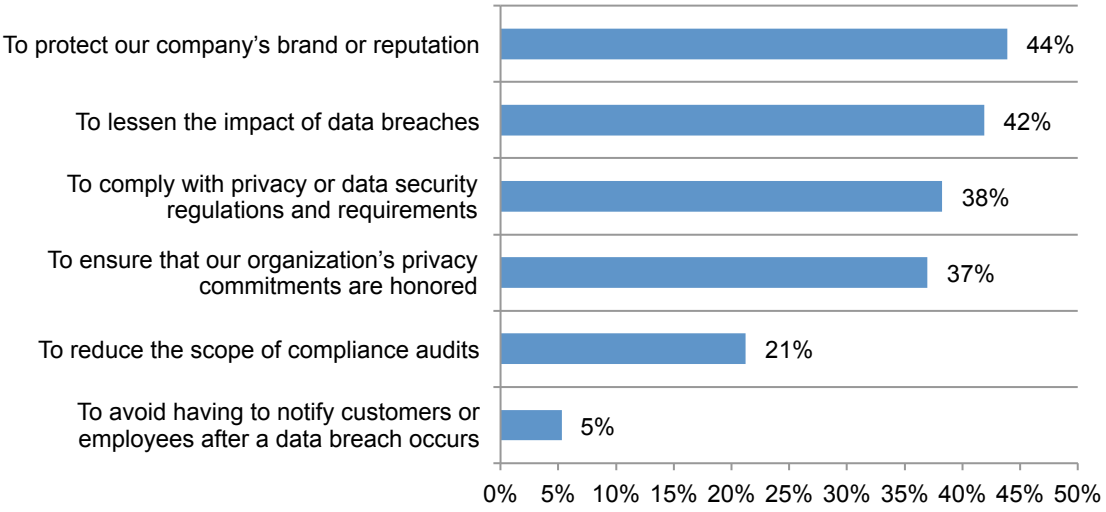
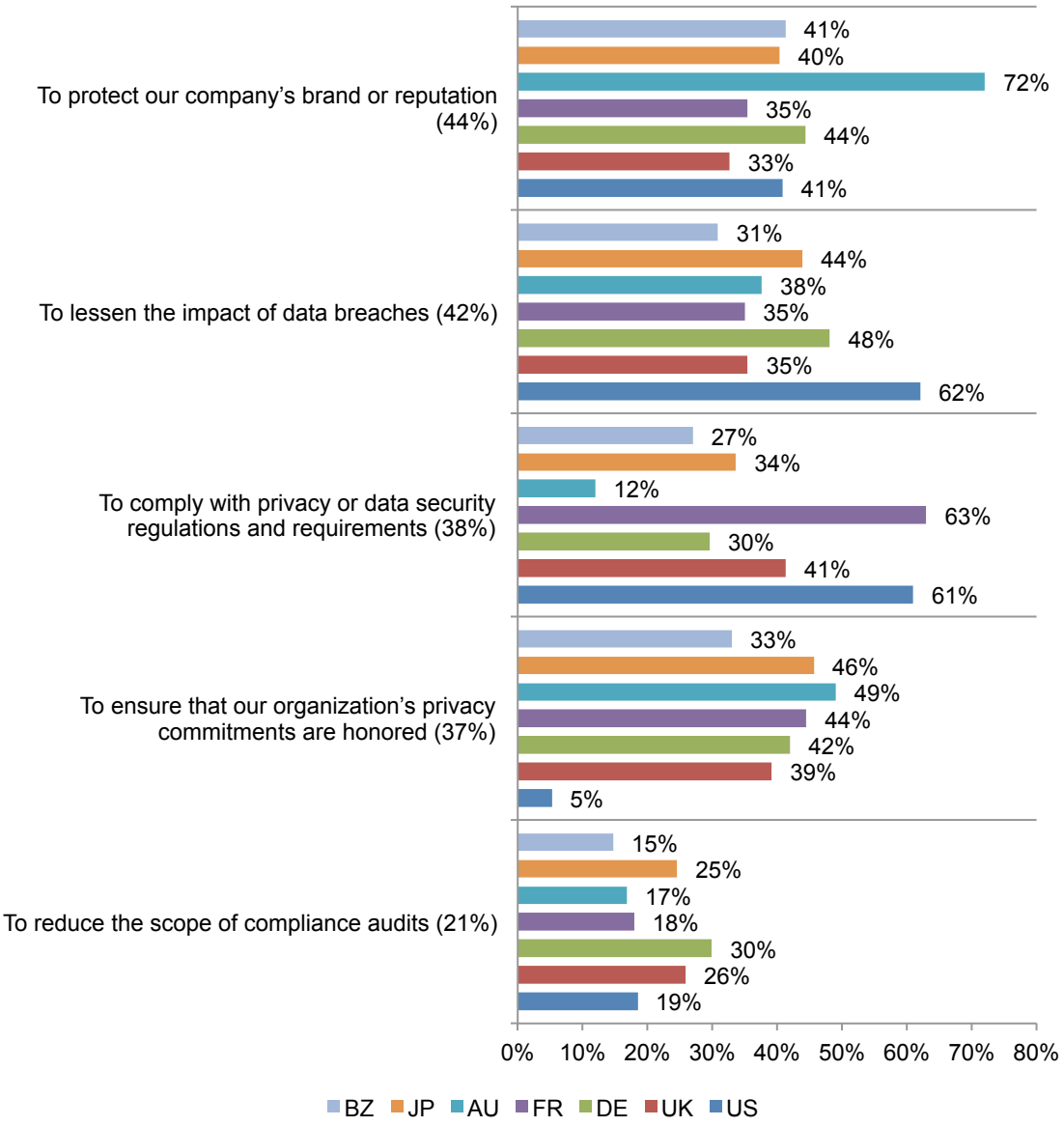


Figure 16 also shows marked country differences. As shown, Australian respondents provide the highest rating to company brand and reputation. US respondents provide the highest rating to lessening the impact of data breaches. French respondents provide the highest ratings to compliance with privacy or data protection regulations.

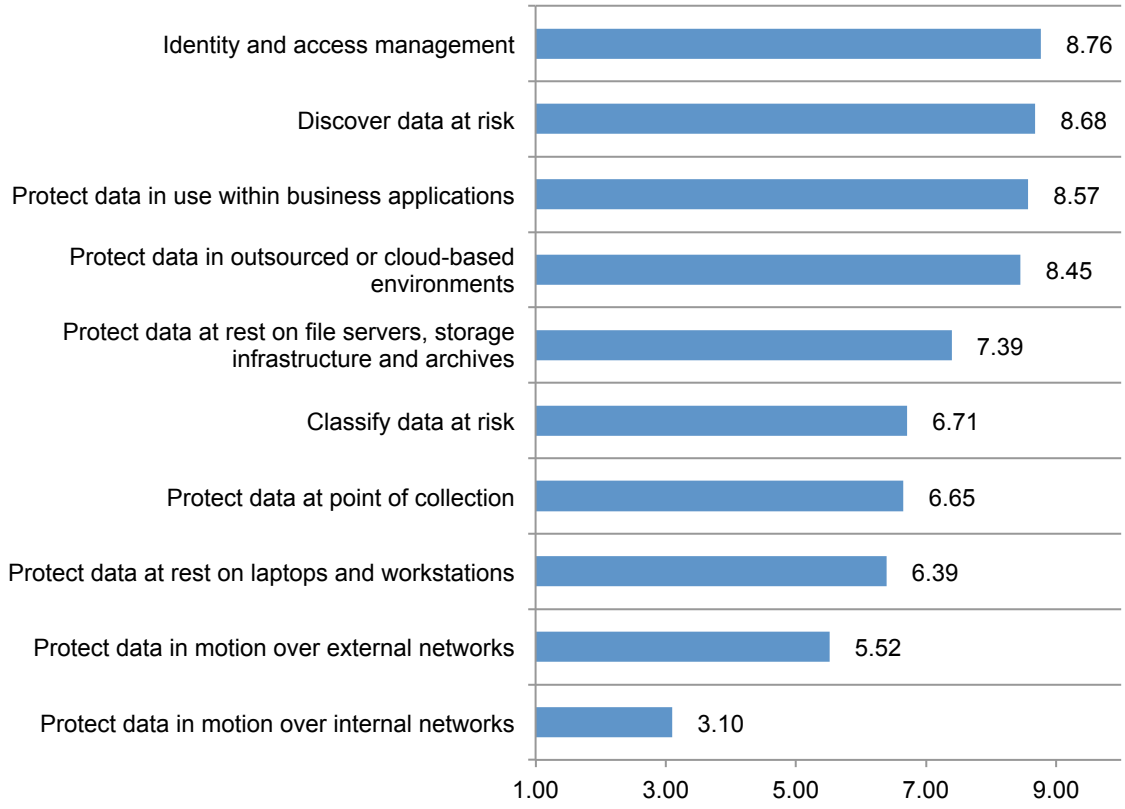
Figure 16. The top five drivers for using encryption



Prioritization of data protection activities. There are numerous aspects to developing a data protection strategy. Some focus on addressing specific threat models and others consider aspects of a more holistic nature. The following figure presents the relative prioritization of these aspects that together make a significant contribution to an overall data protection strategy.

Figure 17 provides a list of 10 aspects that are considered an important part of an organization's data protection strategy in descending order. The top data protection priorities are: identity and access management, data discovery, protecting data in use within business applications and protecting data in outsourced or cloud environments.[8]

Figure 17. Ranking of data protection priorities
Highest rank = 10, lowest rank = 1



[8]Last year's study ranked 13 rather than 10 priority attributes. In that study, protecting data in cloud environments was ranked twelfth. This year's study ranks this same attribute as the fourth most important. This suggests a rise in the importance of data protection in the cloud ecosystem.

