2011 Global Encryption Trends Study

Organizations increase the deployment of encryption in response to compliance regulations and cyber attacks

---

Sponsored by Thales e-Security

Independently conducted by Ponemon Institute LLC

Publication Date: February 2012

2011 Global Encryption Trends Study

2011 Global Encryption Trends Study[1]

Ponemon Institute, February 2012

Part 1. Executive Summary

Ponemon Institute is pleased to present the findings of *the 2011 Global Encryption Trends Study,* sponsored by Thales e-Security. We surveyed 4,140 business and IT managers in 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 and its impact on the security posture of an organization. The first encryption trends study was conducted in the US in 2005.[3] Since then we have expanded the scope of the research to include 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. For the first time we profile organizations according to their level of awareness about security issues and the actions taken to address these issues. Based on this profile, we are able to demonstrate the role encryption plays in helping an organization create a strong security posture.

In this year's study we asked questions about risk management, standards of due care for crypto deployment, tokenization practices, migration to the cloud, data breaches their organization experienced and effectiveness of their company's IT security and data protection efforts. 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:

- High awareness and high action index values. Organizations that understand the threats against them are more likely to have a strategy to reduce those threats.
- Place a high level of importance on data protection activities as an integral part of their risk management efforts.
- Have a formal encryption strategy that spans the entire enterprise.
- Attach a high level of importance to the automated key management and encryption of data.
- Are more likely to dedicate a larger proportion or share of their IT security budget to encryption and key management solutions.
- Show a high level of awareness and acceptance of established deployment best practices – what we have called "standards of due care."
- Are more likely to favor a one unifying solution to encryption key management across the enterprise.

---

[1]The reporting date of the trends series pertains to the year of completion, not publication. This year's study was completed in November 2011 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 seven years (since 2005).

Summary of key findings:

- **Encryption usage is an indicator of a strong security posture.** Organizations that deploy encryption are more aware of threats to sensitive and confidential information and spend more on IT security. In other words, the use of encryption is a barometer of a company's overall security posture.

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

- **The use of encryption as an enterprise security solution is growing.** The encryption of backup files, internal networks, external communications and laptops are most likely to be extensively deployed. In contrast, smart phone, email and file server encryption solutions are the least likely to see enterprise-wide deployment.

- **Since 2005, more organizations are adopting an overall encryption plan or strategy.** Organizations in Germany, US and Japan are most mature in developing an enterprise encryption strategy, while organizations in France and Brazil are least mature.

- **Business unit leaders are gaining influence over their company's use of encryption solutions.** While IT leaders are still most influential in determining the use of encryption (especially in Australia), non-IT business managers have an increasing role in determining their organization's encryption strategy. The increasing influence of business leaders in choosing encryption solutions may reflect a broader trend in the consumerization of IT.

- **Identity and access management followed by the discovery of data at risk are the top two data protection priorities.** Least important data protection priorities were to minimize the impact of viruses, protect against insecure or outsourced environments and safeguard data transmitted within internal networks.

- **Over 75 percent of US organizations view data protection activities as a very important part of enterprise risk management.** In contrast, the other country ratings are closely aligned between 38 and 45 percent.

- **With respect to client-controlled devices, the most serious threats are employee mistakes and not knowing where the data is located.** With respect to data center systems, the most serious threats are not knowing where data is located, broken business processes, and third party mistakes and mismanagement.

- **Compliance drives budget.** Since 2005, IT security, including encryption, relative to total IT spending has been steadily increasing over time. The highest IT security spending dedicated to data protection occurs in countries that rank compliance with regulations and law as the most important driver for encryption.

NEW: For the first time, our survey captured information about encryption in cloud computing environments. These findings will be featured in a forthcoming report. In addition, we will provide individual executive summaries for each of the seven countries in this year's study.

Part 2. Key Findings

Encryption solutions are shown to strengthen an organization's security posture

Profile of respondents' organizations. We wanted to determine the awareness organizations have about the threats to sensitive and confidential information and if that level of awareness affects the deployment of encryption technologies. The questions used to determine awareness pertain to importance ratings to nine enterprise encryption solution features. The encryption deployment variable is based on the use of eight encryption technologies and whether this use or deployment was enterprise-wide or more limited.

Table 1 organizes all 4,140 data points into one of four high-low conditions. Based on the consolidated findings for all 7 countries, 39 percent of respondents can be categorized as having both a high degree of awareness combined with a high degree of encryption deployment. In contrast, a similar percentage (37 percent) have both a low level of awareness and a low deployment level.

Table 1. Percentage frequency of responses corresponding to high-low awareness and encryption deployment variables

	Encryption deployment		
Awareness	Low	High	Total
High	11%	37%	48%
Low	38%	14%	52%
Total	49%	51%	100%

From these two sets of questions about awareness and deployment of encryption, we compiled two indexes – namely, one dealing with the respondents' level of awareness and the other with deployment or usage. The sum of survey items is scaled to a number between +1 (maximum) and -1 (minimum). Figure 1 shows the behavior of index values for the total sample of 4,140. The scattergram of scaled data points indicates a strong linear relationship between awareness and deployment. In other words, both variables appear to move in the same direction.

Figure 1. Scattergram depicting the relationship between awareness and action

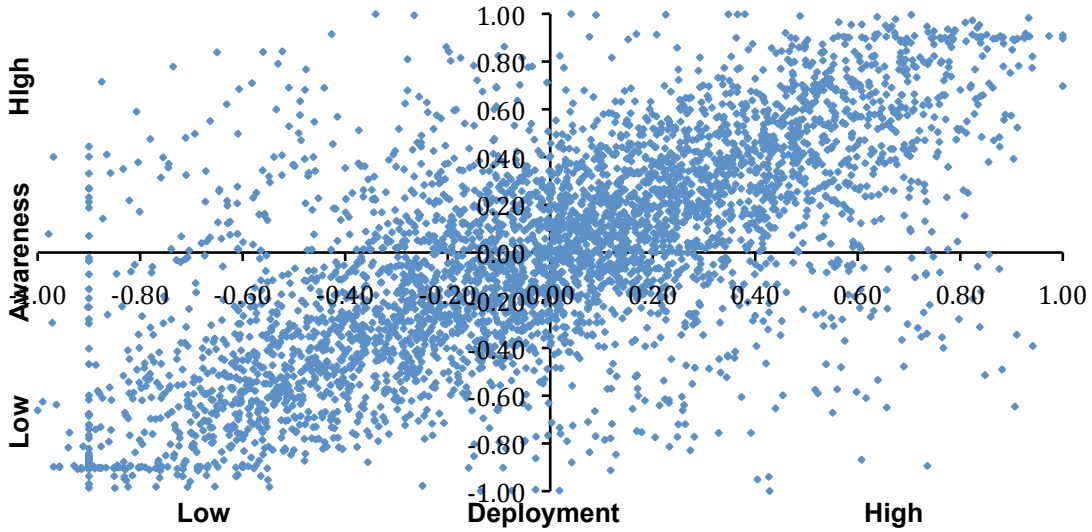


Table 2 describes the business implications for organizations with respect to their location in one of the four quadrants depicted in the scattergram above. Our basic assumption is that awareness (independent variable) drives encryption deployment decisions (dependent variable). The ideal state is defined by the conditions of high awareness and high deployment. Organizations in quadrant one (Q1) are best able to match specific encryption solutions against persistent data risks. This leads to favorable outcomes for both risk mitigation and resource allocation.

We label quadrant four (Q4) as "ignorance is bliss" because organizations in this space do not fully understand or have the know-how to deal with vulnerabilities and threats caused by insecure data. Organizations in quadrant three (Q3) are aware of the security landscape, but they take few steps to secure their data assets. We view organizations in this quadrant as having the highest risk profile because they are most susceptible to criticism and successful litigation in the wake of a data breach. Finally, organizations in quadrant two (Q2) are labeled as least efficient because they lack the knowledge necessary to effectively allocate security resources such as investments in encryption technologies to specific areas of risk or vulnerability.

Table 2. Meaning of the four quadrants

	Low deployment	High deployment
High awareness	**Q3. Highest risk profile.** Organizations are aware of the need for encryption, but they do not make appropriate investment. In a data breach, the company might be subject to charges of gross negligence.	**Q1. Ideal state.** Organizations are aware of the risks relating to insecure data and make the appropriate investments to protect these data assets.
Low awareness	**Q4. Ignorance is bliss.** Organizations are unaware of the a plethora of data risks and take few steps to protect data assets.	**Q2. Lowest efficiency profile** Organizational spending on encryption and other data security solutions is not commensurate with risk and this leads to an inefficient outcome.

Correlation to the security posture of respondents' organizations. To estimate the security posture of organizations, we used the Security Effectiveness Score or SES as part of the survey process.[4] 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. 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.

Figure 2 summarizes the average SES for each country. As shown, Germany achieves the highest score (SES = +1.19), while Brazil has the lowest score (SES = -.48)

Figure 2. Average security effectiveness score (SES) in ascending order by country

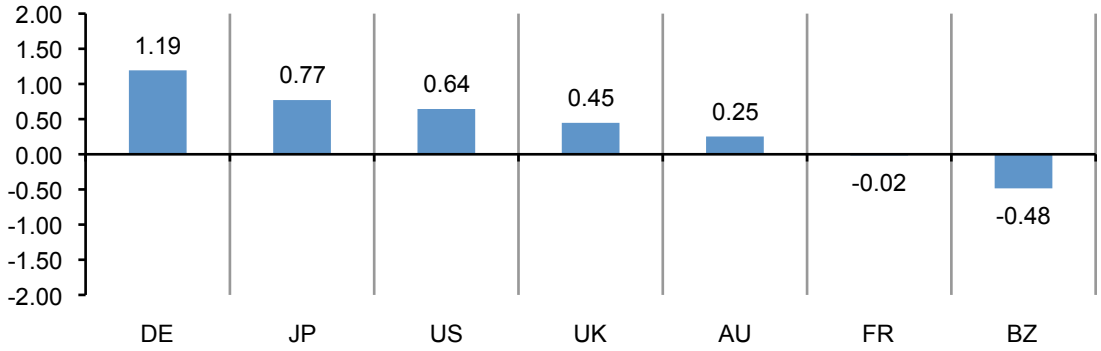
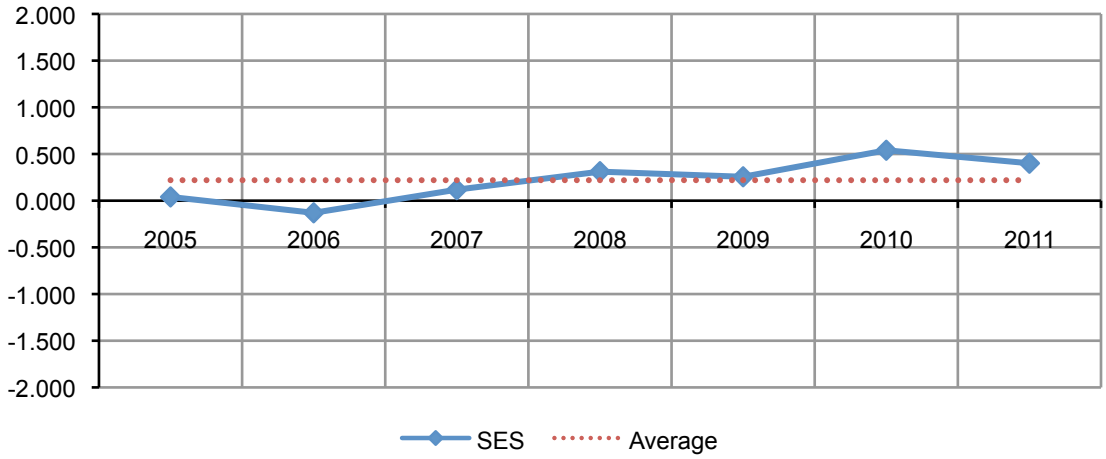


Figure 3 reports the SES results compiled from encryption trend studies over seven years. The trend line shown below is increasing slightly over time, which suggests that the security posture of participating companies has increased over this time period.

Figure 3. Trend in overall average Security Effectiveness Score

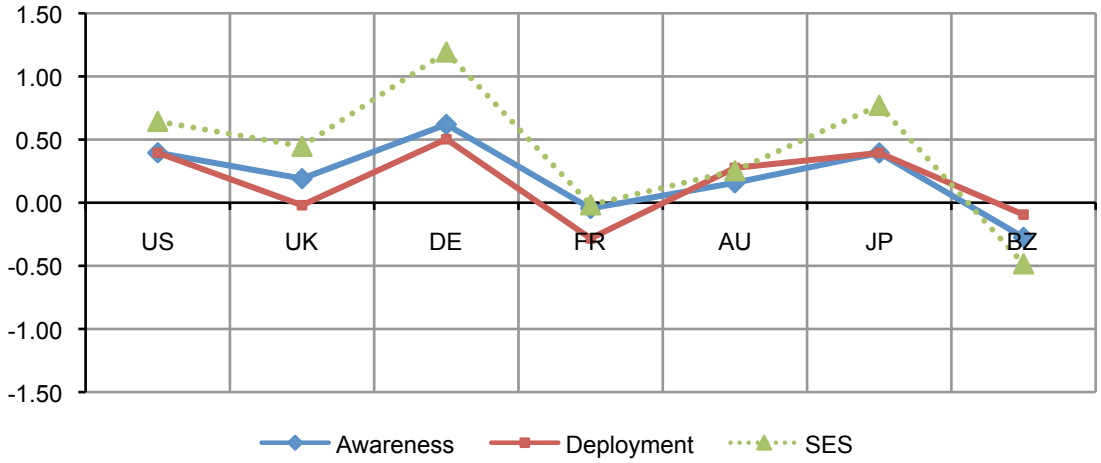


[4] The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent 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.

To determine differences among countries in terms of understanding and responding to general risks, we examined the average index values by country. This is reported in Figure 4. Respondents in Germany, US and Japan report the highest index values for both awareness and deployment variables. This means that organizations in these countries are more likely to understand and respond to data security risks by deploying encryption solutions. France and Brazil have the lowest values, which means organizations in those countries are likely to have a lower level of awareness and, thus, less likely to deploy encryption solutions.

Figure 4 also maps the average SES values by country. As clearly indicated, the SES tracks closely to the awareness and deployment indexes.

Figure 4. Average index values for deployment, awareness and SES by country samples



Main drivers for using encryption are protecting brand or reputation and lessening the impact of data breaches. The following are the main drivers as presented in Figure 5: To protect their organization's brand or reputation if a data breach occurs (45 percent), to lessen the impact of a data breach (40 percent), and to comply with privacy or data security regulations and requirements (39 percent).