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 18, no single technology dominates because organizations have very diverse deployments. Encryption of databases, external public networks and cloud services are most likely to be deployed. The encryption of backup files is the most likely to be used extensively. In contrast, smart phone and tablet, email and file server encryption solutions are less likely to be extensively deployed.

Figure 18. Consolidated view on the use of encryption technologies

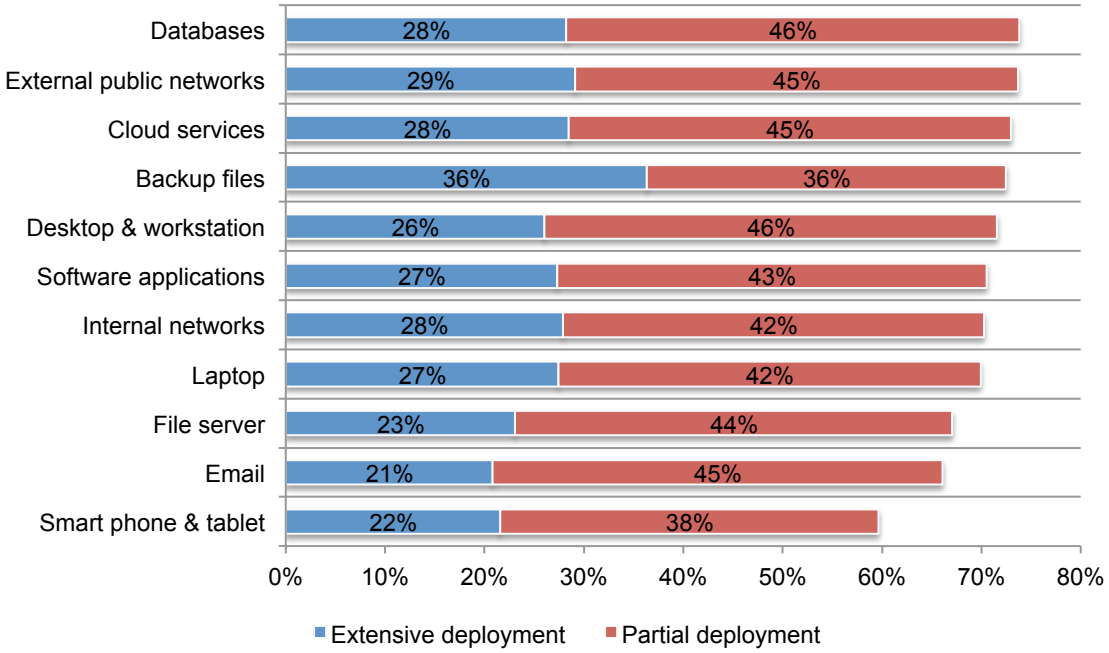
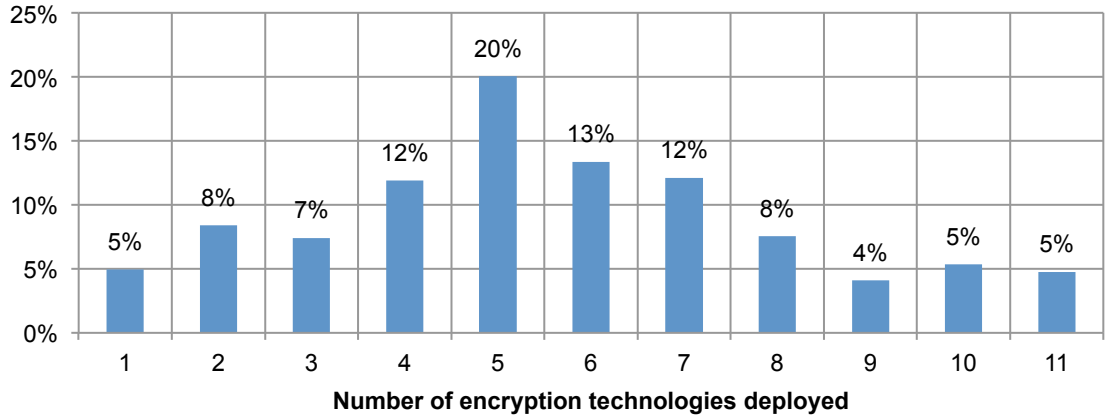


Figure 19 provides a histogram showing the percentage frequency of 11 encryption technologies deployed by respondents in all country samples combined. As can be seen, 67 percent of the consolidated sample say their organizations use five or more separate encryption technologies with 45 percent of organizations deploying between four and six different types of encryption technology.

Figure 19. Percentage frequency of 11 encryption technologies deployed



The use of encryption varies greatly among countries. The following table and chart reports the rank order of eleven (11) encryption technologies for seven countries according to rate of extensive usage. For example, looking at the US sample, we see that laptop encryption enjoys the highest extensive use and internal networks the lowest extensive use. In contrast, the UK sample rates database encryption at the highest use rate and laptop encryption the lowest use rate. The other country rankings are interpreted in the same way.

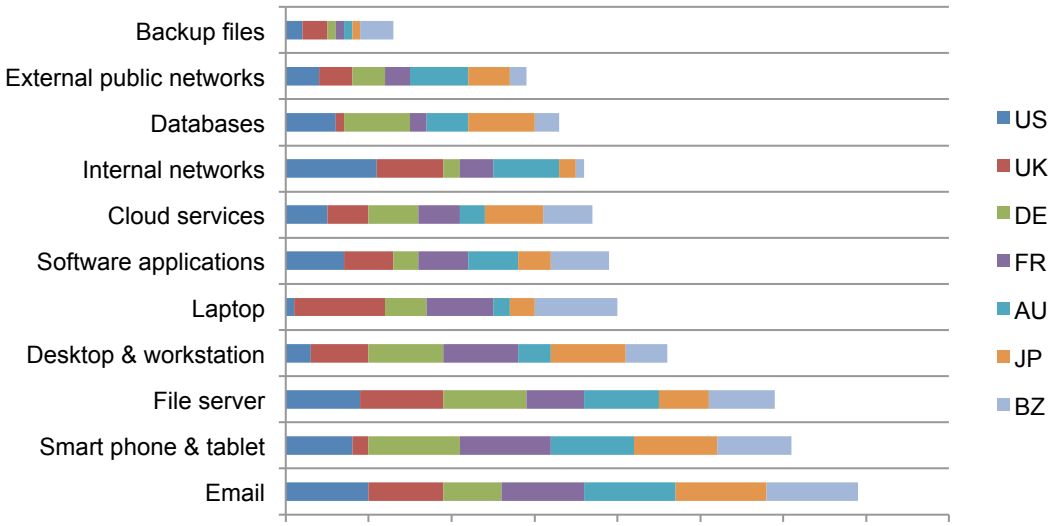
The most frequently utilized encryption technology in Germany, France Australia and Japan is the encryption of backup files. German and French respondents report their organizations are least likely to use encryption technologies for smart phones and tablet computers. Australian and Japanese respondents say their organizations are least likely to use email encryption. Finally, the Brazilian sample shows the encryption of internal networks has the highest use rate. In contrast, email encryption has the lowest extensive use rate in Brazil.

Table 1. Encryption technologies	US	UK	DE	FR	AU	JP	BZ
Backup files	2	3	1	1	1	1	4
External public networks	4	4	4	3	7	5	2
Databases	6	1	8	2	5	8	3
Internal networks	11	8	2	4	8	2	1
Cloud services	5	5	6	5	3	7	6
Software applications	7	6	3	6	6	4	7
Laptop	1	11	5	8	2	3	10
Desktop & workstation	3	7	9	9	4	9	5
File server	9	10	10	7	9	6	8
Smart phone & tablet	8	2	11	11	10	10	9
Email	10	9	7	10	11	11	11

Note: 1 = highest extensive use rate and 11 = lowest extensive use rate

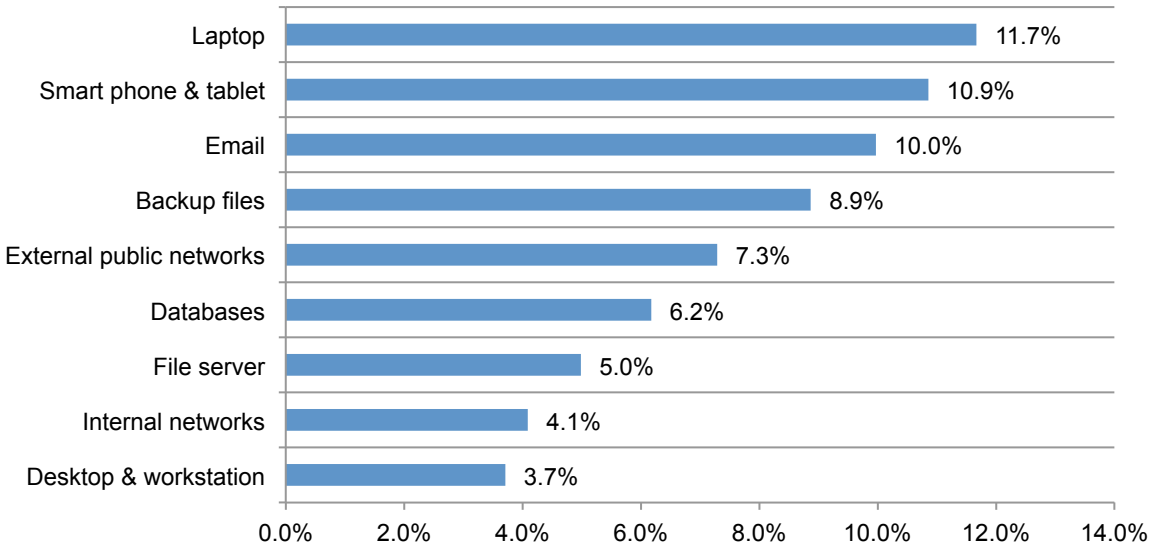
The following chart summarizes the cumulative rank order for all countries shown in Table 1. Like a golf score, a short bar indicates a high use rate and a long bar indicates a lower use rate. Figure 20 shows a generally consistent pattern by country – wherein backup encryption has the highest use rate and email encryption has the lowest use rate.

Figure 20. Rank order of extensively used encryption technologies by country sample



The enterprise-wide use of encryption has steadily increased since our first annual study in 2005 (see Figure 6). The growth rate for nine encryption technology categories for three years is presented in Figure 21. Based on our calculations, laptop encryption achieved the highest growth rate in encryption deployment over the past three years, followed by smart phone and tablet encryption and email encryption. Please note that application level encryption and cloud encryption technologies are not included in this analysis because both categories were added this year.

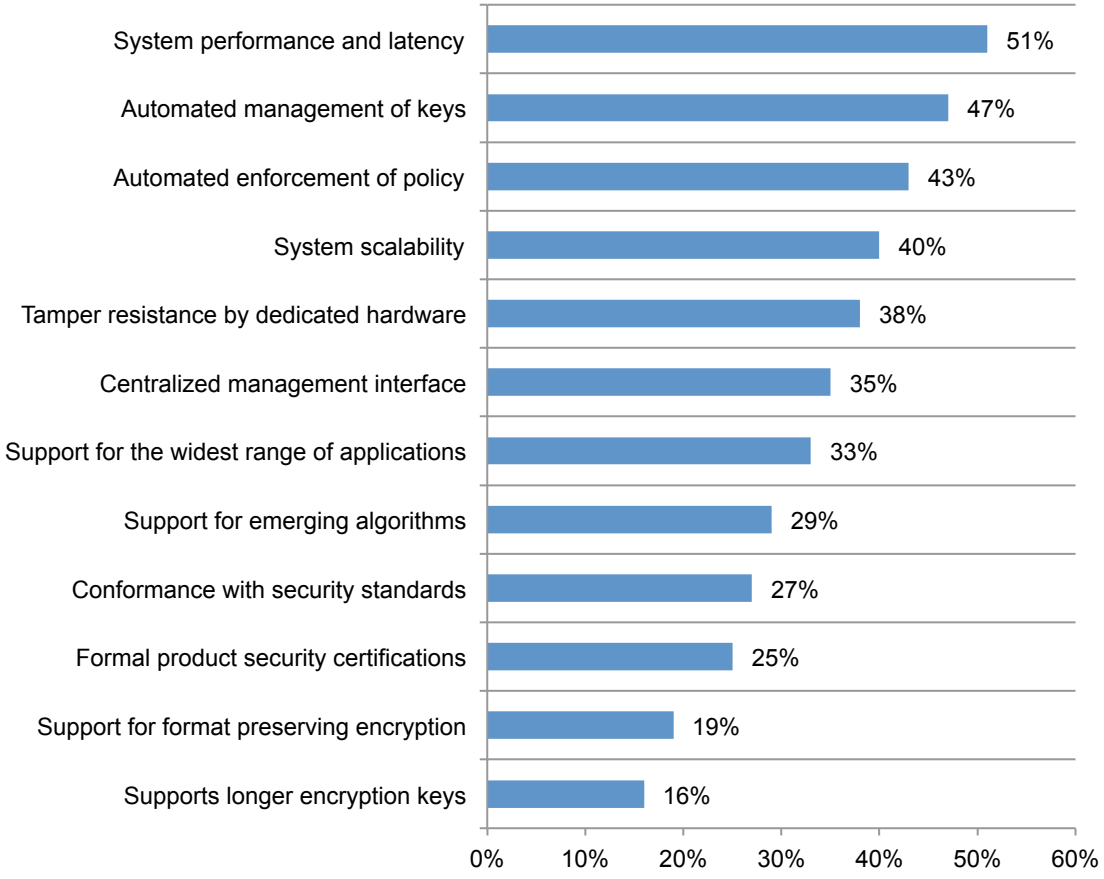
Figure 21. Growth rates for enterprise encryption for nine encryption technologies
Percentages are calculated from average rates over a three-year period



Encryption features considered most important

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, automated management of encryption keys and automated enforcement of policy are the three most important features. The ratings of 12 encryption technology features are listed in descending order of importance in Figure 22.

Figure 22. Most important features of encryption technology solutions
Very important response



Attitudes about key management

Figure 23 reports the percentage of respondents that report their organizations have key management strategies that are independent of the various uses of cryptography within the organization. As shown, Germany and Japan have the highest percentage results, while France and Brazil have the lowest percentage results.

Figure 23. The percentage of organizations that have key management strategies independent of the various uses of cryptography by country samples

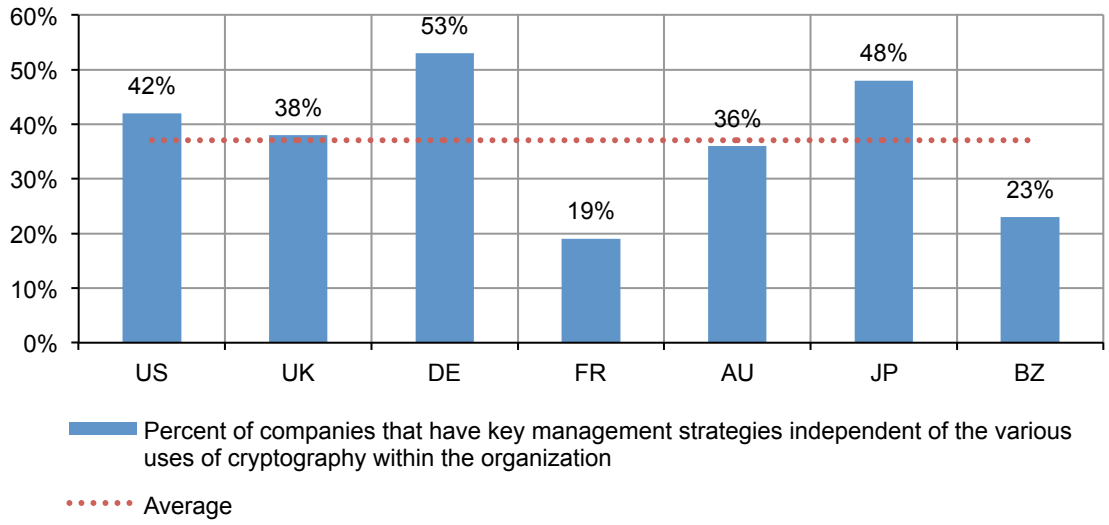


Figure 24 lists what respondents view as the primary drivers for developing a key management strategy. As can be seen, increased business efficiency and reduced operational cost are the top two issues.

Figure 24. Primary drivers for developing a key management strategy

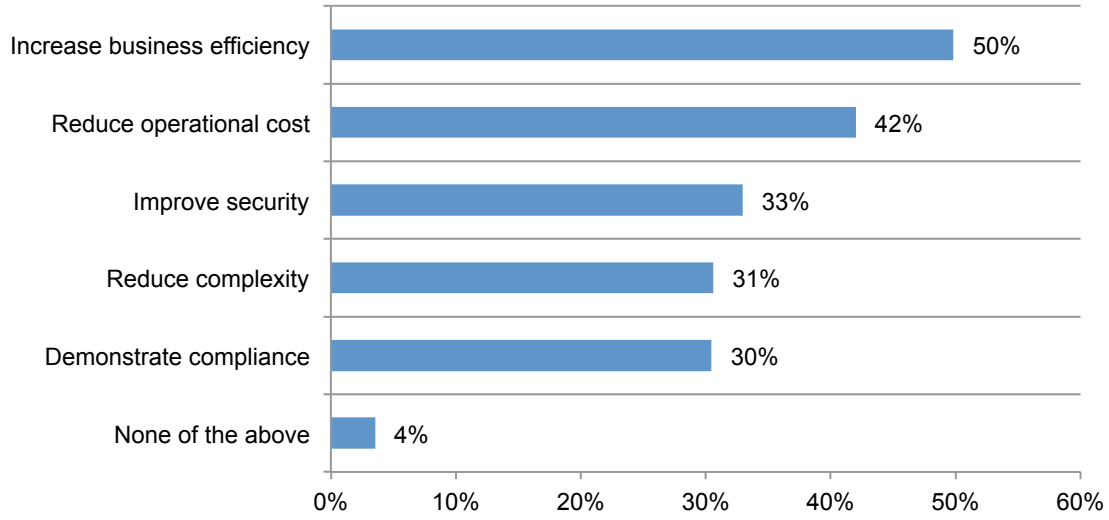


Figure 25 reports on the prevalence of four different deployment models for key management systems that are presently deployed. The combined responses to these four choices are very close implying that a consistent preferred approach to deploying key management has still not emerged in the market. The top two choices are single key management systems and multiple installations of a common key management system.