Figure 5. The main drivers for using encryption technology solutions

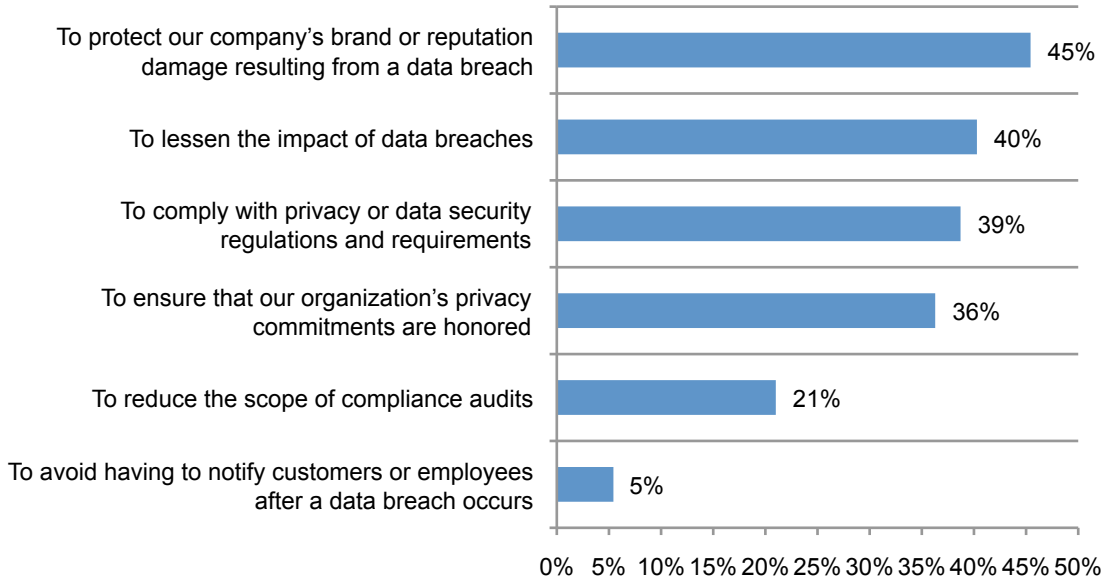
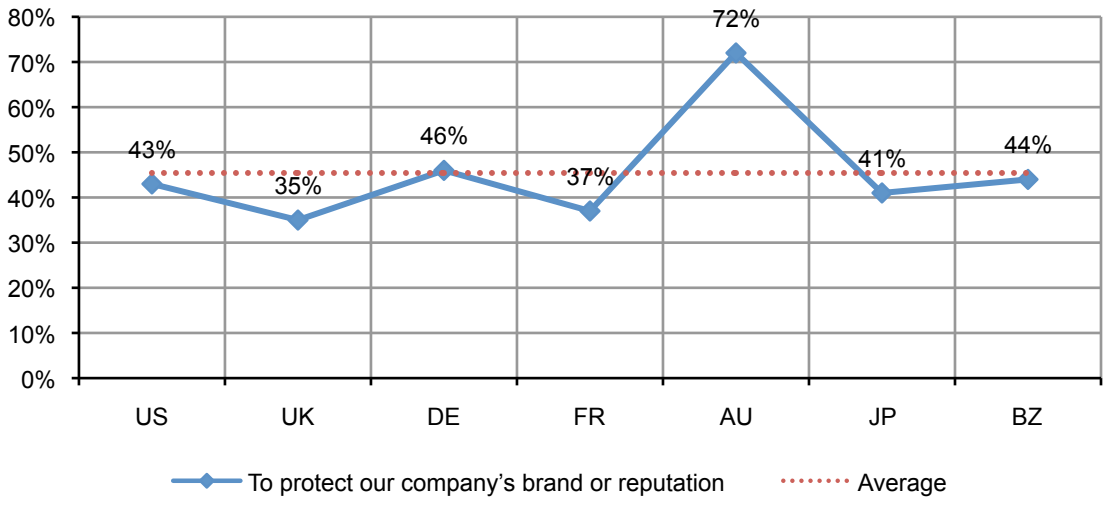


Figure 6 shows responses for seven countries to the top choice – "to protect our company's brand or prevent reputation damage resulting from a data breach." As can be seen, the issue of brand or reputation protection as a main reason for deploying encryption solutions appears to be most important in Australia and least important in the UK.

Figure 6. Importance of reputation as the main driver for encryption by country samples



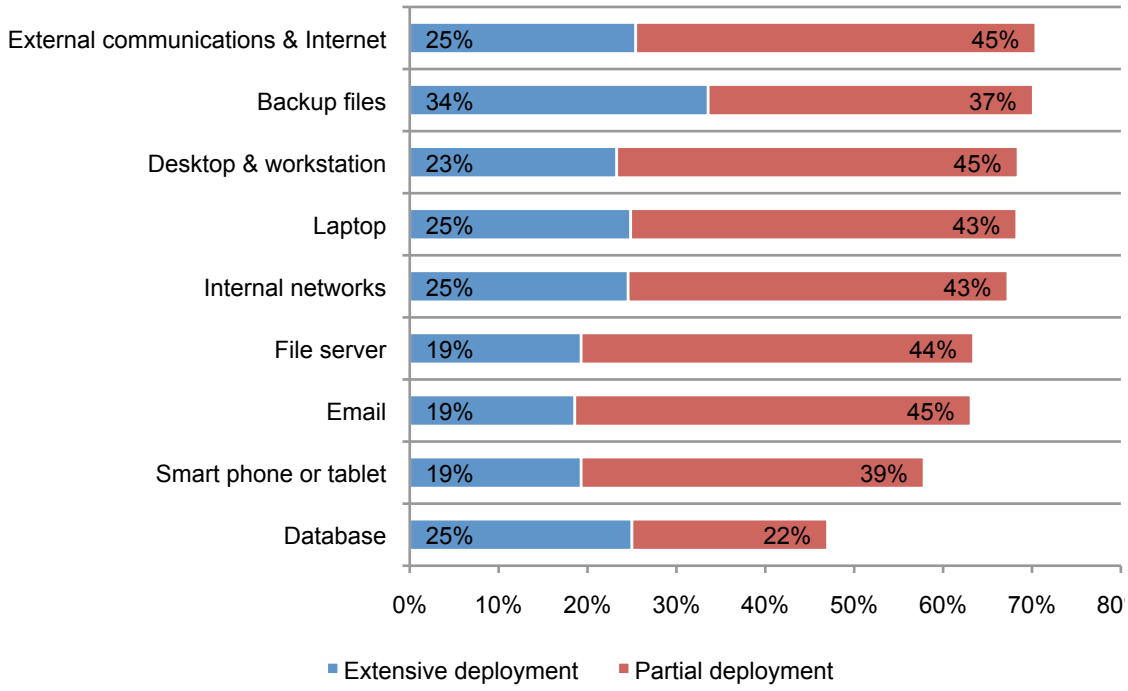
`

While not shown in the above figure, respondents in Germany and Japan are most likely to believe the use of encryption increases customer trust and confidence in their organization's privacy and data protection commitments. In contrast, respondents in Brazil are least likely to believe encryption usage affects customer trust and confidence.

Organizations tend to deploy encryption partially

We asked respondents to indicate if specific encryption solutions are extensively or partially deployed in their organizations. Extensive deployment means that the encryption solution is deployed enterprise-wide and partial deployment means the stated encryption solution is confined or limited to a specific purpose. As shown in Figure 7, encryption of backup files, internal networks, external communications and laptops are most likely to be extensively deployed. In contrast, smart phone, email and file server encryption solutions are the least likely to see extensive deployment.

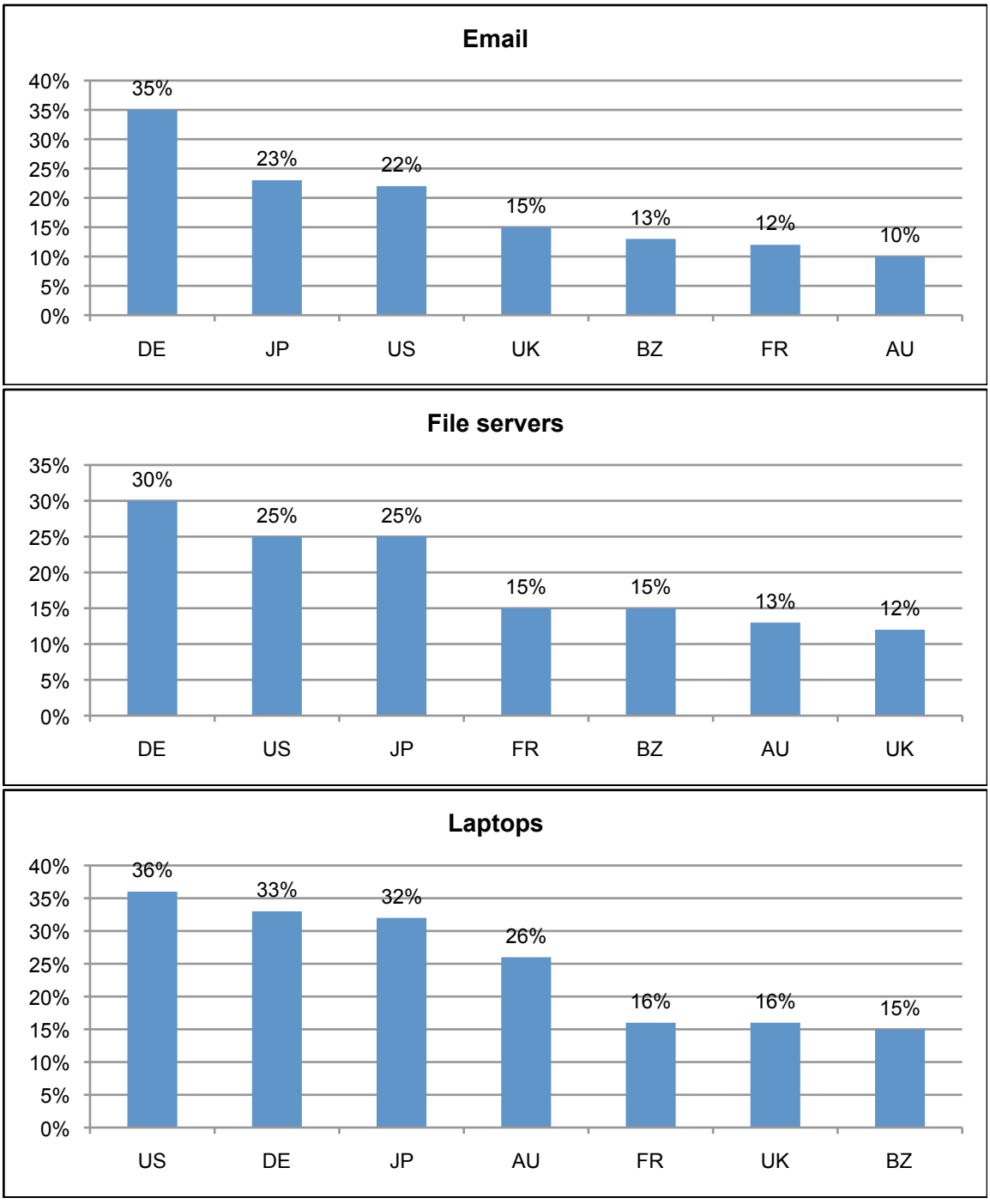
Figure 7. Consolidated view on the use of encryption technologies

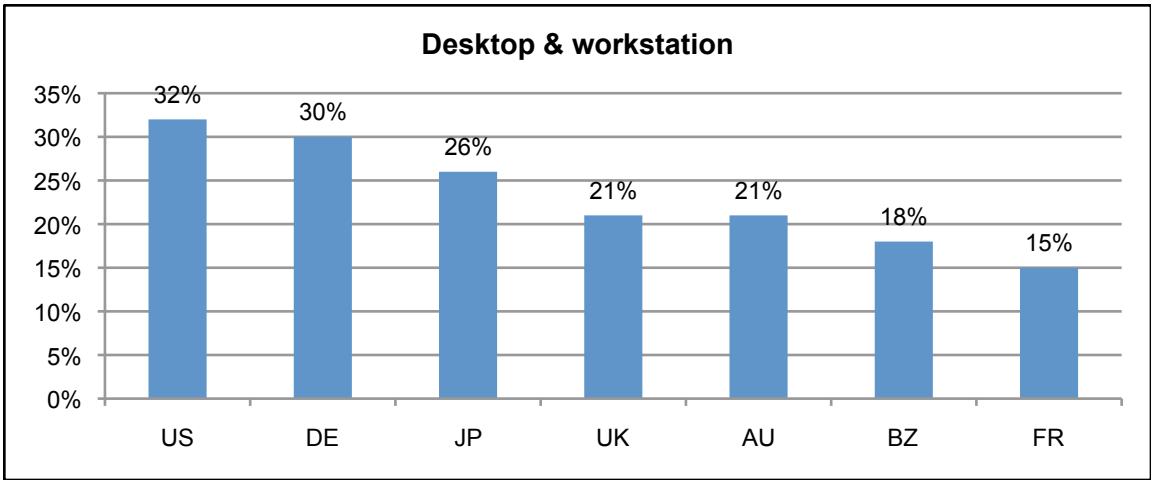


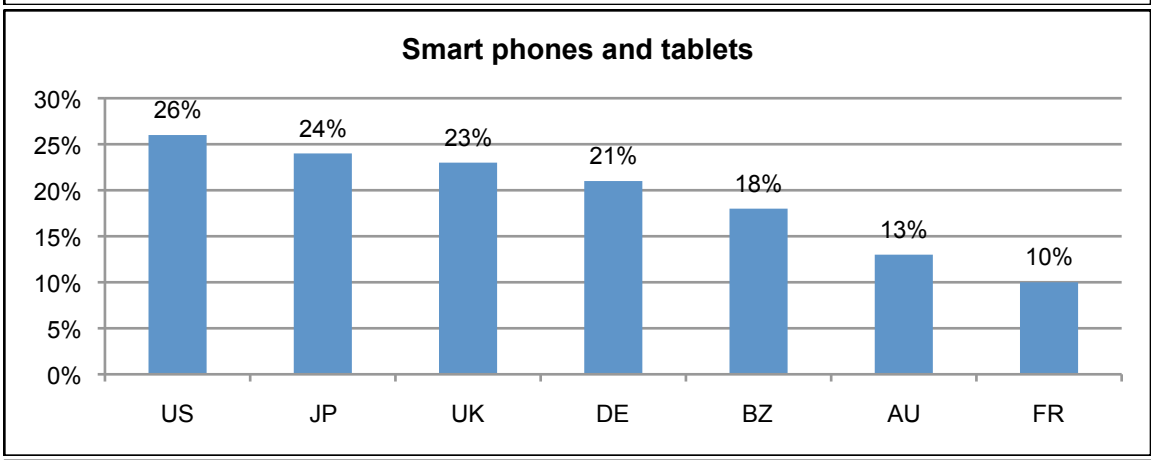
Country-level differences in encryption usage

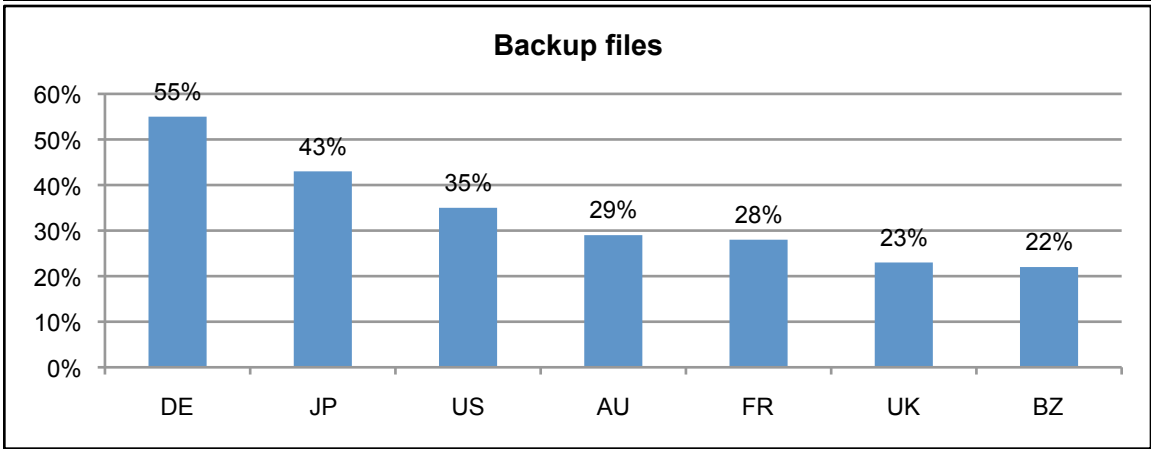
The use of encryption varies greatly among countries. Figure 8 reports the enterprise deployment for nine encryption technologies by country. In general, organizations in Germany, US and Japan enjoy the highest deployment rates. Germany has the highest usage rate in six of nine encryption categories presented in nine panels. Brazil and France tend to have a much lower encryption use rate than all the other countries.