Figure 25. Key management deployment models

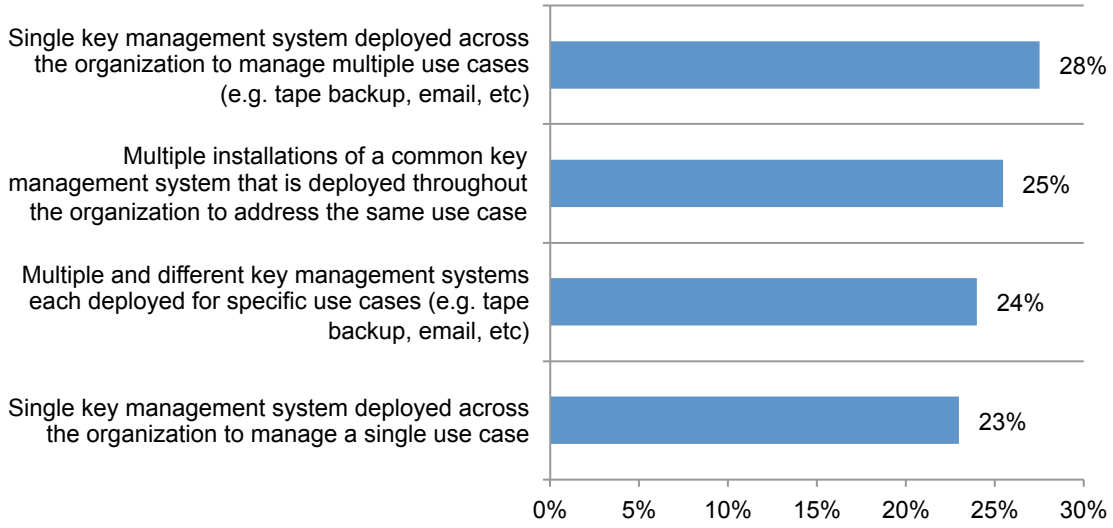


Figure 26 presents the extrapolated number of separate key management systems in use today within the respondent's organization and the number of systems that are planned in the next 12 months. As can be seen, respondents in the US and Brazil anticipate a slight decline, most likely resulting from consolidation of their various key management systems over the forthcoming year.

Figure 26. Separate key management systems currently deployed and planned to be deployed in the next 12 months

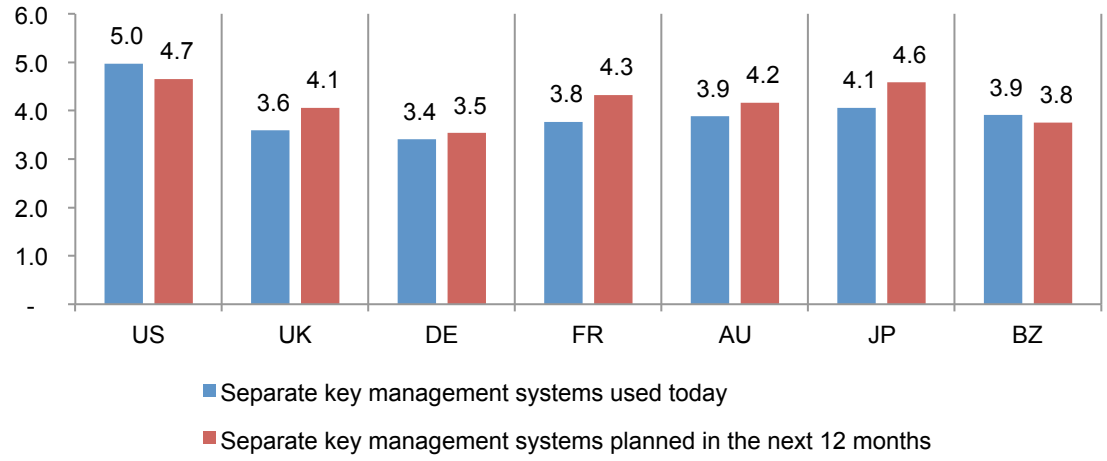


Figure 27 lists five different ways in which organizations might purchase or develop their various key management systems. As shown, the two most common scenarios are for organizations to purchase commercial off-the-shelf centralized key management systems and to utilize the native capabilities of the encryption solutions that are deployed.

Figure 27. Source of organizations' key management systems

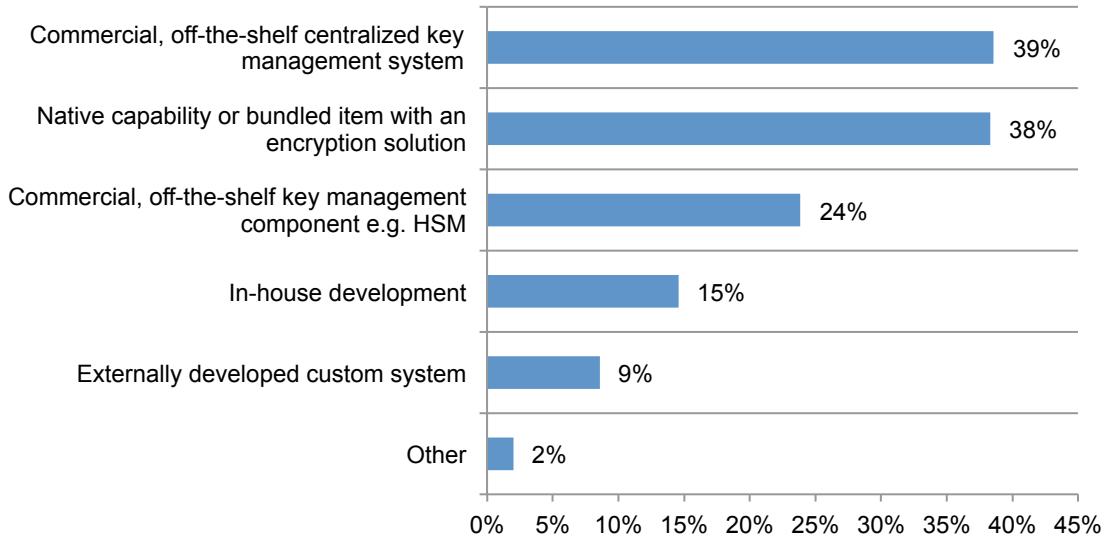


Figure 28 shows the importance of the key management interoperability protocol (KMIP). This is a relatively new standard that is designed to be a comprehensive protocol for communication between enterprise key management systems and encryption devices or applications.

By using a standardized protocol, organizations will be able to simplify key management and deploy centralize key management systems that span multiple use cases and equipment vendors. The KMIP standard is governed by OASIS.

Figure 28 shows the current and projected importance in the next 12 months. KMIP already has established a relatively high level of awareness among IT and IT security practitioners, and interest in KMIP is projected to rise over the next 12 months.

Figure 28. Importance of KMIP to organizations' key management strategy
Combined very important and important response

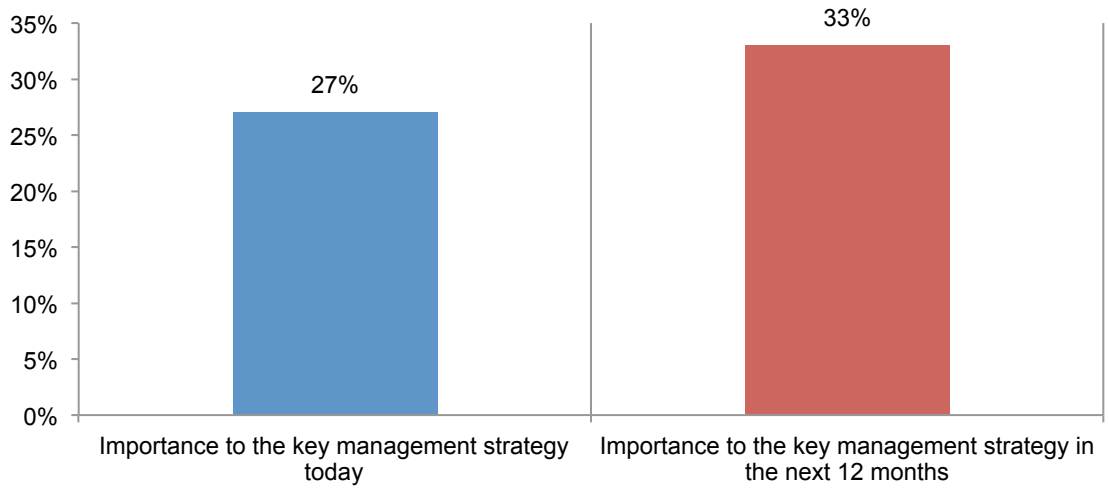


Figure 29 lists the areas where KMIP is considered most important for organizations' encryption and key management strategies. As shown, cloud-based applications and storage and traditional datacenter storage systems are viewed as most important.

Figure 29. Where KMIP is expected to make the biggest contribution to encryption and key management strategy

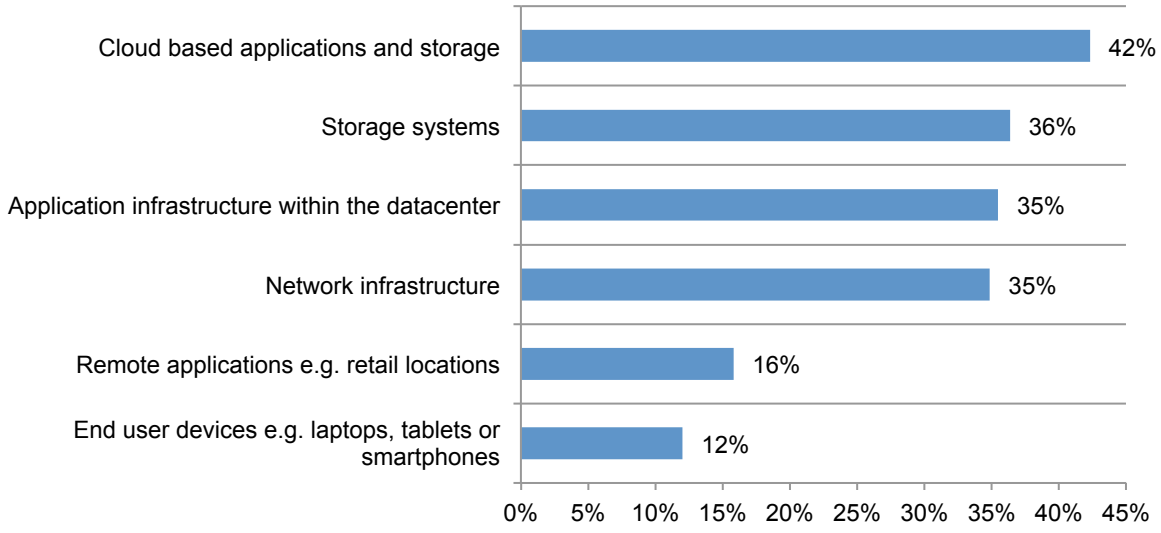
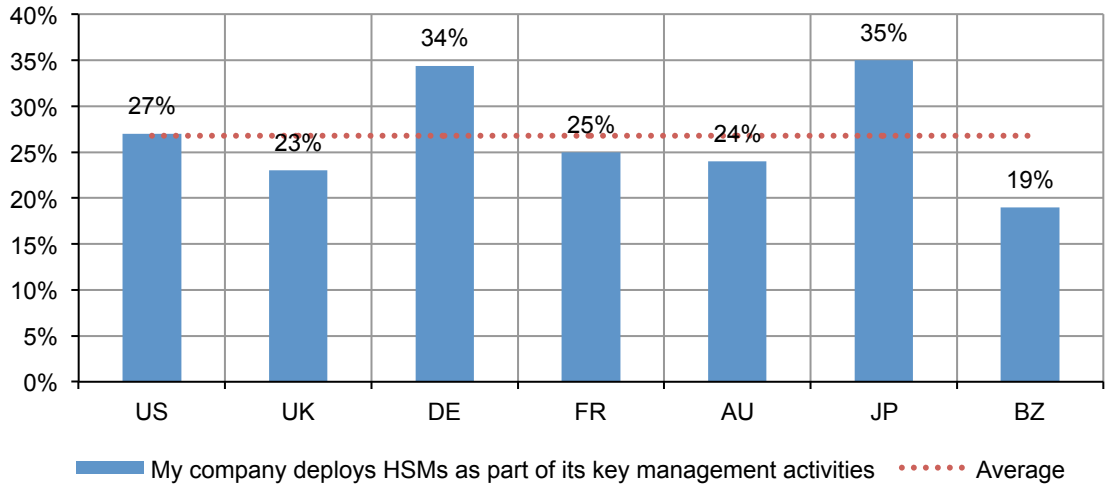


Figure 30 summarizes the percentage of companies that use hardware security modules (HSM) as part of their key management program or activities. HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g. encryption or digital signing) 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. Japanese and German companies are most likely to deploy HSM as part of encryption key management.

Figure 30. Percentage of organizations that deploy HSMs as part of their key management by country samples



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 31 reports the average percentage of IT security spending relative to total IT spending over the last eight 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 31. Trend in the percent of IT security spending relative to the total IT budget

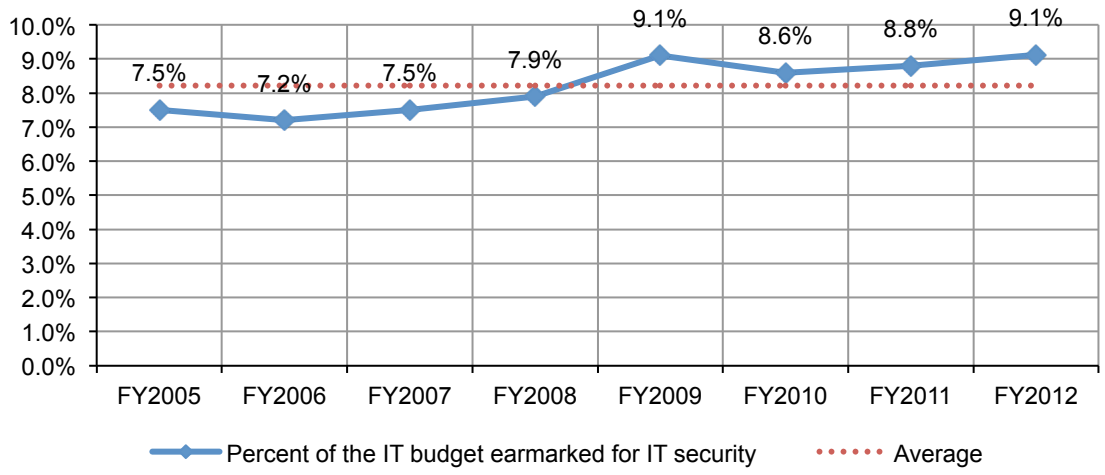
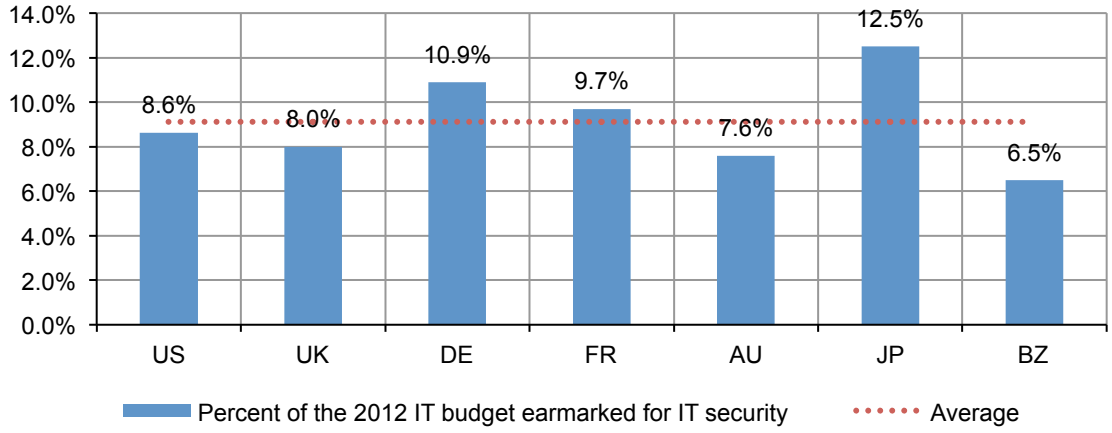


Figure 32 shows the percent of current IT security spending relative to the total IT budget for individual countries. As shown, Germany and Japan report the highest proportional ratings and Brazil and France report the lowest proportional ratings.

Figure 32. Percent of current IT security spending relative to the total IT budget by country samples



Budget allocated to data protection. Figure 33 reports the percentage of data protection spending relative to the total IT security budget over eight 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 33. Trend in the percent of IT security spending dedicated to data protection activities

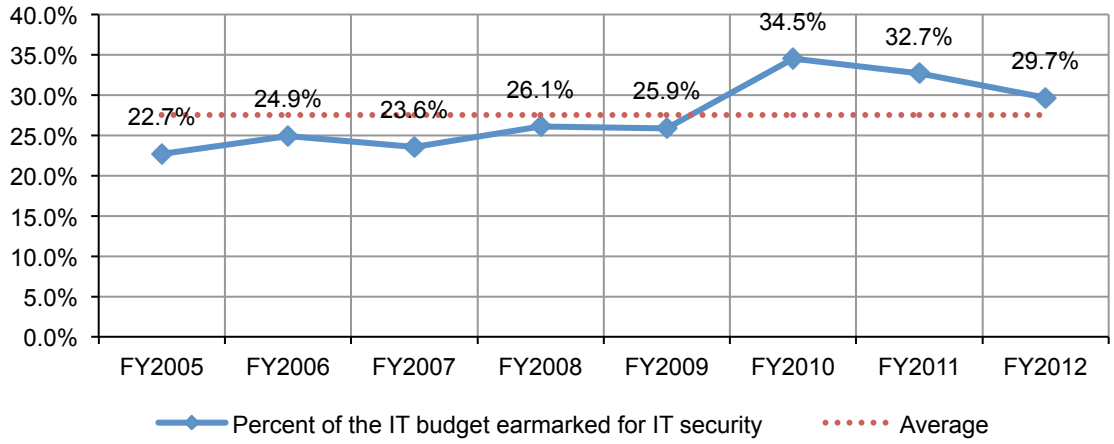
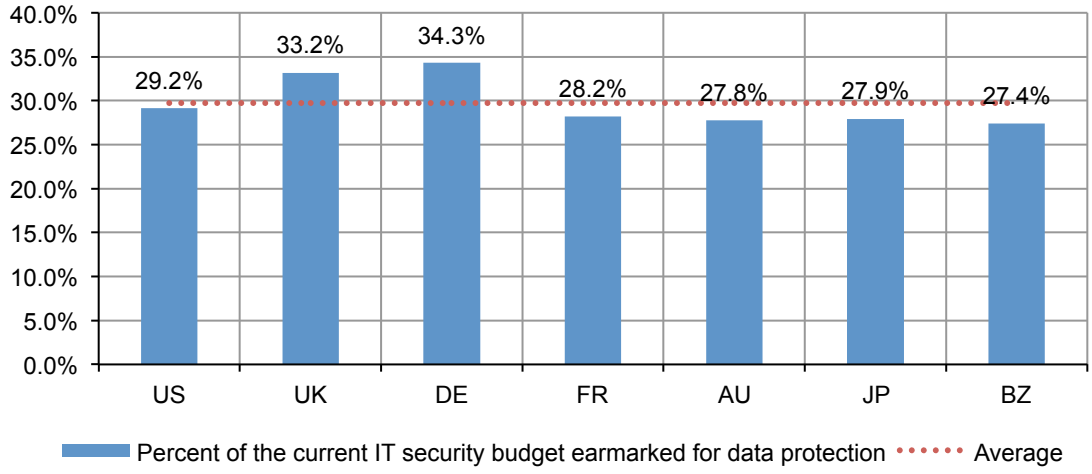


Figure 34 shows the average percent of current IT security spending dedicated to data protection spending by country sample. As shown, the percentage of data protection spending relative to total IT security is highest in Germany and lowest in Brazil. Perhaps more important is the consistency in percentage values observed across most countries.

Figure 34. Percent of current IT security spending dedicated to data protection activities by country samples



Budget allocated to encryption. Figure 35 reports the eight-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 17.6 percent in the present year's encryption trends study.