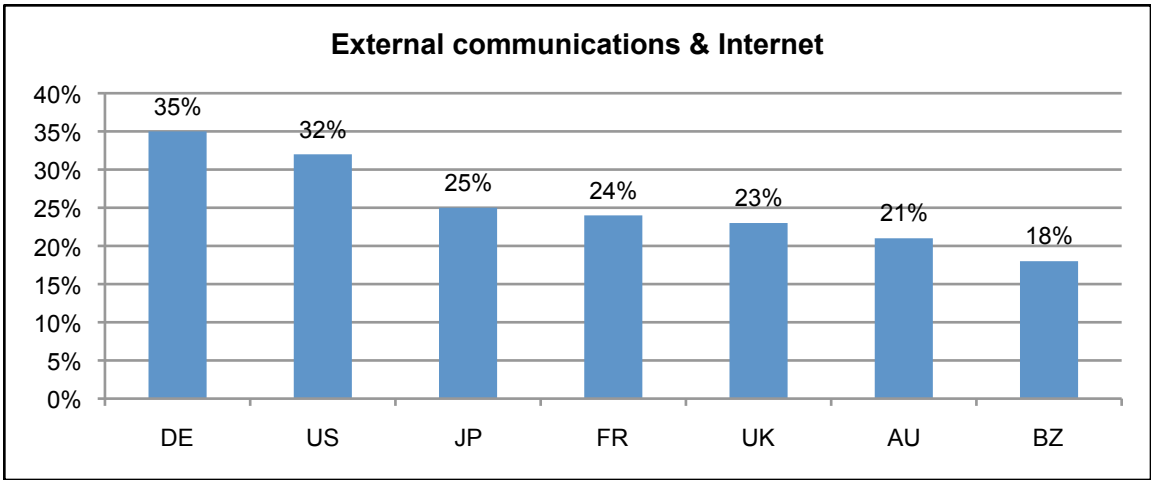
Figure 8. Rates of extensive deployment by country for nine encryption categories

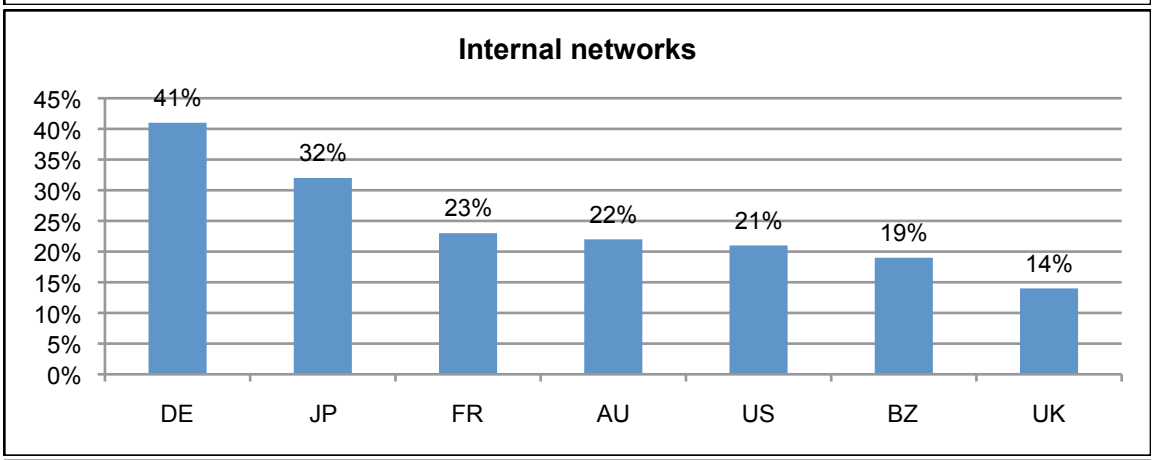


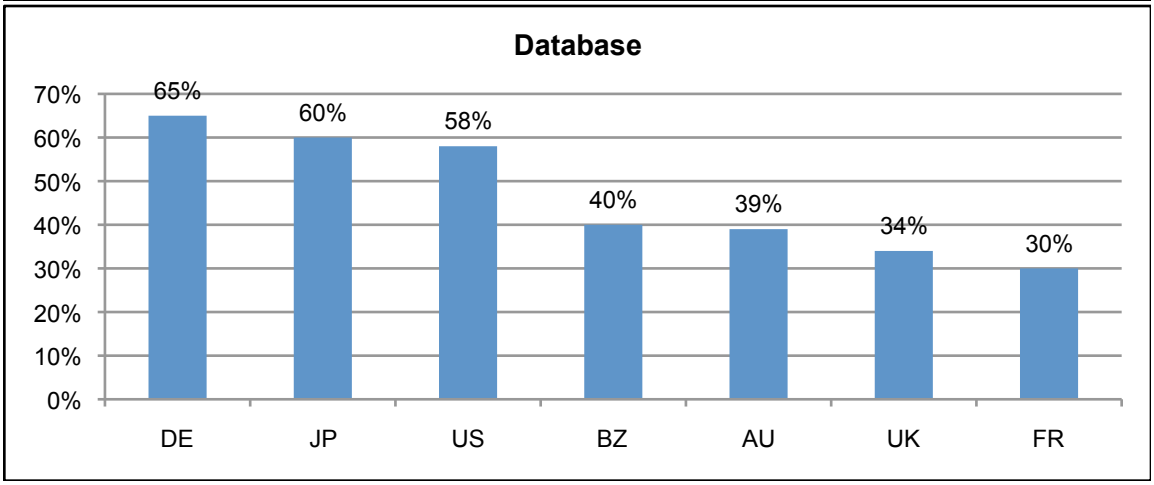

Desktop & workstation
35%
30%
25%
20%
15%
10%
5%
0%
32%
30%
26%
21%
21%
18%
15%
US
DE
JP
UK
AU
BZ
FR


Smart phones and tablets
30%
25%
20%
15%
10%
5%
0%
26%
24%
23%
21%
18%
13%
10%
US
JP
UK
DE
BZ
AU
FR


Backup files
60%
50%
40%
30%
20%
10%
0%
55%
43%
35%
29%
28%
23%
22%
DE
JP
US
AU
FR
UK
BZ


External communications & Internet
40%
35%
30%
25%
20%
15%
10%
5%
0%
35%
32%
25%
24%
23%
21%
18%
DE
US
JP
FR
UK
AU
BZ

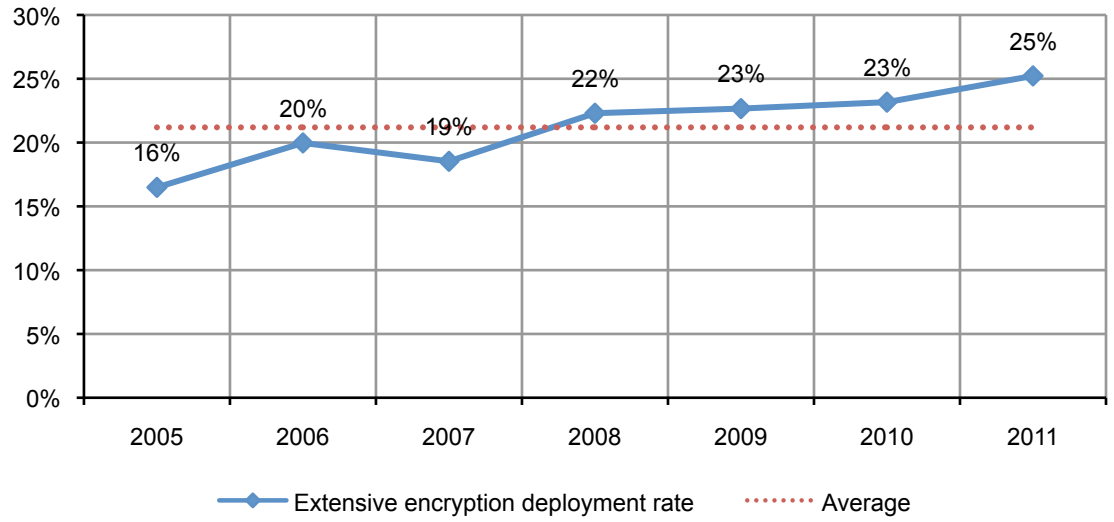

Internal networks
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
41%
32%
23%
22%
21%
19%
14%
DE
JP
FR
AU
US
BZ
UK


Database
70%
60%
50%
40%
30%
20%
10%
0%
65%
60%
58%
40%
39%
34%
30%
DE
JP
US
BZ
AU
UK
FR

Seven-year trend in usage[5]

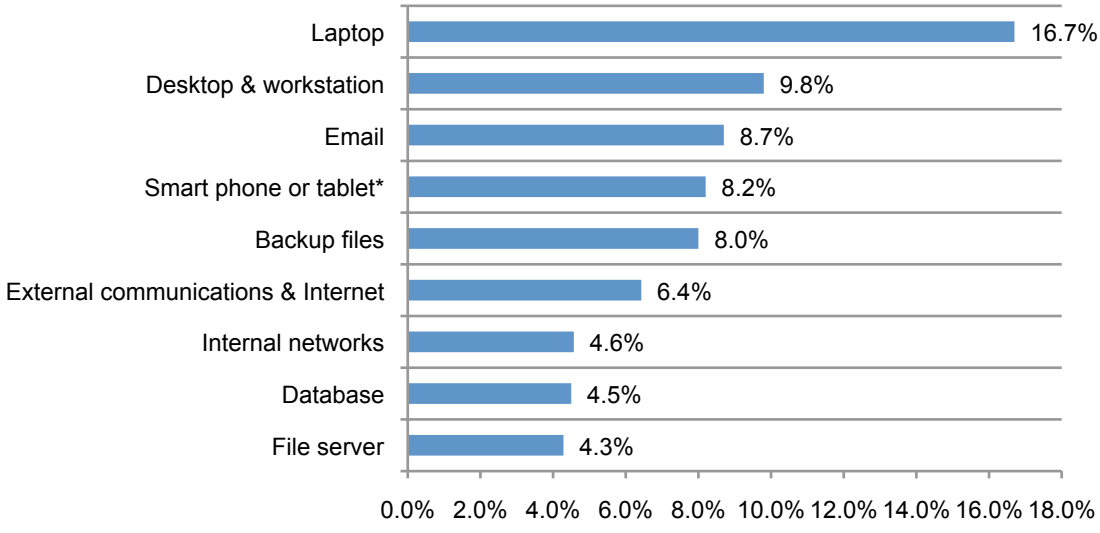
Since we began tracking the enterprise-wide use of encryption in 2005, there has been a steady increase in the encryption solutions used by organizations (i.e., a compound increase of 9 percent computed over a seven-year period). Figure 9 summarizes extensive (a.k.a. enterprise-wide) encryption usage consolidated for the nine technology categories previously discussed over seven years. A pattern of continuous growth in enterprise deployment provides strong support that encryption continues to make an important contribution to organizations' security posture.

Figure 9. Trend on the extensive use of encryption technologies



The growth rate for nine encryption technology categories are presented in Figure 10 calculated over seven years. As shown, laptop encryption achieved the highest growth rate in encryption deployment over seven years, followed by desktop and workstation and email encryption.

Figure 10. Growth rates for enterprise encryption by technology category
Percentages are calculated from average rates over a seven-year period from 2005 to 2011
*The growth rate for smart phone or tablet technologies was calculated over two years

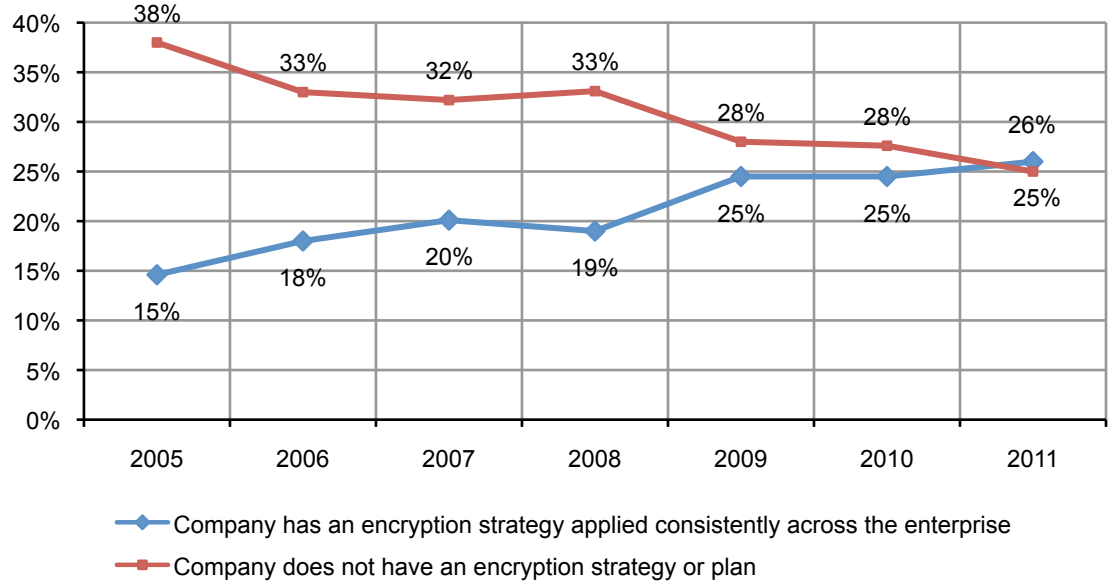


[5]The combined sample used to analyze trends is explained in Part 3. Methods.

Trends in strategy

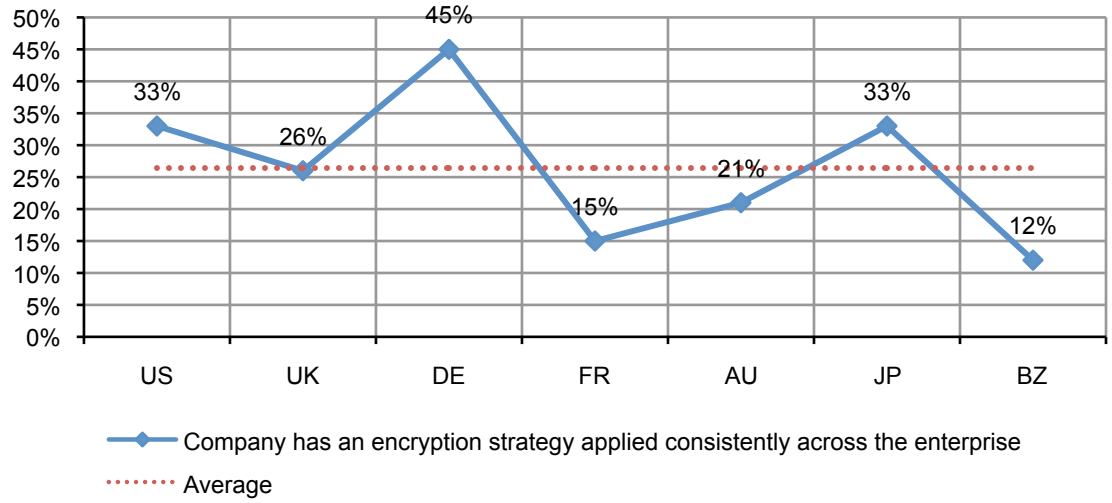
There has been a steady increase in organizations with an overall encryption plan or strategy that is applied consistently across the entire enterprise and a steady decline in not having an encryption plan or strategy. Figure 11 shows how the response has changed over the past seven years. It is clear that the percentage of respondents' companies reporting that they have an enterprise encryption strategy is steadily increasing. Correspondingly, the percentage of respondents who say their companies do not have an encryption strategy is steadily declining.

Figure 11. Trends in encryption strategy



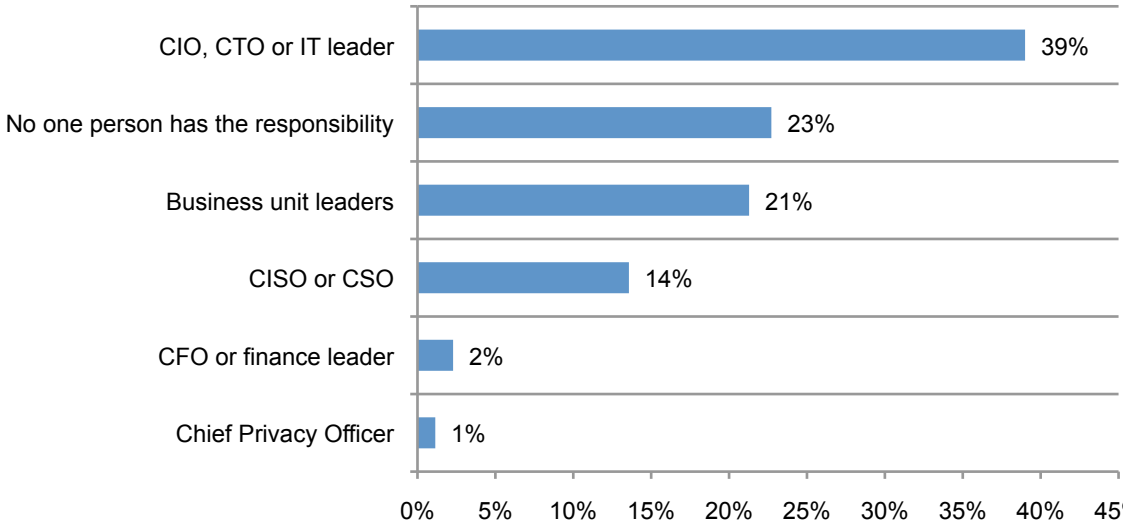
According to Figure 12, the prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany followed by the US and Japan. Respondents in France and Brazil report the lowest prevalence of an enterprise strategy.

Figure 12. Differences in enterprise encryption strategies by country samples



Who is most influential in determining the company's encryption strategy? Figure 13 shows the consolidated view from 4,140 respondents. The chart shows that the IT function is most influential in framing the organization's approaches to encryption.

Figure 13. Most influential for determining the company's encryption strategy



Business unit leaders have been steadily gaining influence over their company's encryption strategy since we began studying trends in encryption usage. The consolidated global trends in Figure 14 show that the IT leader is still the most influential person in framing the organization's approaches to encryption followed by no one person has the responsibility. As mentioned earlier, the increasing influence of business leaders in choosing encryption solutions may reflect a broader trend in the consumerization of IT.

Figure 14. Trends encryption strategy influence by IT and business unit leaders

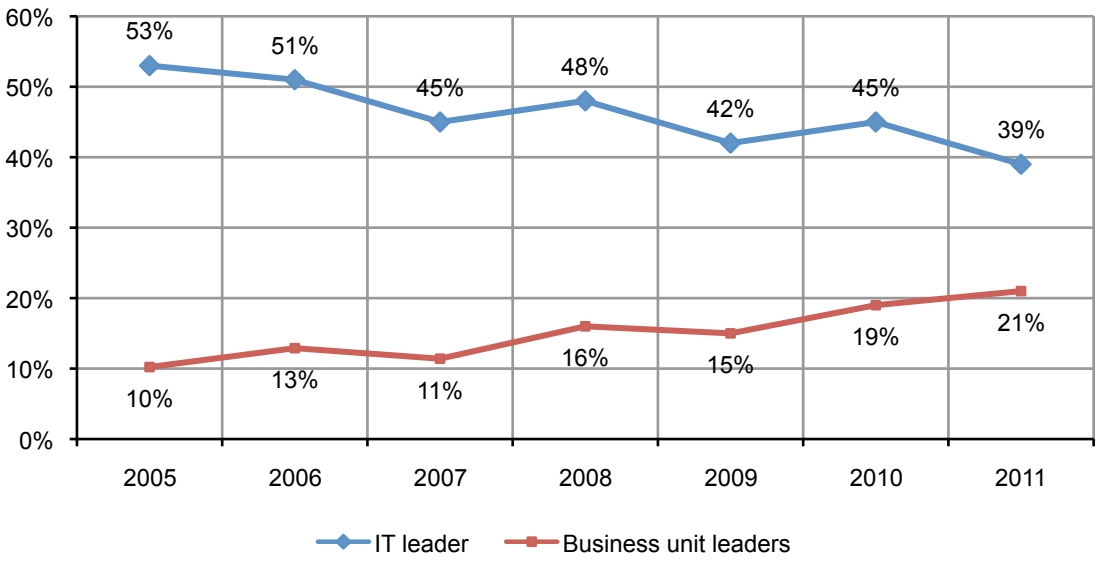


Figure 15 shows the distribution of respondents who rate business unit leaders as the most influential in determining their organization's encryption strategy. This graph clearly shows the business unit leader is most influential in the US (28 percent), Japan (26 percent) and Germany (25 percent). In contrast, the business unit leader is least influential in Brazil (14 percent) and France (15 percent).

Figure 15. Influence of business leader by country samples

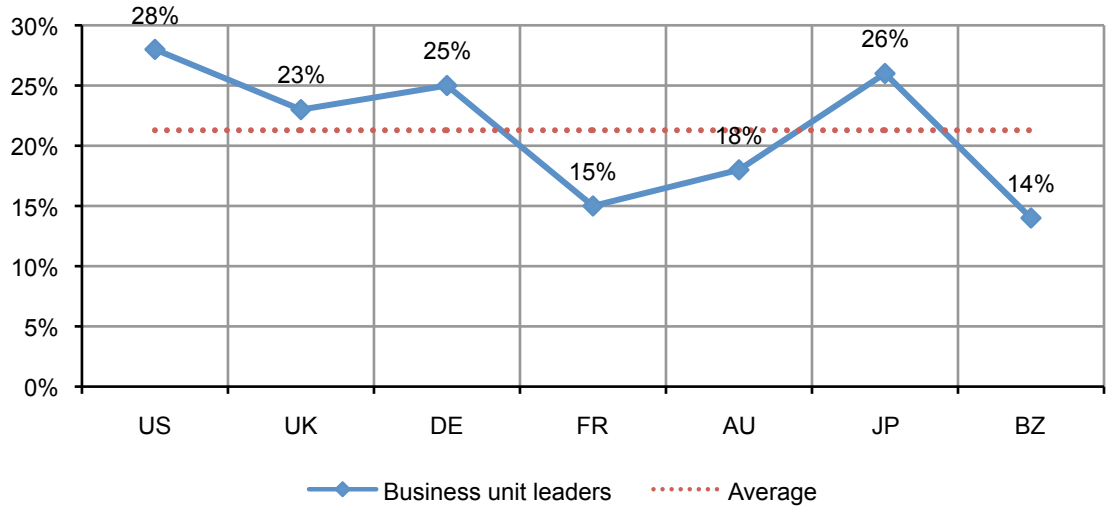
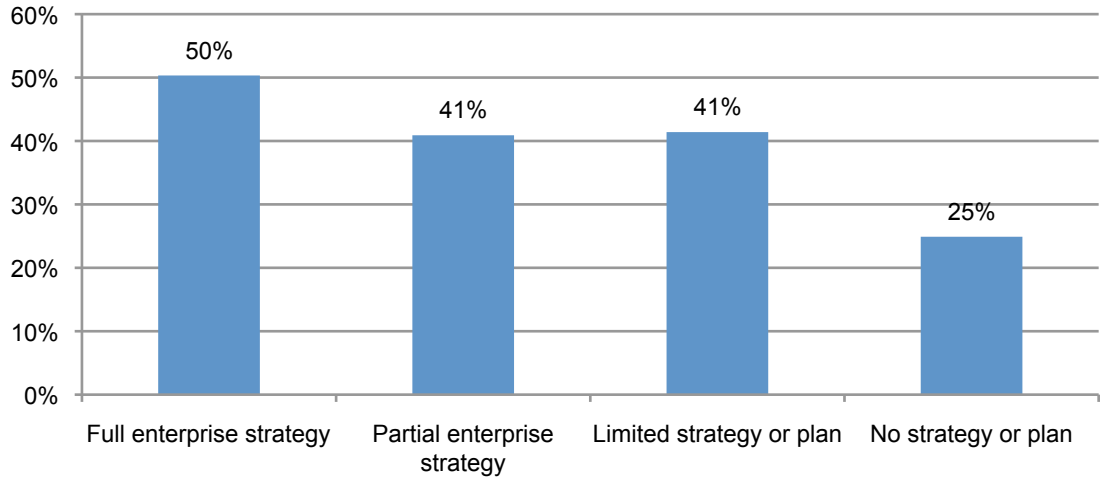


Figure 16 illustrates a cross-tabulation between two questions. One question asked respondents to select the main drivers to encryption deployment.[6] The other question asked respondents to place their organization into one of four possible encryption strategy groups. Among the respondents who say their organizations have a full enterprise strategy, 50 percent rate compliance as a main driver to encryption. In contrast, among those who say their organizations do not have a strategy or plan, only 25 percent rate compliance as a main driver.

Figure 16. The organization's compliance orientation and its encryption strategy



[6]Respondents' compliance orientation is derived from one survey selection to a question analyzed in Figure 5. Accordingly, this question asked respondents to select the main drivers to encryption deployment. On average, 39 percent of respondents selected the "compliance with privacy and data security regulations" option (which is the third highest rated response).

Prioritization: Respondents rank the most important data protection priorities

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 view. This section considers the relative prioritization of these aspects that together make a significant contribution to an overall data protection strategy.

Figure 17 provides a list of aspects that we consider an important part of an organization's data protection strategy. As shown, identity and access management, data discovery, protecting data at risk and protecting data in motion on public facing Internet applications were viewed as top priorities. Lower priorities are protecting against viruses, protecting against insecure outsourced or cloud environments, and protecting data via internal networks, all of which received relatively low average priority ranks.

Figure 17. Ranking of data protection priorities
Highest rank = 13, lowest rank = 1

Encryption features considered most important. Respondents were asked to rate eight encryption technology features considered most important as shown in Figure 18. According to the consolidated findings, automated management of encryption keys (a.k.a. key management) and the administration of the encryption program through one interface for all applications were the two top rated features.

Figure 18. Most important features of encryption technology solutions
Very important & important response combined

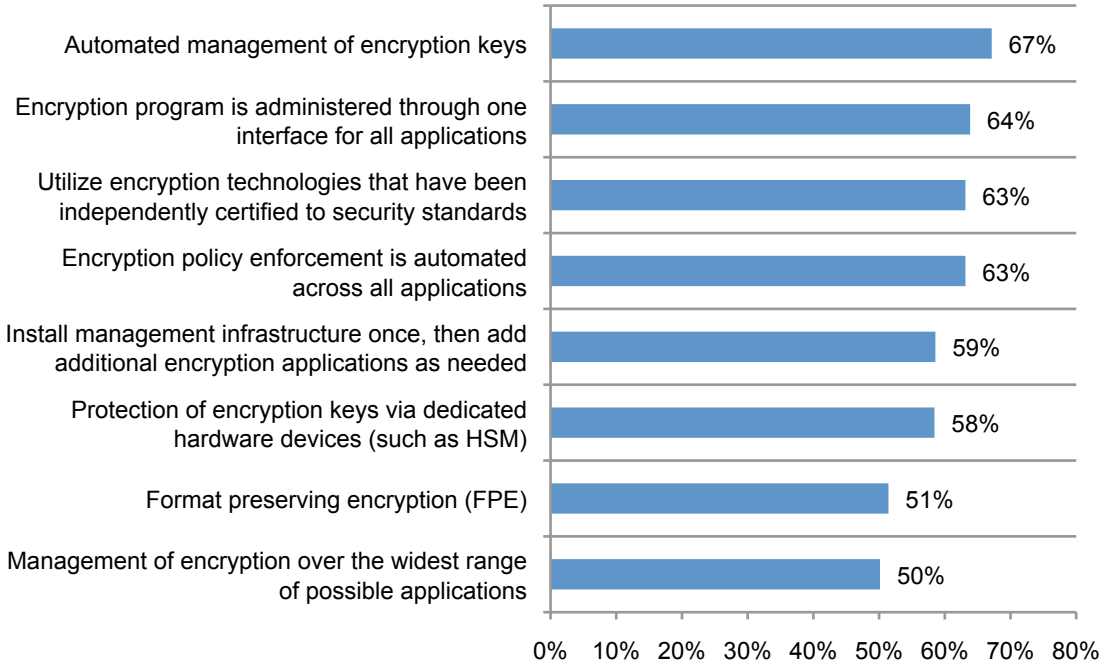
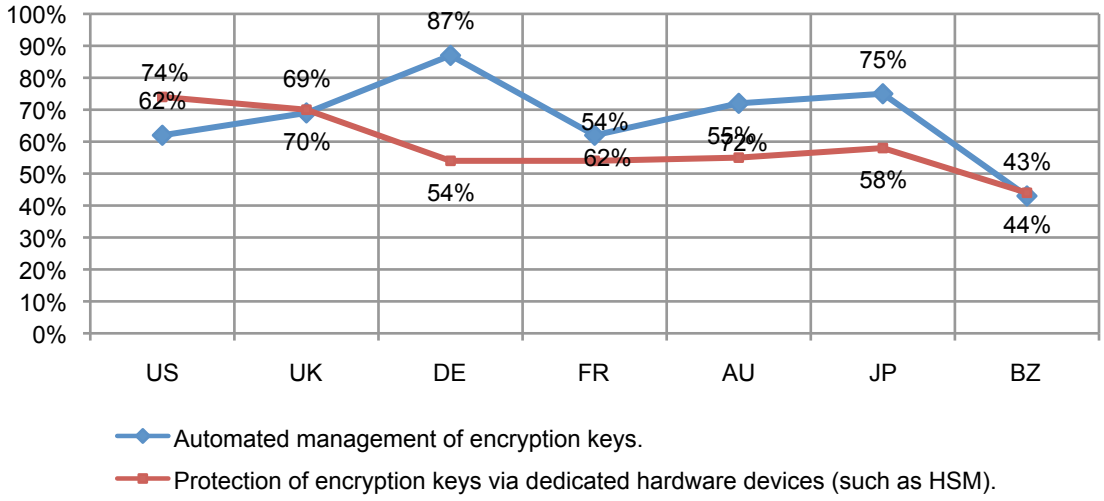


Figure 19 reports the two aspects relating to key management by country samples. With the exception of Brazil, respondents in all other countries attach a high level of importance (above 50 percent) to key management. The protection of encryption keys via dedicated hardware devices (such as HSM) is also highly rated in all countries except Brazil.

Figure 19. Two encryption technology features by country samples



Data protection and how it relates to risk management efforts. The consolidated findings reveal that throughout the globe, data protection is a critical part of organizations' risk management efforts. As shown in Figure 20, 46 percent say data protection is very important and 40 percent say it is important to their organization's risk management efforts.