Figure 35. Trend in the percent of IT security budget dedicated to encryption

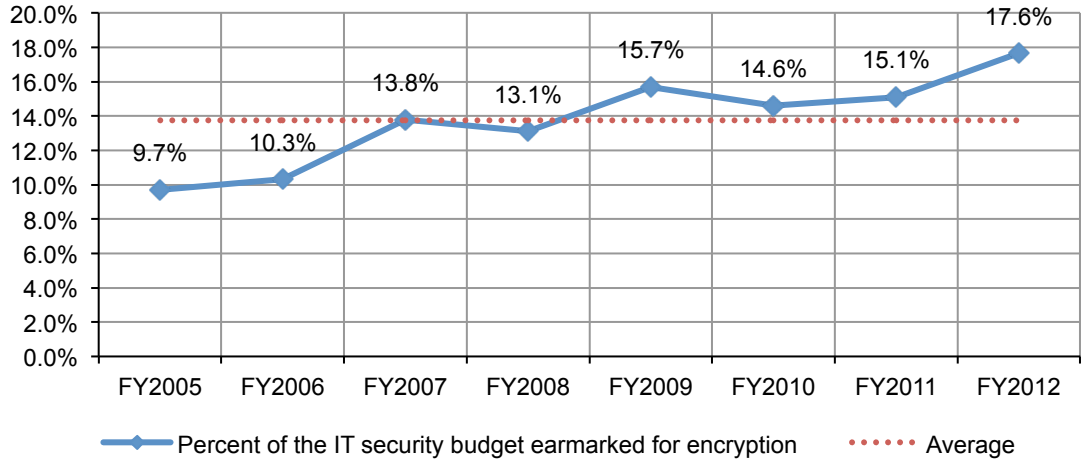
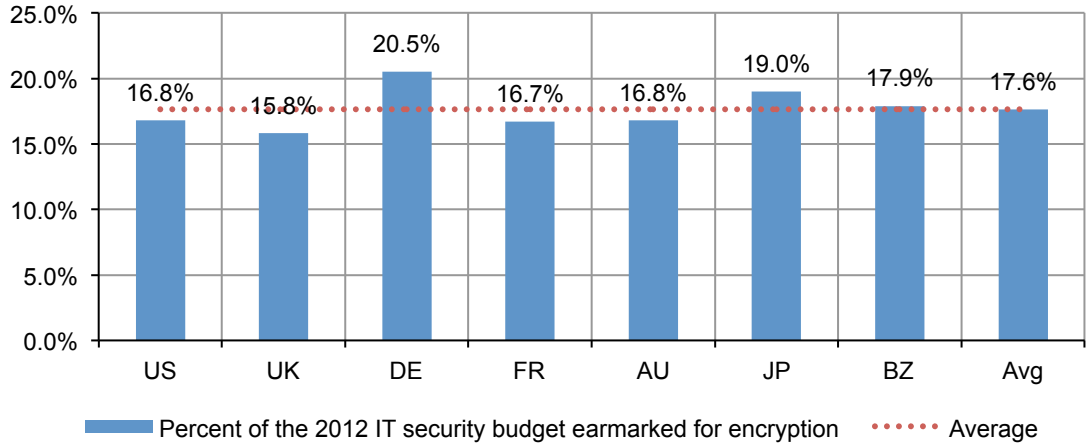


Figure 36 reports the percentage of IT security spending dedicated to encryption.[9] Again, the country comparisons are very consistent. Respondents in Germany show the highest average percentage of encryption spending, while those in the UK show the lowest average percentage spending levels.

Figure 36. Percent of the IT security budget dedicated to encryption by country samples



[9]The figures in this graph suggest that encryption spending represents nearly 60 percent of the total data protection budget (which is a subset of the total IT security budget). However, debriefing interviews with a subset of respondents revealed that encryption spending might not be contained solely in the data protection category, but rather other earmark categories such as security technologies.

Budget allocated to key management. Figure 37 reports the two-year comparison in the percentage of encryption key management spending as a proportion of the overall encryption spend, showing a six percent increase.[10]

Figure 37. Budget allocation to key management

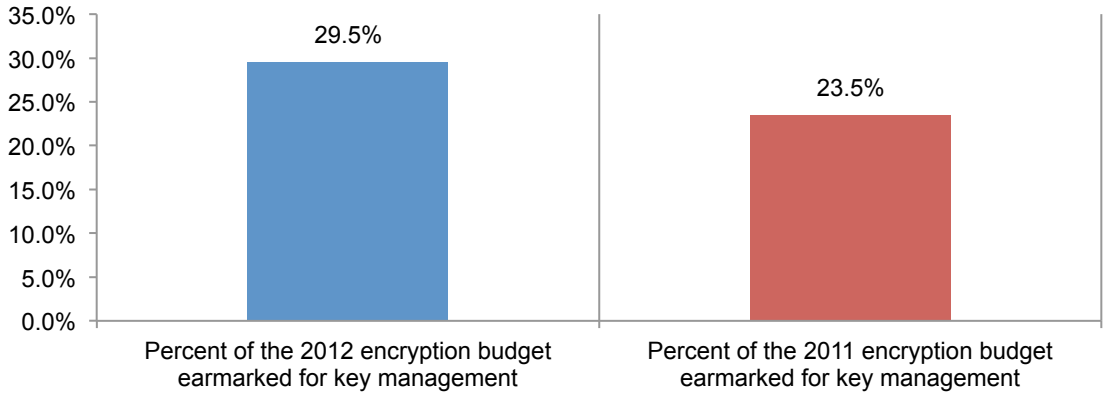
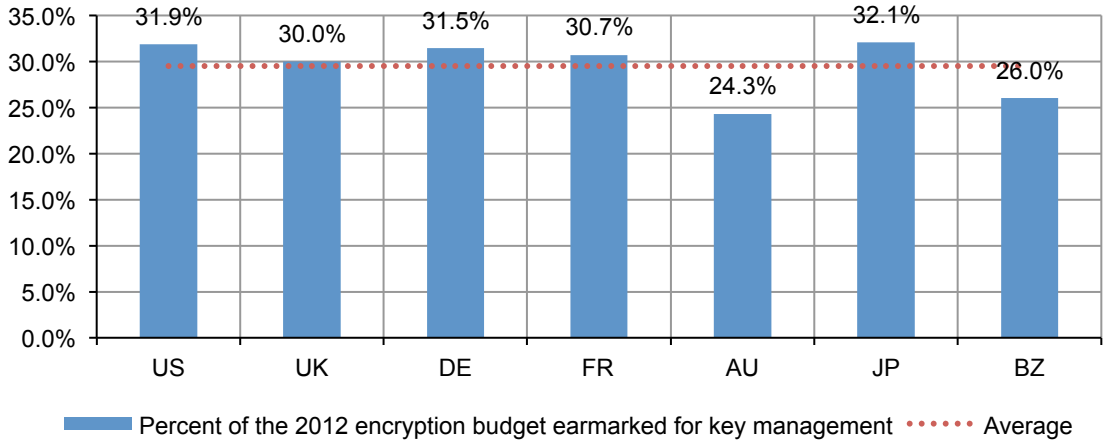


Figure 38 reports the proportion of spending on key management relative to the total spending on encryption solutions for country samples. Perhaps the most interesting finding is the consistency in spending on key management across all seven countries, with the exception of Australia and Brazil.

Figure 38. Percent of encryption spending dedicated to key management activities by country samples



[10]The analysis of key management spending was first conducted in 2011 and, hence, we don't have the ability to conduct a formal trend analysis.

Part 3. Methods & Limitations

Table 2 reports the sample response for seven separate country samples. The sample response for this study conducted over a 50-day period ending in December 2012. Our consolidated sampling frame of practitioners in all countries consisted of 115,217 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 4,670 returns of which 465 were rejected for reliability issues. Our final consolidated 2012 sample was 4,205, thus resulting in a 3.6% response rate.

The first encryption trends study was conducted in the US in 2005.[11] Since then we have expanded the scope of the research to include seven separate country samples. Trend analysis was performed on combined country samples. As noted below, we added Brazil in 2011. As illustrated in various figures, Brazil appears to be less mature in terms of encryption awareness and deployment decisions. Further, Brazilian organizations tend to have a lower SES than other countries. As a result, the inclusion of Brazil may have dampened upward trends for the other countries included in this research.

Table 2. Sample response in seven countries

Countries	Sampling frame	Total returns	Rejected surveys	Final sample
United States	27,763	1,037	99	938
United Kingdom	16,371	710	73	637
Germany	16,989	638	54	584
France	16,952	585	86	499
Australia	9,810	506	40	466
Japan	13,400	594	44	550
Brazil	13,932	600	69	531
Totals	115,217	4,670	465	4,205

As noted in Table 3, the respondents' average (mean) experience in IT, IT security or related fields is 9.95 years. Approximately 26 percent of respondents are female and 74 percent male.[12]

Table 3. Other characteristics of respondents

Experience levels	Mean	Gender	Combined%
Overall experience	10.27	Female	26%
IT or security experience	9.95	Male	74%

[11]The following matrix summarizes the samples and sample sizes used in all figures showing trends.

Country/year	2012	2011	2010	2009	2008	2007	2006	2005
Australia	938	471	477	482	405	0	0	0
Brazil	637	525	0	0	0	0	0	0
France	584	511	419	414	0	0	0	0
Germany	499	526	465	490	453	449	0	0
Japan	466	544	0	0	0	0	0	0
United Kingdom	550	651	622	615	638	541	489	0
United States	531	912	964	997	975	768	918	791
Total	4,205	4,140	2,947	2,998	2,471	1,758	1,407	791

[12]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 seven countries sampled.

Figure 38 summarizes the approximate position levels of respondents in our study. As can be seen, the majority (53 percent) of respondents are at or above the supervisory level.