Figure 20. Importance of data protection to the organization's risk management efforts

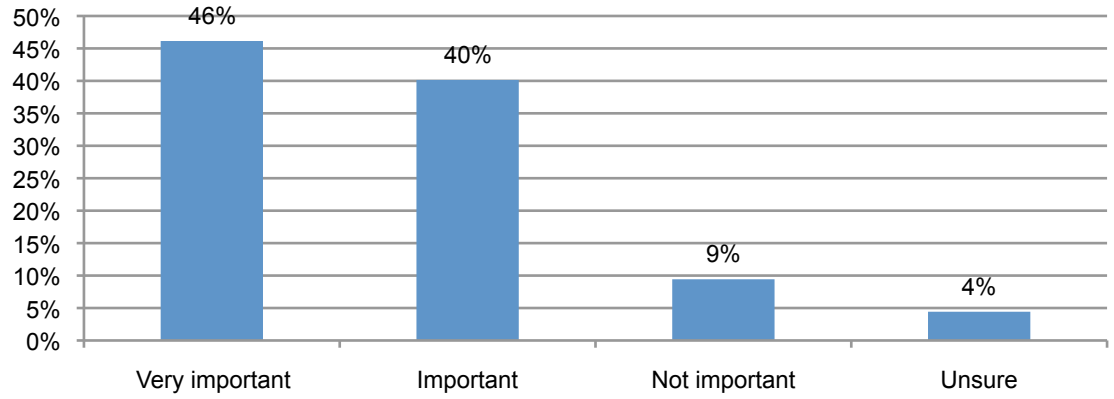
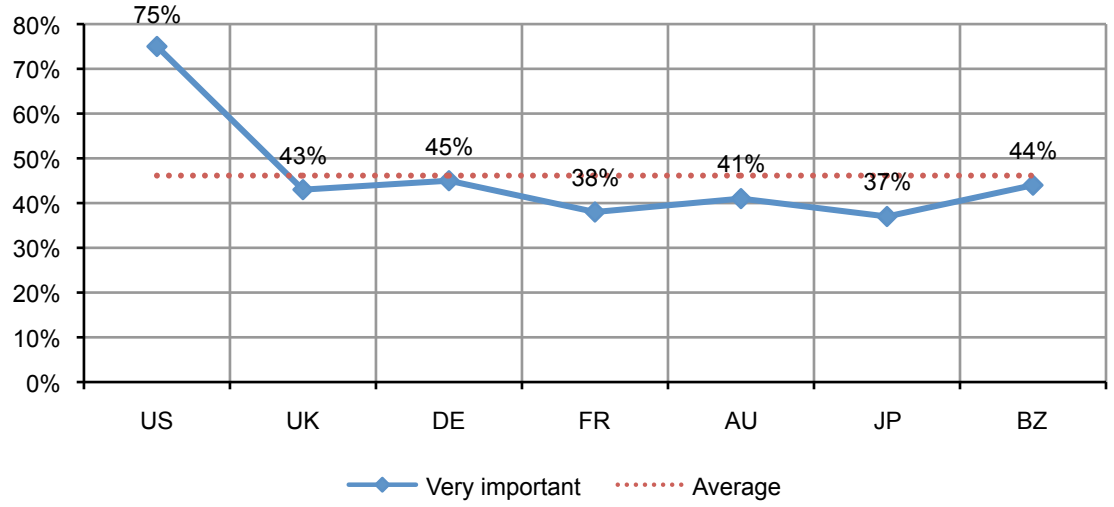


Figure 21 reports the very important response across seven countries. With an average very important rating of 75 percent, the US appears as an outlier when compared to other countries. In contrast, the other country ratings are closely aligned between 38 and 45 percent.

Figure 21. Importance of data protection to risk management efforts by country samples
Very important response only



Awareness of threats

Primary threats to sensitive data in client-controlled devices such as desktops, laptops and workstations and data center systems are consistent among organizations. As reported in Figure 22, employee mistakes or negligence rate highest for client-controlled devices. In the data center systems environment, the two highest threats to sensitive or confidential data are broken business processes and third party mishaps or mistakes.

Figure 22. The most salient threats to sensitive data in client-controlled devices and data center systems

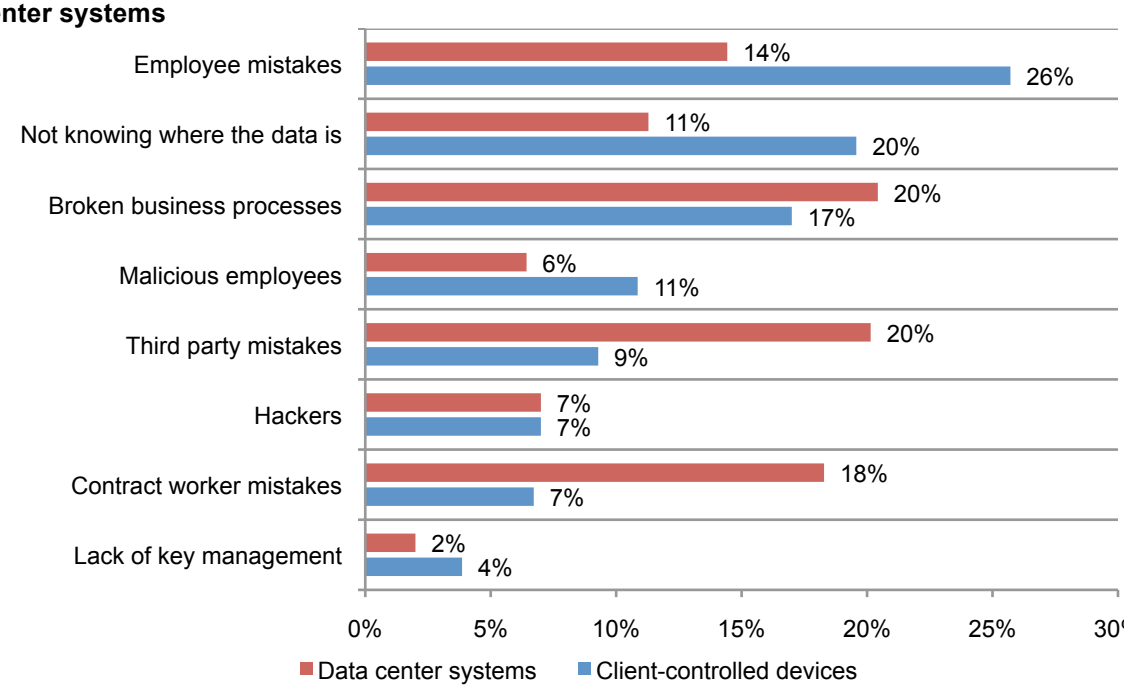


Figure 23 reports the top three threats for client-controlled devices by country, which are employee mistakes, not knowing where the data is and broken business processes. Employee mistakes are rated highest in France, Australia and the US. The inability to locate data is rated highest in Australia and France. Broken business processes are rated highest in Brazil, and rated lowest in Australia and France.

Figure 23. Top three threats for client-controlled devices by country samples

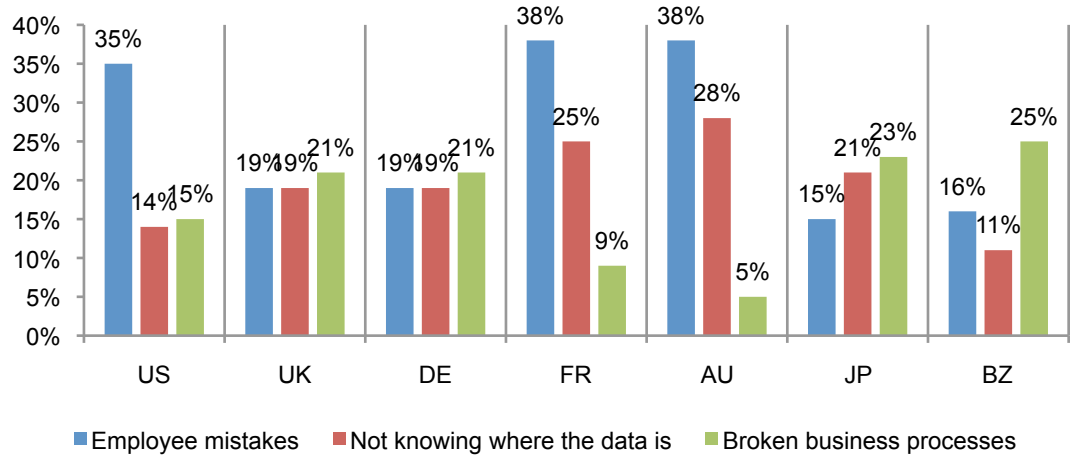
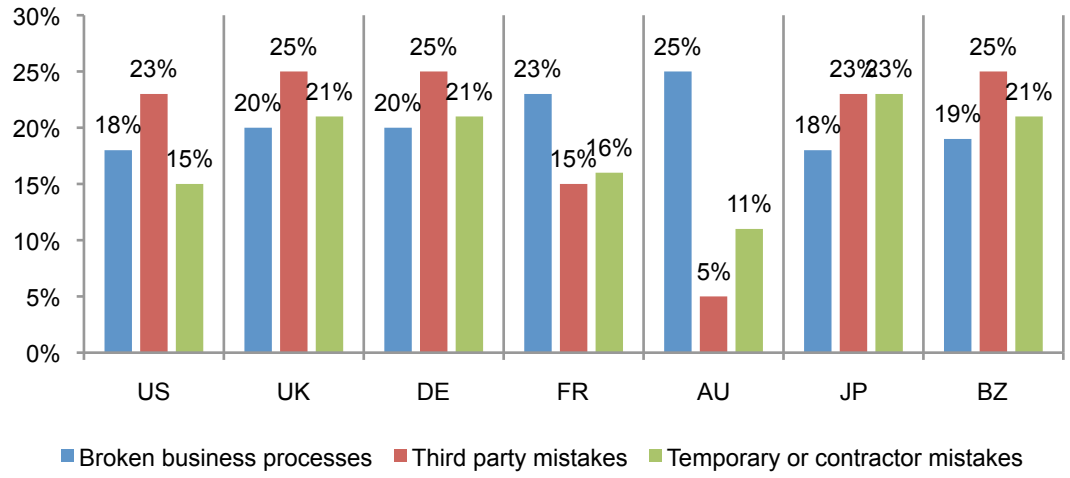


Figure 24 reports the top three threats for data center systems by country, which are broken business processes, third party mistakes and temporary or contractor mishaps. Respondents in Australia and France are most likely to rate broken business processes as a top threat to sensitive or confidential data. Third party mistakes are rated highest in Brazil, Germany and the UK. Mishaps caused by temporary or contract workers are rated highest in Japan. Respondents in Australia rate third party mistakes and contract work mishaps at a much lower level than all other countries.

Figure 24. Top three threats to data center systems by country samples



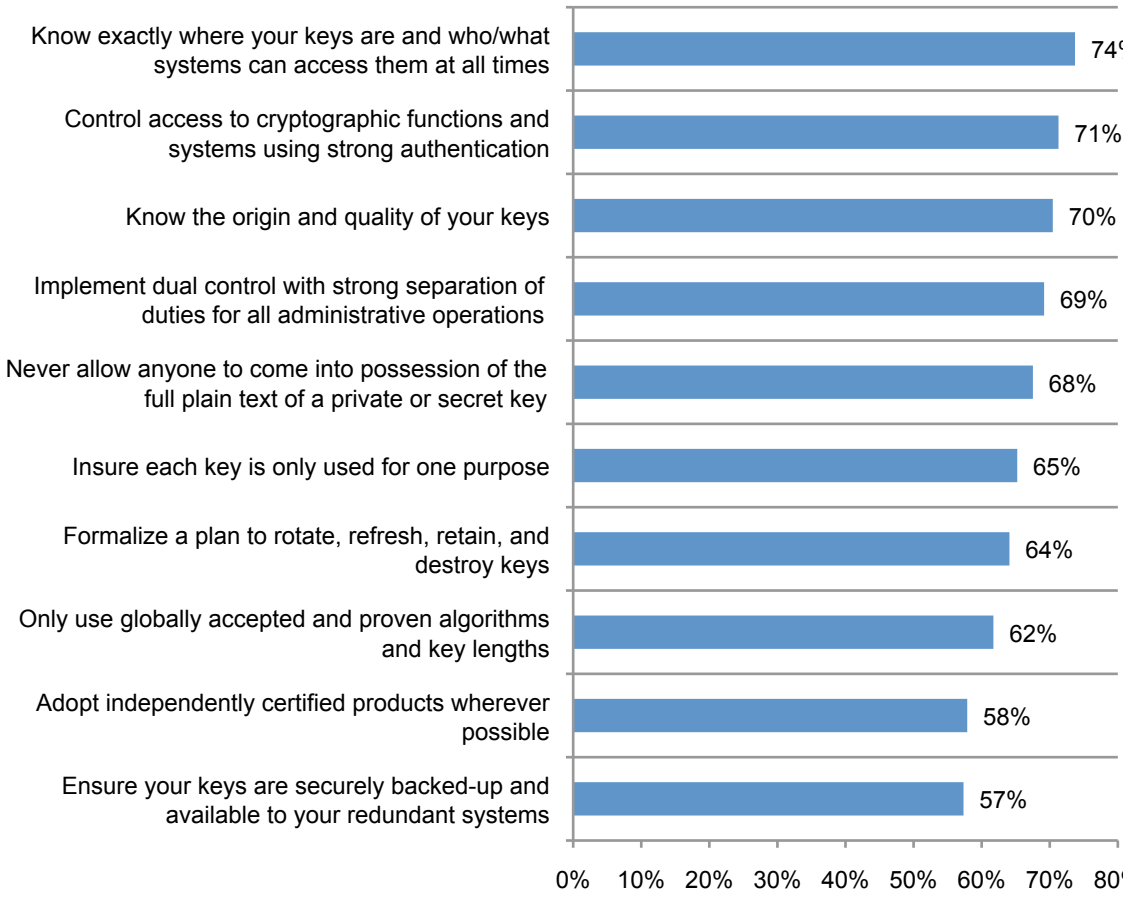
"Standards of due care" for crypto deployment

These are well established best practices regarding deployment issues around cryptography that impact the effective security of systems.

Respondents were asked to rate the importance of 10 standards of due care for crypto deployment. Figure 25 provides a summary of the very important and important response for all respondents, The fact that the average rating for all crypto standards are above the 50 percent mark is strong evidence that responses acknowledge these standards as best practices.

The top three standards as shown are: know exactly where your keys are and who/what systems can access them at all times; control access to cryptographic functions and systems using strong authentication and know the origin and quality of their keys.

Figure 25. Average importance ratings for 10 crypto development "standards of due care"
Very important & important response combined



Tokenization practices

In this year's survey, we asked questions about tokenization because it is sometimes viewed as an alternative to encryption. The average tokenization usage level is approximately half (49 percent) of the consolidated sample. Figure 26a reports 40 percent of tokenization users say their organizations deploy a commercial product. Another 31 percent say their organizations use an in-house developed tokenization system, and 29 percent say they use an external tokenization service. The most common classes of data tokenized include employee and cardholder information as shown in figure 26b.