Figure 38. Distribution of respondents according to position level
Consolidated from seven separate country samples

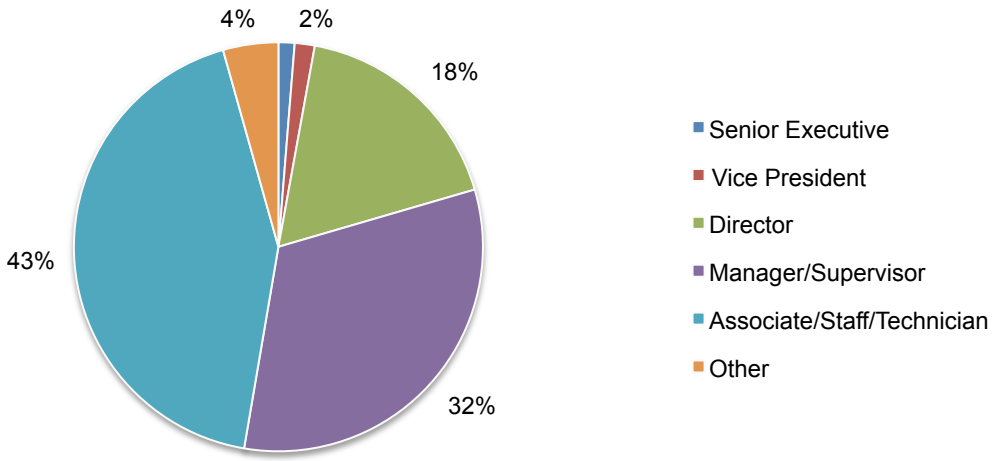
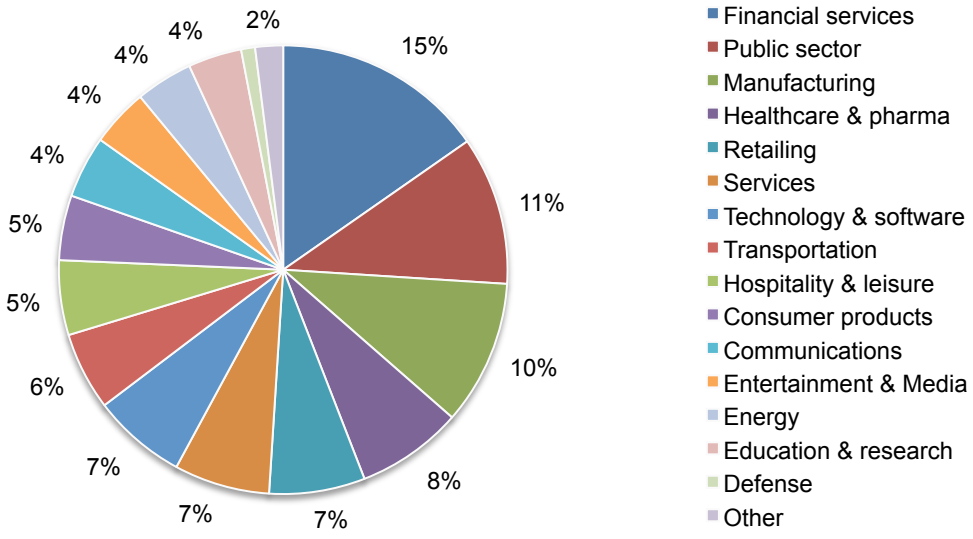


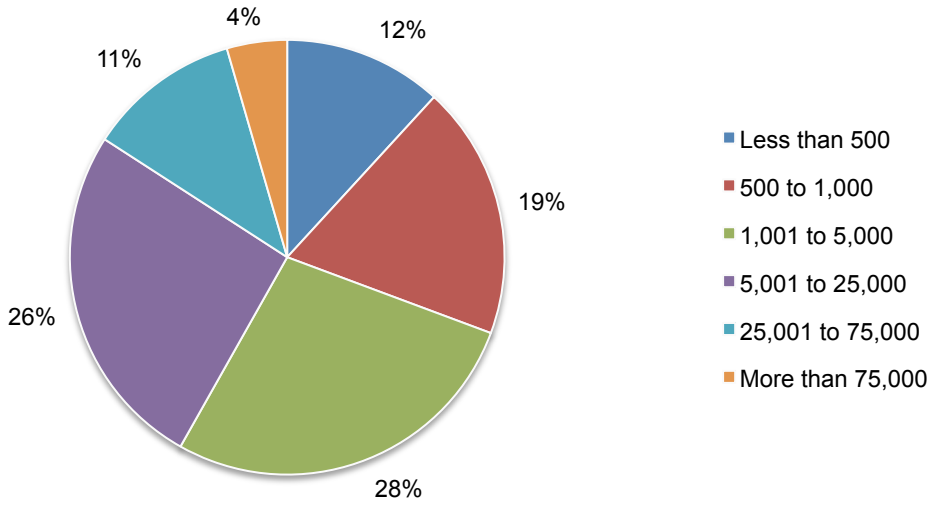
Figure 39 reports the respondents' organizations primary industry segments. As shown, 15 percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 11 percent are located in public sector organizations, including central and local government.

Figure 39. Distribution of respondents according to primary industry classification
Consolidated from seven separate country samples



According to Figure 40, the majority of respondents (69 percent) are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 40. Distribution of respondents according to organizational headcount
Consolidated for seven 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 seven 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 seven 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: Consolidated Findings

The following tables provide the percentage frequencies for all survey questions (combined) presented in this report. The consolidated survey results for seven separate country samples are reported. All survey responses were gathered over a 36-day period ending in December 2012. Please note that certain survey questions were omitted.

Part 1: Your organization's encryption posture

Q1. Please check one statement that best describes your organization's approach to encryption implementation across the enterprise.	Combined
We have an overall encryption plan or strategy that is applied consistently across the entire enterprise	29%
We have an overall encryption plan or strategy that is adjusted to fit different applications and data types	24%
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	25%
We don't have an encryption plan or strategy	22%
Total	100%

.

Q2a. Does your organization encrypt sensitive and confidential data when sending it by email?	Combined
Yes, most of the time	21%
Yes, some of the time	45%
No	34%
Total	100%

Q2b. Does your organization encrypt sensitive and confidential data stored on shared storage such as a file server?	Combined
Yes, most of the time	23%
Yes, some of the time	44%
No	33%
Total	100%

Q2c. Does your organization encrypt sensitive and confidential data stored on a laptop computer?	Combined
Yes, most of the time	27%
Yes, some of the time	42%
No	30%
Total	100%

Q2d. Does your organization encrypt sensitive and confidential data stored on a desktop or workstation?	Combined
Yes, most of the time	26%
Yes, some of the time	46%
No	28%
Total	100%

Q2e. Does your organization encrypt sensitive and confidential data stored on a mobile data-bearing device such as a smart phone or tablet?	Combined
Yes, most of the time	22%
Yes, some of the time	38%
No	40%
Total	100%

Q2f. Does your organization encrypt sensitive and confidential data stored on backup files or tapes before sending it to off site storage locations?	Combined
Yes, most of the time	36%
Yes, some of the time	36%
No	28%
Total	100%

Q2g. Does your organization encrypt sensitive and confidential data when sending it by external public networks such as the Internet?	Combined
Yes, most of the time	29%
Yes, some of the time	45%
No	26%
Total	100%

Q2h. Does your organization encrypt sensitive and confidential data when sending it by internal networks?	Combined
Yes, most of the time	28%
Yes, some of the time	42%
No	30%
Total	100%

Q2i. Does your organization encrypt sensitive and confidential data located in databases?	Combined
Yes, most of the time	28%
Yes, some of the time	46%
No	26%
Total	100%

Q2j. Does your organization encrypt sensitive and confidential data within business software applications that are exposed to it?	Combined
Yes, most of the time	27%
Yes, some of the time	43%
No	29%
Total	100%

Q2k. Does your organization encrypt sensitive and confidential data that is passed to external cloud based services?	Combined
Yes, most of the time	28%
Yes, some of the time	45%
No	27%
Total	100%

Q3. In your organization, who has responsibility or is most influential in directing your organization's strategy for using encryption? Please check the one best choice.	Combined
No single function has responsibility	23%
IT operations	37%
Finance	2%
Lines of business (LOB)	22%
Security	14%
Compliance	2%
Other	0%
Total	100%

Q4. What are the reasons why your organization encrypts sensitive and confidential data? Please check the top two reasons.	Combined
To lessen the impact of data breaches	42%
To avoid having to notify customers or employees after a data breach occurs	5%
To ensure that our organization's privacy commitments are honored	37%
To protect our company's brand or reputation	44%
To comply with privacy or data security regulations and requirements	38%
To reduce the scope of compliance audits	21%
Total	187%

Q5a. With respect to your organization's enterprise data protection priorities, please rank the following ten (10) key activities from 1=highest priority to 10=lowest priority. If possible, please avoid tied ranks.	Combined
Classify data at risk	4.3
Discover data at risk	2.3
Protect data in motion over internal networks	7.9
Protect data in motion over external networks	5.5
Protect data at rest on laptops and workstations	4.6
Protect data at rest on file servers, storage infrastructure and archives	3.6
Identity and access management	2.2
Protect data in outsourced or cloud-based environments	2.5
Protect data in use within business applications	2.4
Protect data at point of collection (e.g., point of sale)	4.3

Q5b. With respect to your organization's enterprise data protection priorities, please rank the following ten (10) key activities from 1=highest priority to 10=lowest priority. If possible, please avoid tied ranks.	Combined
Classify data at risk	6.6
Discover data at risk	2.6
Protect data in motion over internal networks	9.9
Protect data in motion over external networks	8.3
Protect data at rest on laptops and workstations	6.7
Protect data at rest on file servers, storage infrastructure and archives	5.1
Identity and access management	2.9
Protect data in outsourced or cloud-based environments	3.1
Protect data in use within business applications	2.9
Protect data at point of collection (e.g., point of sale)	6.9

Q6. What are the main threats that might result in the exposure of sensitive or confidential data? Please select your top two choices.	Combined
Hackers	14%
Malicious insiders	11%
System or process malfunction	15%
Employee mistakes	26%
Temporary or contract workers	8%
Third party service providers	9%
Legal and law enforcement (e.g., e-discovery)	16%
Other (please specify)	1%
Total	100%

Q7. How important are the following features associated with encryption solutions that may be used by your organization? Please rate each feature using the adjacent scale from very important to irrelevant.	Combined
Automated enforcement of policy	63%
Automated management of keys	66%
Support for the widest range of applications	51%
Centralized management interface	65%
System scalability	59%
Tamper resistance by dedicated hardware (e.g. HSM)	58%
Conformance with security standards	63%
Support for format preserving encryption (FPE)	51%
System performance and latency	67%
Support for emerging algorithms (e.g. ECC)	61%
Supports longer encryption keys	48%
Formal product security certifications (e.g. FIPS 140)	55%

Part 2: Cloud encryption questions will be presented in forthcoming paper

Part 3: IT security & encryption budget

Q9a. Are you responsible for managing all or part of your organization's IT budget in 2012?	Combined
Yes	57%
No (Go to Part 4)	43%
Total	100%

Q9b. Approximately, what is the dollar range that best describes your organization's IT budget for 2012?	NA
Extrapolated average value in millions (billions for JPY)	

Extrapolated values computed from scaled responses	Combined
Q9c. Approximately, what percentage of the 2012 IT budget will go to IT security activities?	9%
Q9d. Approximately, what percentage of the 2012 IT security budget will go to data protection activities?	30%
Q9e. Approximately, what percentage of the 2012 IT security budget will go to encryption activities?	18%
Q9f. Approximately, what percentage of the 2012 encryption budget will go to key management activities?	30%
Q10b. Approximately, what percentage of the 2013 IT security budget will go to encryption activities?	30%
Q10c. Approximately, what percentage of the 2013 encryption budget will go to encryption key management activities?	27%

Q10a. Please check the security initiatives that will be earmarked in the 2013 budget? Select all that apply.	Combined
Identity & access management	50%
Intrusion detection and prevention systems	88%
Data loss prevention	19%
Encryption solutions	55%
Key and certificate management	39%
Security intelligence (e.g., SIEM)	19%
Tokenization	18%
Public key encryption (PKI)	38%
Database monitoring & behavior analysis	54%
Endpoint security	37%

Part 4. Encryption key management

Q11a. Does your organization have a key management strategy that is independent of the various uses of cryptography within your organization?	Combined
Yes	37%
No	63%
Total	100%

Q11b. If yes, what are the primary drivers for developing a key management strategy? Please select the top two choices?	Combined
Increase business efficiency	50%
Reduce operational cost	42%
Reduce complexity	31%
Demonstrate compliance	30%
Improve security	33%
Other (please specify)	0%
None of the above	4%
Total	190%

Q12a. What types of key management systems (KMS) does your organization use? Please select all that apply.	Combined
Single key management system deployed across the organization to manage multiple use cases (e.g. tape backup, email, etc)	28%
Single key management system deployed across the organization to manage a single use case	23%
Multiple installations of a common key management system that is deployed throughout the organization to address the same use case	25%
Multiple and different key management systems each deployed for specific use cases (e.g. tape backup, email, etc)	24%
Total	100%

Q12b-1. How many separate key management systems are used today?	Combined
1	20%
2	20%
3	20%
4	6%
5	16%
6 to 10	11%
More than 10	7%
Total	100%
Extrapolated value	3.94

Q12b-2. How many separate key management systems will be used in the next 12 months?	Combined
1	19%
2	18%
3	16%
4	9%
5	18%
6 to 10	13%
More than 10	7%
Total	100%
Extrapolated value	4.16

Q12c. What is the source of your organization's key management system(s)? Please check all that apply.	Combined
In-house development	15%
Externally developed custom system	9%
Native capability or bundled item with an encryption solution	38%
Commercial, off-the-shelf centralized key management system	39%
Commercial , off-the-shelf key management component e.g. HSM	24%
Other (please specify)	2%
None of the above	11%
Total	137%

Q12d Does your organization operate its own internal PKI?	Combined
Yes	22%
No	78%
Total	100%

Q13. What best describes your level of knowledge about KMIP?	Combined
Very knowledgeable	23%
Knowledgeable	34%
Not knowledgeable	26%
No knowledge (Go to Q17)	17%
Total	100%

Q14. Does your organization deploy KMIP as part of its key management activities?	Combined
Yes	23%
No, but we plan to do so in the next 12 months	24%
No	53%
Total	100%

Q15. In your opinion, how important is KMIP to your key management strategy?	Combined
Q15a. Importance today	27%
Q15b. Importance in the next 12 months	33%

Q16. In what areas of your encryption and key management strategy is KMIP most important? Please select you top two choices.	Combined
Storage systems	36%
Application infrastructure within the datacenter	35%
End user devices e.g. laptops, tablets or smartphones	12%
Remote applications e.g. retail locations	16%
Cloud based applications and storage	42%
Network infrastructure	35%
Other (please specific)	1%
None	9%
Total	187%

Q17. What best describes your level of knowledge about HSMs?	Combined
Very knowledgeable	23%
Knowledgeable	37%
Not knowledgeable	27%
No knowledge (Go to Part 5)	12%
Total	100%

Q18a. Does your organization deploy HSMs?	Combined
Yes	27%
No, but we plan to do so in the next 12 months	32%
No	42%
Total	100%

Q18b. How many HSMs does your organization currently deploy?	Combined
1 to 5	26%
6 to10	24%
11 to15	15%
16 to 20	13%
21 to 50	14%
More than 50	8%
Total	100%

Q18c-1.For what purpose does your organization presently deploy HSMs?	Combined
Application level encryption	39%
Database encryption	50%
SSL	49%
PKI or credential management	25%
Document signing (e.g. electronic invoicing)	16%
Code signing	8%
Authentication	52%
Payments processing	37%
Other (please specify)	1%
Total	276%

Q18c-2. For what purpose does your organization plan to deploy HSMs in the next 12 months?	Combined
Application level encryption	44%
Database encryption	54%
SSL	52%
PKI or credential management	29%
Document signing (e.g. electronic invoicing)	24%
Code signing	18%
Authentication	55%
Payments processing	41%
Other (please specify)	0%
Total	318%

Q19. How important is HSM to your encryption or key management strategy?	Combined
Q19a. Importance today	39%
Q19b. Importance in the next 12 months	44%

Q20. Who are your primary vendors for HSM products and services? Please select all that apply.	Combined
Thales/nCipher	13%
SafeNet/Eracom	14%
IBM	19%
Symantec/Utimaco	15%
HP/Atalla	8%
FutureX	4%
Bull	5%
Other (specify)	3%
None of the above (not using HSM)	41%

Part 5: Data security threats

Q21. Did your organization experience a data breach in the past 12 month period?	Combined
Yes, only one incident	30%
Yes, two to five incidents	22%
Yes, more than five incidents	14%
No	34%
Total	100%

Q22. Did your organization have to disclose a data breach in the past 12 month period?	Combined
Yes, only one incident	8%
Yes, two to five incidents	10%
Yes, more than five incidents	10%
No	71%
Total	100%

Q23. In which global regions does your organization devote most of its resources for managing compliance with privacy and data protection laws? Please select the top two.	Combined
North America	51%
Europe (EU countries)	57%
Europe (non-EU countries)	20%
Middle east & Africa	14%
Asia-Pacific	33%
Latin America	18%
Total	194%

Part 6: Standard SES questions will be provided upon request	
Computed value based on 48 items from combined sample	0.512

Part 7: Your role

D1. What organizational level best describes your current position?	Combined
Senior Executive	1%
Vice President	2%
Director	18%
Manager/Supervisor	32%
Associate/Staff/Technician	43%
Other	4%
Total	100%

D2. Check the functional area that best describes your organizational location.	Combined
IT operations	55%
Security	14%
Compliance	8%
Finance	4%
Lines of business (LOB)	16%
Other	2%
Total	100%

D3. Total years of business experience (mean value)	Combined
Total years of security experience	9.95
Total years in current position	5.50

D4. What industry best describes your organization's industry focus?	Combined
Financial services	15%
Public sector	11%
Technology & software	7%
Healthcare & pharmaceutical	8%
Manufacturing	10%
Communications	4%
Consumer products	5%
Hospitality & leisure	5%
Transportation	6%
Retailing	7%
Services	7%
Defense	1%
Education & research	4%
Energy	4%
Entertainment & Media	4%
Other	2%
Total	100%

D5. Where are your employees located? (check all that apply):	Combined
United States	76%
Canada	58%
Europe	79%
Middle east & Africa	32%
Asia-Pacific	60%
Latin America	35%
Total	340%

D6. What is the worldwide headcount of your organization?	Combined
Less than 500	12%
500 to 1,000	19%
1,001 to 5,000	27%
5,001 to 25,000	26%
25,001 to 75,000	11%
More than 75,000	4%
Total	100%

About Thales e-Security
Thales e-Security is a leading global provider of data encryption and cyber security solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 70 percent of worldwide payment transactions. Thales e-Security has offices in France, Hong Kong, Norway, United States and the United Kingdom. www.thales-esecurity.com.

About Thales
Thales is a global technology leader for the Defense & Security and the Aerospace & Transport markets. In 2011, the company generated revenues of €13 billion with 68,000 employees in more than 50 countries. With its 22,500 engineers and researchers, Thales has a unique capability to design, develop and deploy equipment, systems and services that meet the most complex security requirements. Thales has an exceptional international footprint, with operations around the world working with customers as local partners. www.thalesgroup.com.

About Ponemon Institute
Ponemon Institute is dedicated to independent research and education that advances information security, data protection and privacy management practices within businesses and governments. Our mission is to conduct high quality, empirical studies on critical issues affecting the security of information assets and the IT infrastructure. As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. www.ponemon.org.