Figure 26a
Types of tokenization deployed

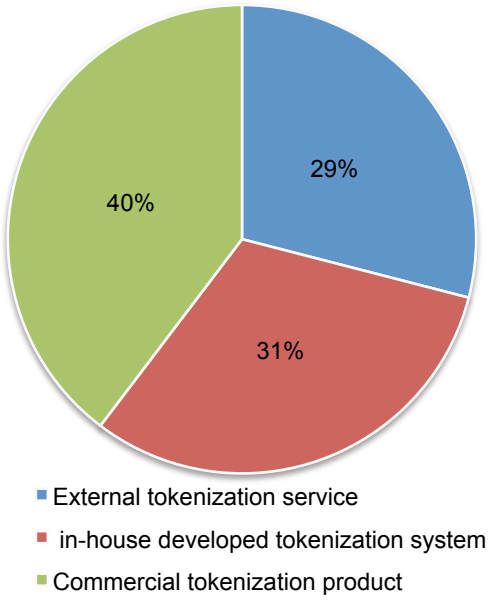
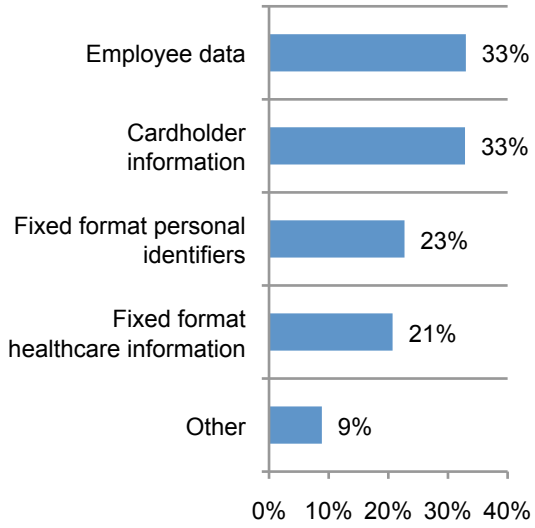
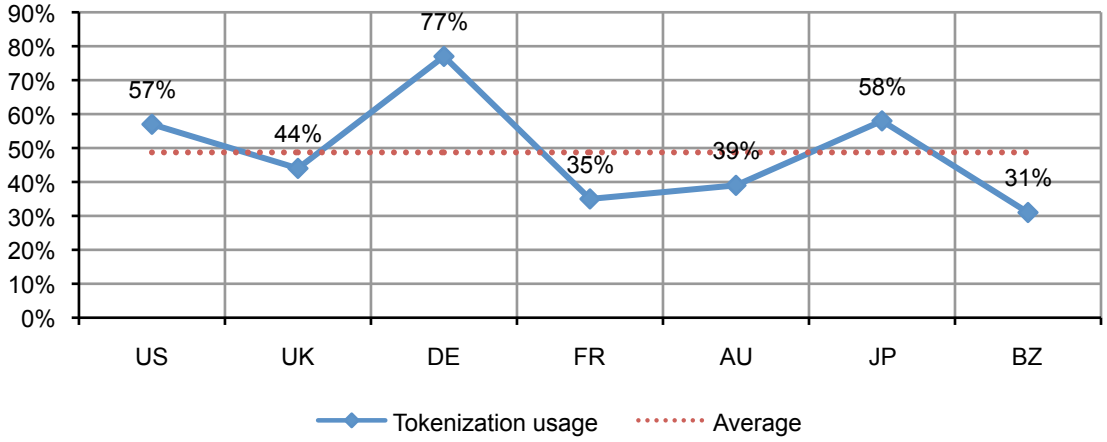


Figure 26b
Classes of data tokenized



As shown in Figure 27, tokenization is being used in all countries represented in this study. As shown, Germany reports the highest usage, followed by Japan and the US. Brazil reports the lowest tokenization usage level. It is important to note, however, that we did not determine if tokenization use was extensive (across the enterprise) or only partially deployed (limited).

Figure 27. Tokenization usage by country samples



The following two figures reveal attitudes about tokenization for those respondents who say their organizations use tokenization. Figure 28a shows 54 percent see tokenization as an alternative to encryption deployment. As noted in Figure 28b, the two main reasons for using tokenization versus encryption are: compliance obligations, ease of use and interoperability.

Figure 28a
Is tokenization an alternative to encryption?

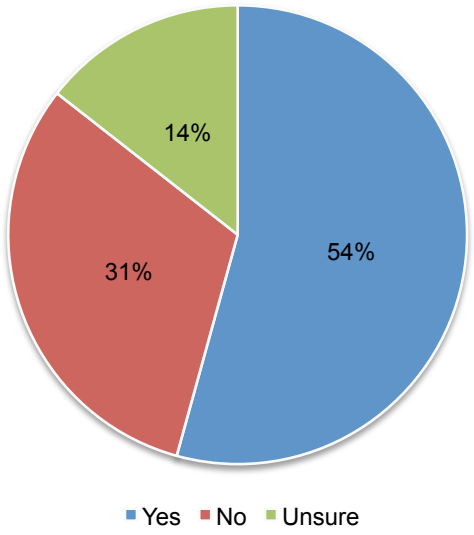


Figure 28b
Main reasons for deploying tokenization

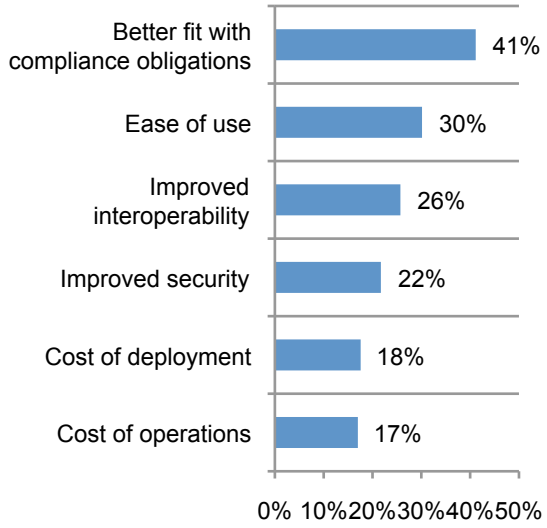
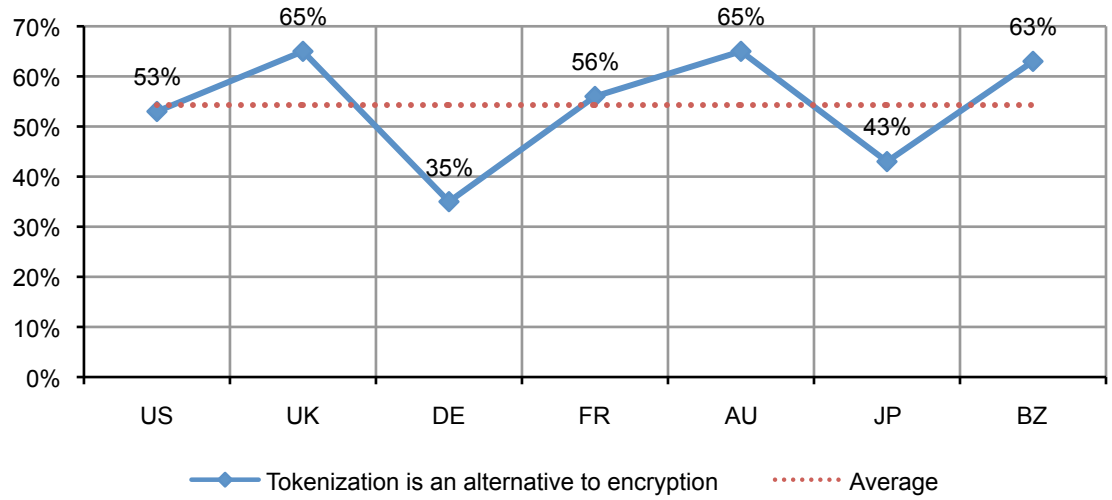


Figure 29 reports the average results by country to the question "Is tokenization an alternative to encryption deployment?" Despite the fact that Germany reports the highest percentage usage of tokenization, respondents in this country are least likely to see tokenization as an alternative to encryption. In contrast, UK, Australian and Brazilian respondents who are tokenization users are most likely to view tokenization as an alternative to encryption.

Figure 29. Is tokenization an alternative to encryption? Analysis of country samples



Budget earmarked for encryption by country and over time

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 30 shows the percent of current IT security spending relative to the total IT budget. As shown, Germany, Japan and the US report the highest percentages and Brazil and France report the lowest percentage values.

Figure 30. Percent of current IT security spending relative to the total IT budget by country samples

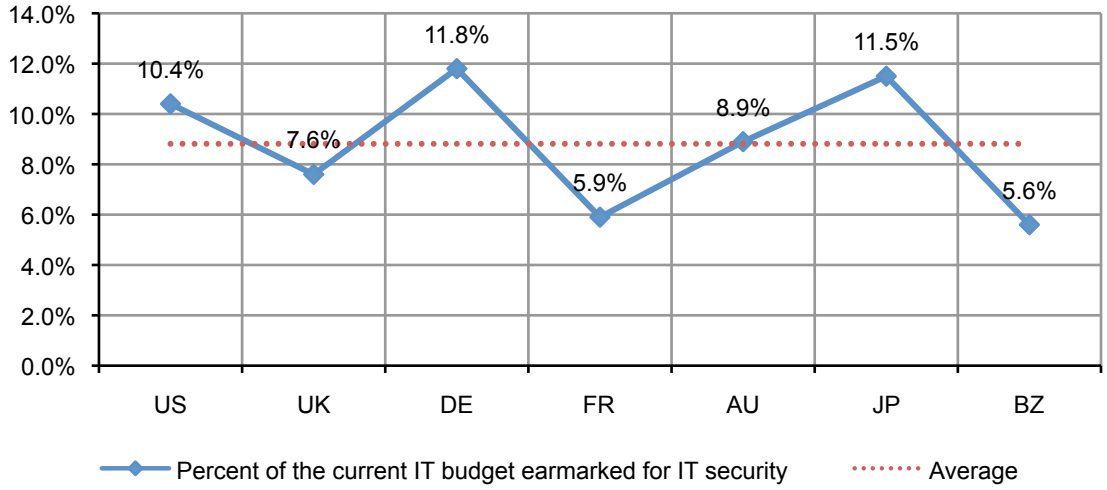


Figure 31 reports the average percent of current IT security relative to total IT over seven years. As shown, the trend appears to be upper sloping, which suggests the proportion of IT spending dedicated to security activities including encryption is increasing over time.

Figure 31. Trend in the percent of current IT security relative to the total IT budget

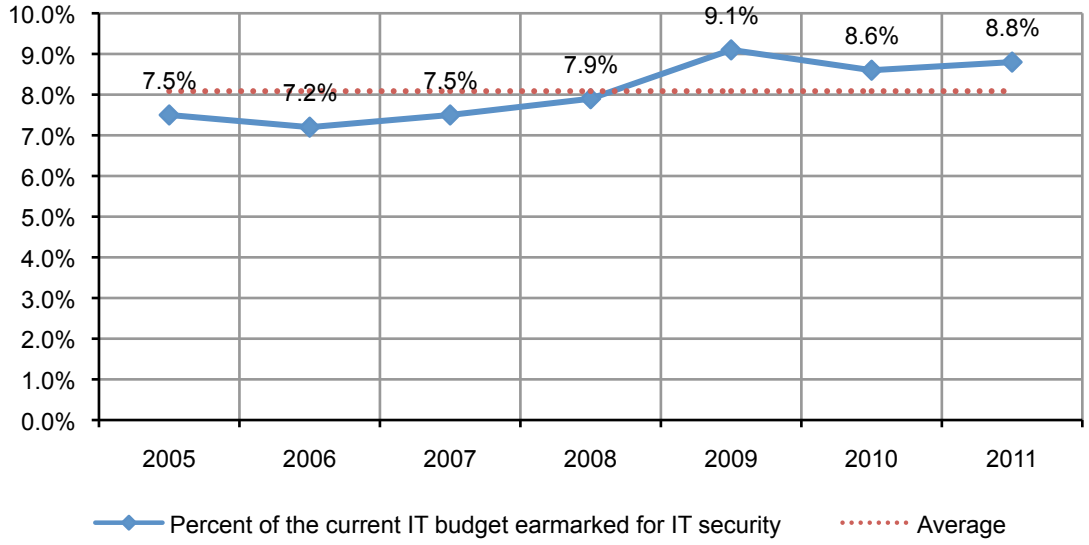


Figure 32 shows the average percent of current IT security spending dedicated to data protection spending by country sample. As shown, the percentage of data protection spending relative to total IT security is highest in the US and France, and lowest in Brazil. Perhaps more importantly is the consistency in percentage values observed across most countries.

Figure 32. Percent of current IT security spending dedicated to data protection activities by country sample

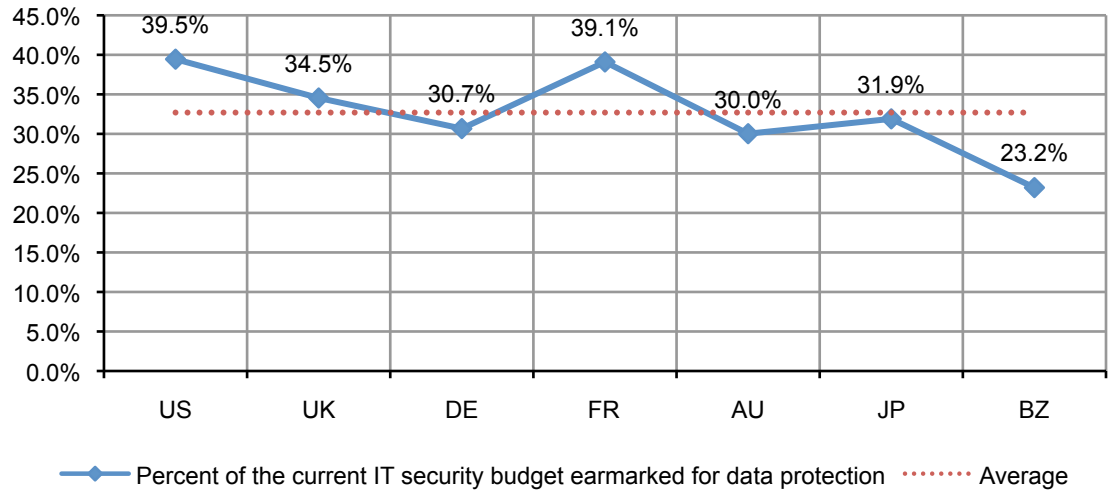


Figure 33 reports the percentage of data protection spending relative to the total IT security budget over seven years. Again, this trend appears to be upward sloping, which suggests data protection spending as a proportion of total IT security is on the rise.

Figure 33. Trend in the percent of current IT security spending dedicated to data protection activities

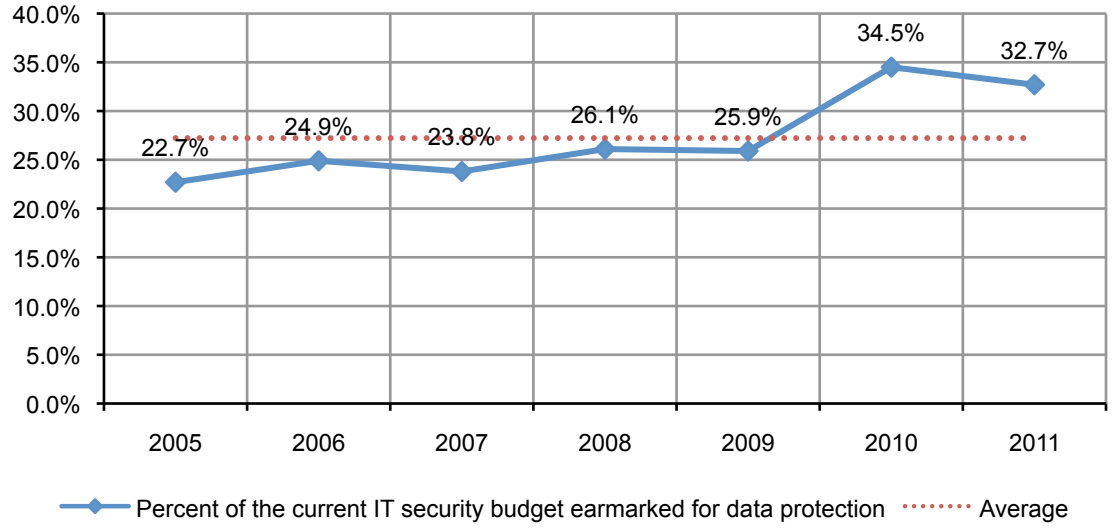


Figure 34 reports the percentage of IT security spending dedicated to encryption.[7] This figure also reports the forecasted proportion of encryption spending next year. The pattern shown below by country clearly shows next year's spending at a higher percentage than the current year's spending on encryption. Respondents in Japan and Germany show the highest average percentage of encryption spending, while those in Brazil and France show the lowest average percentage spending levels. The largest estimated increases in encryption spending over the forthcoming year occurs in Brazil, Japan and Germany.

Figure 34. Percent of the IT security budget dedicated to encryption by country samples

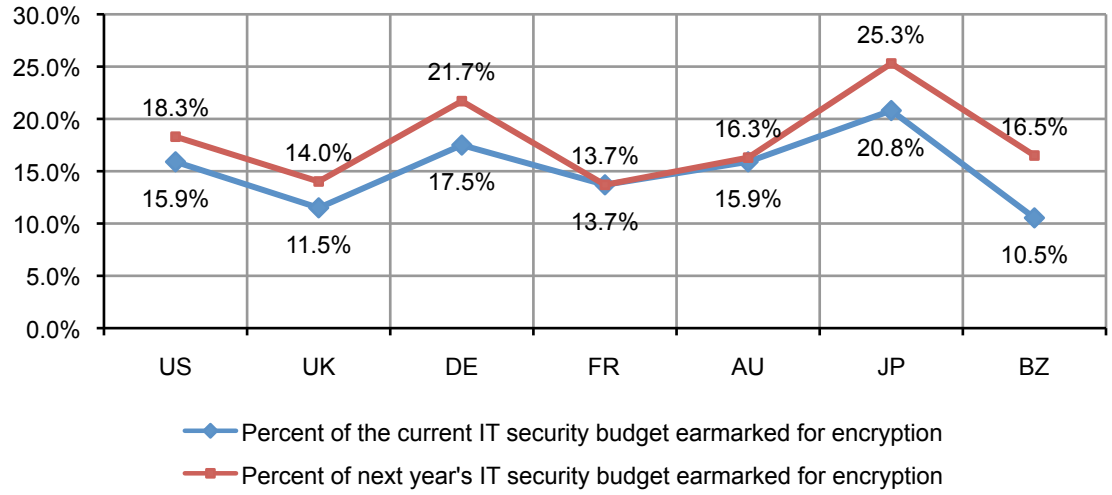
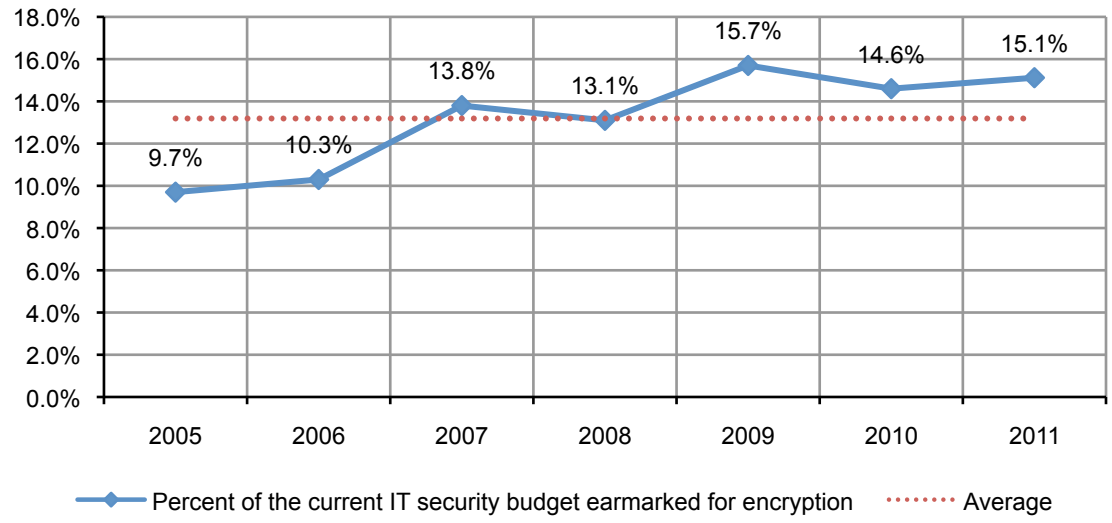


Figure 35 reports the seven-year trend in the percentage of encryption spending relative to the total IT security budget. Again, the trend appears to be increasing from a low of 9.7 percent in 2005 to 15.1 percent in the present year's encryption trends study.

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



[7]The figures in this graph suggests 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.

Trends in the spending and use of key management

Figure 36 reports the proportion of spending on encryption key management relative to the total spending on encryption solutions. The chart reports this percentage value for the current year and a forecast percentage value for next year. Perhaps the most interesting finding is the general consistency in the percentage spending on key management across all seven countries.

Figure 36. Percent of encryption spending dedicated to key management activities

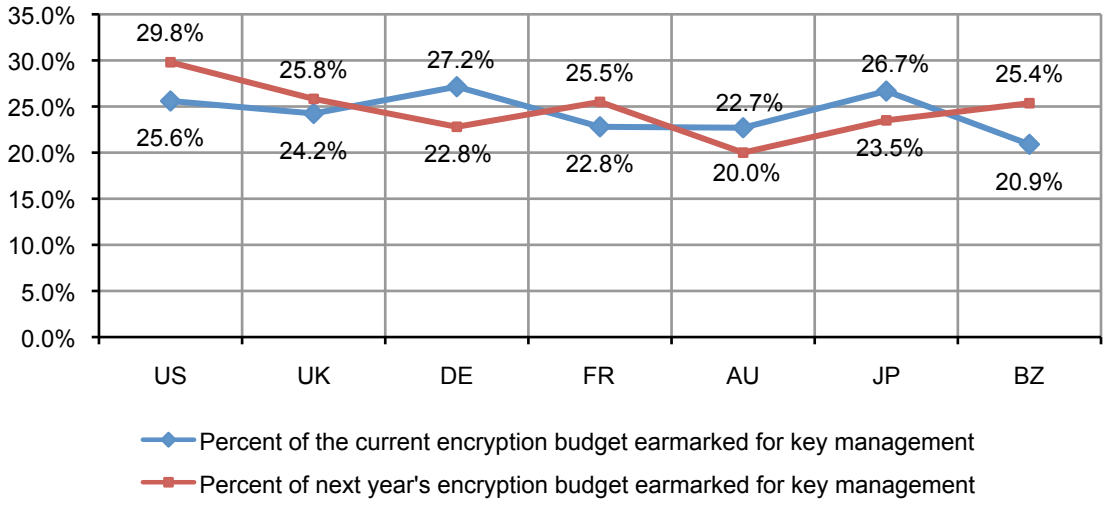


Figure 37 reports the types of key management solutions already deployed or being considered by respondents. The top two choices are multiple key management solutions either from a single vendor (21 percent) or from potentially different vendors for specific applications (20 percent). Only eight percent believe their organization's existing key management solutions are sufficient.

Figure 37. Key management solutions deployed or being considered by respondents

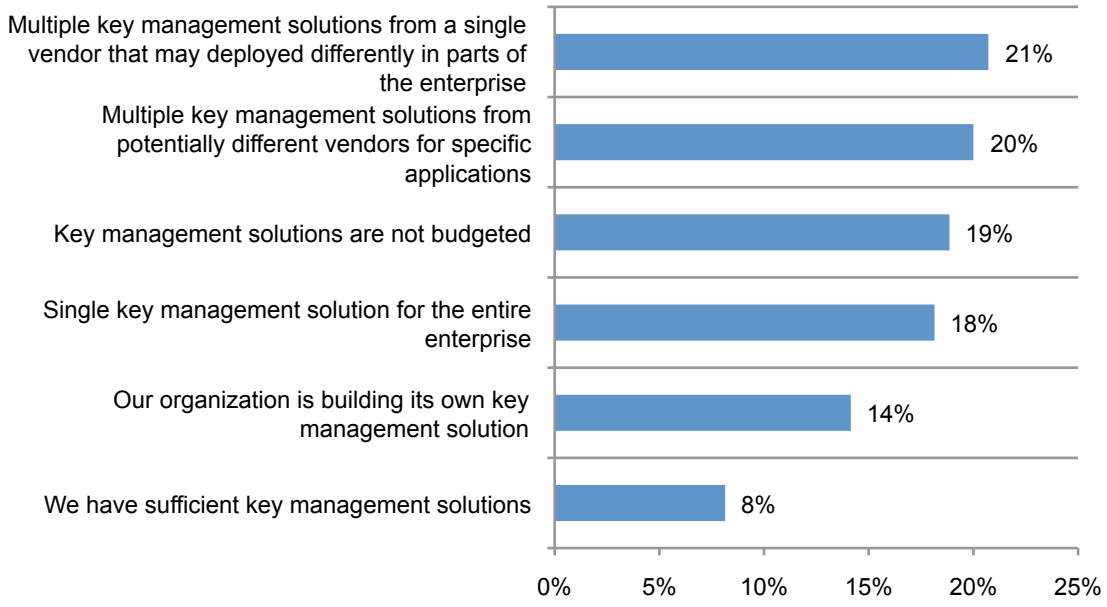


Figure 38 provides a deeper analysis to the response "single key management solution for the entire enterprise" by the calculated SES. As previously mentioned, we use the SES as a measure of each organization's security posture. As can be seen, respondents within the first quartile (highest SES group) appear to be much more inclined to select one enterprise key management solution as their top choice than respondents in all other quartile groups.

Figure 38. Analysis of the response "single key management solution for the entire enterprise" by sample quartiles defined by SES

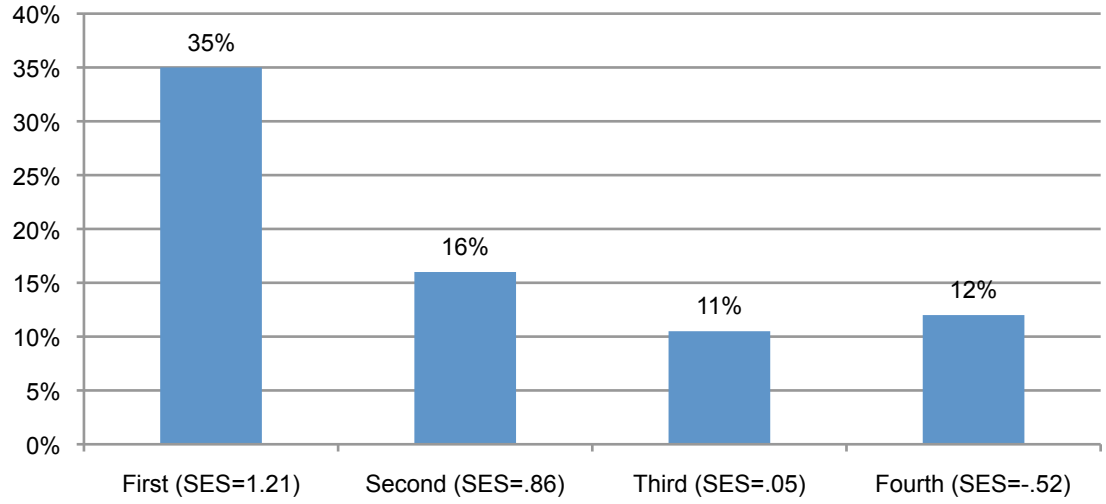
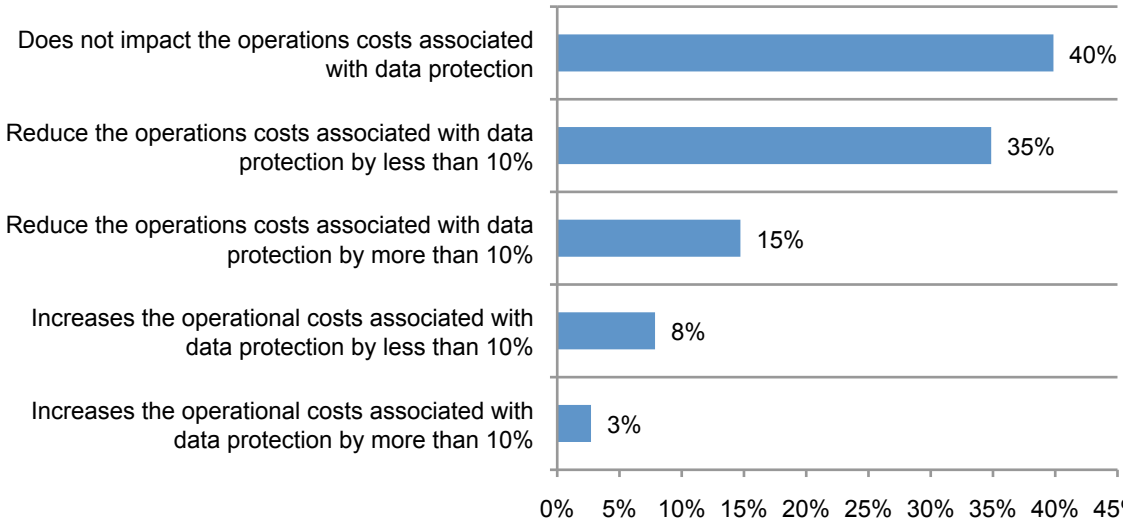


Figure 39 summarizes what respondents perceive as the economic impact of key management solutions on operating costs. Fifty (15 + 35) percent of respondents hold a favorable view – wherein 35 percent see a cost decrease by less than 10 percent and 15 percent see a cost decrease by more than 10 percent. Forty percent of respondents do not see any cost impact resulting from new key management expenditures.

Figure 39. The economic impact of key management on IT operating costs



Part 3. Methods & Limitations

Table 3 reports the sample response for seven separate country samples. The sample response for this study conducted over a 60-day period ending in December 2011. Our consolidated sampling frame of practitioners in all countries consisted of 114,379 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 4,567 returns of which 427 were rejected for reliability issues. Our final consolidated 2011 sample before screening was 4,140, thus resulting in a 3.6% response rate.

The first encryption trends study was conducted in the US in 2005.[8] 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 between 2010 and 2011.

Table 3. Sample response in seven countries

Countries	Sample frames	Invitations	Final sample	Response rate
United States	26,501	24,562	912	3.4%
United Kingdom	16,788	15,756	651	3.9%
Germany	14,890	14,001	526	3.5%
France	11,900	10,992	511	4.3%
Australia	12,067	11,050	471	3.9%
Japan	16,235	15,001	544	3.4%
Brazil	15,998	14,564	525	3.3%
Totals	114,379	105,926	4,140	3.6%

As noted in Table 4, the respondents' average (mean) experience in IT, IT security or related fields is 10.2 years. Approximately 27 percent of respondents are female and 73 percent male.[9]

Table 4. Other characteristics of respondents

Experience levels	Mean	Gender:	Consolidated%
Overall experience	12.23	Female	27%
IT or security experience	10.20	Male	73%
Years in present position	5.98	Total	100%

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

Country/year	Legend	2011	2010	2009	2008	2007	2006	2005
Australia	AU	471	477	482	405	0	0	0
Brazil	BZ	525	0	0	0	0	0	0
France	FR	511	419	414	0	0	0	0
Germany	DE	526	465	490	453	449	0	0
Japan	JP	544	0	0	0	0	0	0
United Kingdom	UK	651	622	615	638	541	489	0
United States	US	912	964	997	975	768	918	791
Total		4,140	2,947	2,998	2,471	1,758	1,407	791

[9]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 37 summarizes the approximate position levels of respondents in our study. As can be seen, the majority (59 percent) of respondents are at or above the supervisory level.

Figure 37. Distribution of respondents according to position level
Consolidated from seven separate country samples

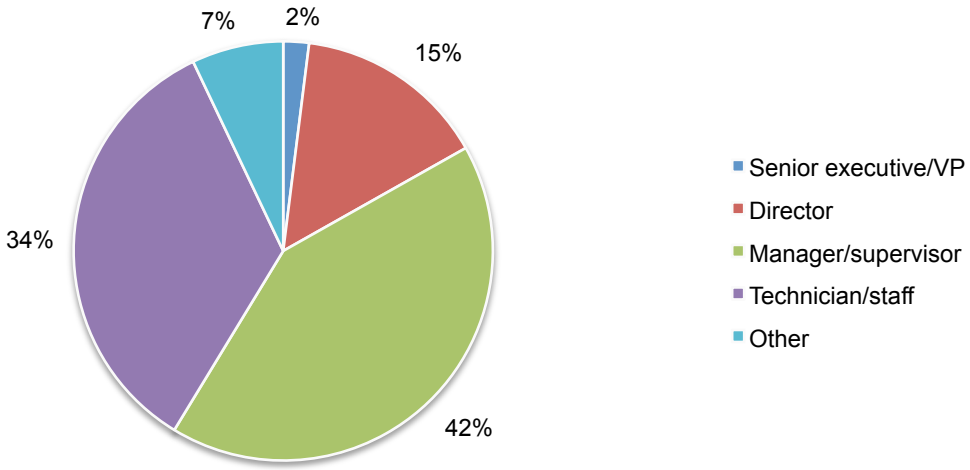
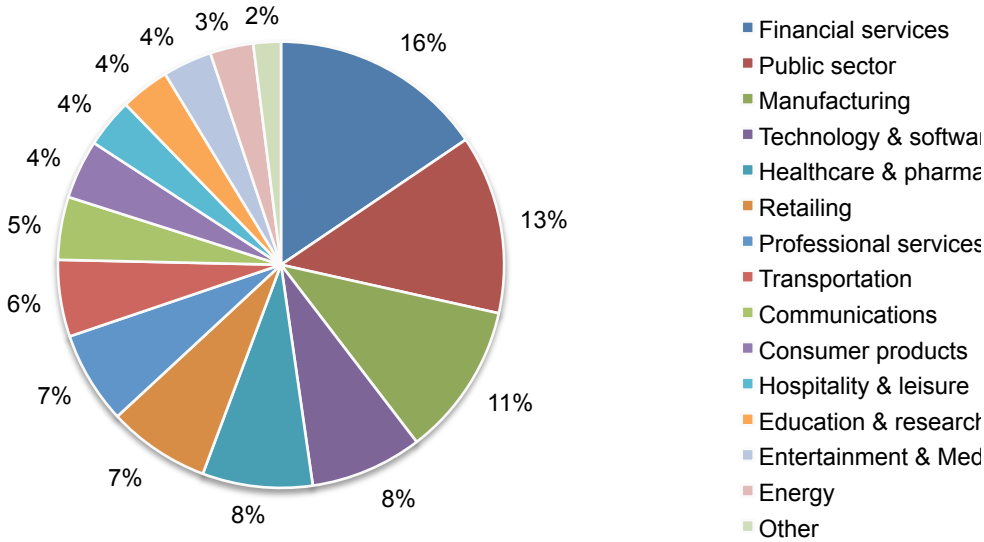


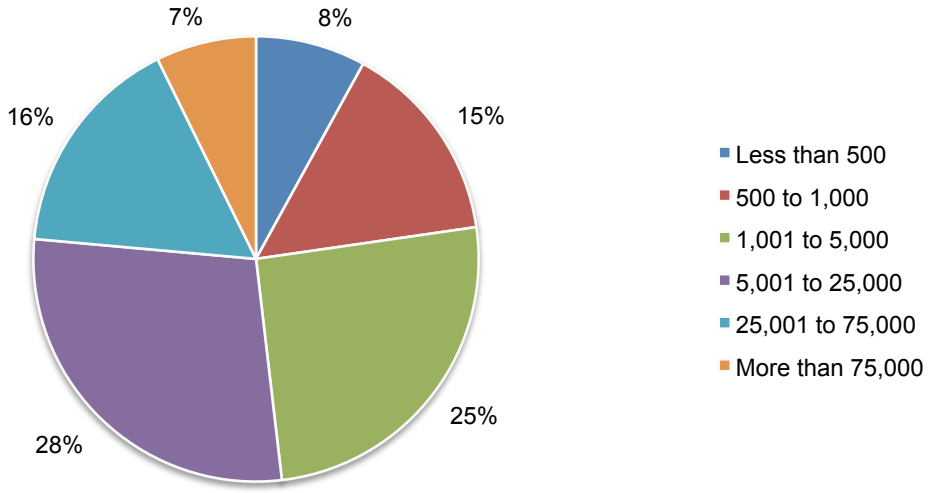
Figure 38 reports the respondents' organizations primary industry segments. As shown, 16 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 13 percent are located in public sector organizations, including central and local government.

Figure 38. Distribution of respondents according to primary industry classification
Consolidated from seven separate country samples



According to Figure 39, the majority of respondents (52 percent) are located in larger-sized organizations with a global headcount of more than 5,000 employees.

Figure 39. 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: Consolidated Findings

The following tables provide the percentage frequencies for all survey questions presented in this report. The consolidated survey results for seven separate country samples are reported. All survey responses were gathered over a 60-day period ending in December 2011.

Part 1. Maturity of your organization's IT security and data protection program	
Q1. Please check all the activities that your organization currently deploys for enterprise data protection. Place the check under the heading: (1) activity just launched, (2) activity is in process, or (3) the activity is fully executed or in maintenance mode.	Fully executed
Implementation of network-based data loss detection and prevention technologies	41%
Implementation of endpoint-based data loss prevention technologies	29%
Implementation of end-user data encryption technologies	34%
Implementation of data center encryption technologies (excluding SSL and VPN)	36%
Implementation of tokenization technologies	27%
Implementation of encryption in data archive systems	41%
Implementation of strong authentication devices	32%
Implementation of endpoint device control technologies	43%
Implementation of enterprise key management activities	24%
Implementation of data classification	40%

Part 2. Experience and knowledge about encryption	
Q2a. Does your organization encrypt sensitive and confidential data when sending them by email?	Consolidated
Yes, most of the time	19%
Yes, some of the time	45%
No	37%
Total	100%

Q2b. Does your organization encrypt sensitive and confidential data stored on shared storage such as a file server?	Consolidated
Yes, most of the time	19%
Yes, some of the time	44%
No	37%
Total	100%

Q2c. Does your organization encrypt sensitive and confidential data stored on a laptop computer?	Consolidated
Yes, most of the time	25%
Yes, some of the time	43%
No	32%
Total	100%

Q2d. Does your organization encrypt sensitive and confidential data stored on a desktop or workstation?	Consolidated
Yes, most of the time	23%
Yes, some of the time	45%
No	32%
Total	100%

Q2e. Does your organization encrypt sensitive and confidential data stored on mobile data-bearing device such as a smart phone or PDA?	Consolidated
Yes, most of the time	19%
Yes, some of the time	39%
No	42%
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?	Consolidated
Yes, most of the time	34%
Yes, some of the time	37%
No	30%
Total	100%

Q2g. Does your organization encrypt sensitive and confidential data when sending it by external communications such as SSL Internet?	Consolidated
Yes, most of the time	25%
Yes, some of the time	45%
No	30%
Total	100%

Q2h. Does your organization encrypt sensitive and confidential data when sending it by internal networks?	Consolidated
Yes, most of the time	25%
Yes, some of the time	43%
No	33%
Total	100%

Q3. Please check how encryption is used within your organization. Check all that apply.	Consolidated
Virtual Private Network (VPN)	44%
Database encryption	47%
Desktop email encryption	34%
Gateway email encryption	30%
FTP batch transfer	30%
Full disk encryption	38%
Virtual volume encryption	11%
USB flash drive encryption	21%
XML transaction encryption	24%
File server encryption	48%
NAS/SAN encryption	19%
VOIP encryption	11%
Tape encryption	25%
Mainframe encryption	7%
Native disk drive encryption (built into drive)	17%

Q4. Please check 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	26%
We have an overall encryption plan or strategy that is adjusted to fit different applications and data types	23%
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	25%
Total	100%

Q5. In your organization, who has responsibility for directing your organization's approach to encryption? Please check the one best choice.	Consolidated
No one person has the responsibility	23%
CIO, CTO or IT leader	39%
CFO or finance leader	2%
Business unit leaders	21%
CISO or CSO	14%
Privacy officer	0%
Other	1%
Total	100%

Q6. How does data protection relate to your organization's risk management efforts? Please select only one statement that best fits your organization.	Consolidated
Data protection is a very important part of risk management	46%
Data protection is an important part of risk management	40%
Data protection is not an important part of risk management	9%
Unsure	4%
Total	100%

Q7a. What are the reasons why your organization encrypts sensitive or confidential information? Please check the top two reasons.	Consolidated
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	38%
To protect our company's brand or reputation damage resulting from a data breach	46%
To comply with privacy or data security regulations and requirements	41%
To reduce the scope of compliance audits	22%
Total	194%

Q7b. [If you checked privacy or data security regulations or to reduce the scope of compliance audits] which regulations were most influential to your decision to use encryption?	Consolidated
Detailed analysis for responses to this question will be provided on request	

Q8. Do you believe that the use of encryption increases your primary customer's trust and confidence in your organization's privacy or data security commitments?	Consolidated
Yes	43%
No	37%
Unsure	20%
Total	100%

Q9. With respect to your organization's enterprise data protection priorities, please rank the following thirteen (13) key activities from 13=highest priority to 1=lowest priority. If possible, please avoid tied ranks.	Consolidated
Protecting against external penetration (hackers)	7.10
Protecting against viruses, malware and spyware infection	4.00
Classifying data at risk	10.04
Discovering data at risk	11.33
Training and certification of employees	8.60
Protecting sensitive or confidential data in motion via internal networks	5.70
Protecting sensitive or confidential data in motion in client-oriented VPN	8.40
Protecting sensitive or confidential data in motion on public facing Internet	10.26
Protecting sensitive or confidential data at rest on laptops and workstations	9.65
Protection sensitive or confidential data at rest on servers, storage infrastructure and archives	10.54
Identity and access management	11.78
Restricting access by internal staff	9.23
Protecting data in outsourced or cloud-based environments	5.54

Q10a. What is your biggest threat to sensitive or confidential data at rest on client-controlled devices such as desktops, laptops and workstations? Please check one (1) choice only.	Consolidated
Hackers	7%
Malicious employees	11%
Broken business processes	17%
Employee mistakes	26%
Temporary worker or contractor mistakes	7%
Third party or outsourcer management of data	9%
Not knowing where the data is	20%
Lack of key management for encrypted data	4%
Total	100%

Q10b. What is your biggest threat to sensitive or confidential data at rest on data center systems such as servers, storage infrastructure and in archives? Please check one (1) choice only.	Consolidated
Hackers	7%
Malicious employees	6%
Broken business processes	20%
Employee mistakes	14%
Temporary worker or contractor mistakes	18%
Third party or outsourcer management of data	20%
Not knowing where the data is	11%
Lack of key management for encrypted data	2%
Total	100%

Q11. How important to you are the following features concerning encryption solutions that may be used by your organization? Please use the scale provided below each question.	
Q11a. Encryption policy enforcement is automated across all applications.	Consolidated
Very important	20%
Important	44%
Sometimes important	21%
Not important	10%
Irrelevant	5%
Total	100%

Q11b. Automated management of encryption keys.	Consolidated
Very important	22%
Important	45%
Sometimes important	20%
Not important	9%
Irrelevant	3%
Total	100%

Q11c. Management of encryption over the widest range of possible applications.	Consolidated
Very important	17%
Important	33%
Sometimes important	31%
Not important	14%
Irrelevant	5%
Total	100%

Q11d. Encryption program is administered through one interface for all applications.	Consolidated
Very important	21%
Important	43%
Sometimes important	19%
Not important	11%
Irrelevant	6%
Total	100%

Q11e. Install management infrastructure once, then add additional encryption applications as needed.	Consolidated
Very important	18%
Important	41%
Sometimes important	23%
Not important	12%
Irrelevant	6%
Total	100%

Q11f. Protection of encryption keys via dedicated hardware devices (such as HSM).	Consolidated
Very important	26%
Important	33%
Sometimes important	20%
Not important	15%
Irrelevant	7%
Total	100%

Q11g. Utilize encryption technologies that have been independently certified to security standards	Consolidated
Very important	33%
Important	30%
Sometimes important	23%
Not important	10%
Irrelevant	5%
Total	100%

Q11h. Format preserving encryption (FPE)	Consolidated
Very important	24%
Important	27%
Sometimes important	27%
Not important	14%
Irrelevant	7%
Total	100%

Q11i. Encryption of data on mobile data-bearing devices used by employees.	Consolidated
Very important	29%
Important	37%
Sometimes important	19%
Not important	12%
Irrelevant	3%
Total	100%

Q12. How important are the following 10 standards of due care for crypto deployment?

Q12a. Know the origin and quality of your keys.	Consolidated
Very important	34%
Important	37%
Sometimes important	12%
Not important	10%
Irrelevant	8%
Total	100%

Q12b. Know exactly where your keys are and who/what systems can access them at all times.	Consolidated
Very important	34%
Important	40%
Sometimes important	16%
Not important	7%
Irrelevant	3%
Total	100%

Q12c. Insure each key is only used for one purpose.	Consolidated
Very important	32%
Important	34%
Sometimes important	22%
Not important	10%
Irrelevant	2%
Total	100%

Q12d. Formalize a plan to rotate, refresh, retain, and destroy keys.	Consolidated
Very important	27%
Important	37%
Sometimes important	20%
Not important	11%
Irrelevant	6%
Total	100%

Q12e. Only use globally accepted and proven algorithms and key lengths.	Consolidated
Very important	34%
Important	28%
Sometimes important	20%
Not important	13%
Irrelevant	5%
Total	100%

Q12f. Adopt independently certified products wherever possible.	Consolidated
Very important	29%
Important	29%
Sometimes important	28%
Not important	10%
Irrelevant	4%
Total	100%

Q12g. Implement dual control with strong separation of duties for all administrative operations.	Consolidated
Very important	33%
Important	36%
Sometimes important	18%
Not important	8%
Irrelevant	5%
Total	100%

Q12h. Ensure your keys are security backed-up and available to your redundant systems.	Consolidated
Very important	32%
Important	26%
Sometimes important	24%
Not important	14%
Irrelevant	5%
Total	100%

Q12i. Control access to cryptographic functions and systems using strong authentication.	Consolidated
Very important	36%
Important	35%
Sometimes important	18%
Not important	9%
Irrelevant	1%
Total	100%

Q12j. Never allow anyone or any open system to come into possession of the full plain text of a private or secret key.	Consolidated
Very important	34%
Important	34%
Sometimes important	18%
Not important	8%
Irrelevant	6%
Total	100%

Part 3. Tokenization practices	
Q13a. Your organization's tokenization use	Consolidated
Does your organization use an in-house developed tokenization system?	21%
Does your organization use a commercial tokenization product?	27%
Does your organization use an external tokenization service?	20%

Q13b. What classes of data are you tokenizing?	Consolidated
Cardholder information	33%
SSN (or other fixed format personal identifiers),	23%
Fixed format healthcare information (dates, medication, test results etc.)	21%
Employee data (e.g. salary, contact details)	33%
Other (please specify)	9%
Unsure	9%
Total	127%

Q13c. What best describes how your organization tokenizes?	Consolidated
Deterministic process	34%
Non-deterministic process	47%
Unsure	19%
Total	100%

Q13d. How does your organization tokenize?	Consolidated
Shared tokenization system or service	41%
Locally at the point of capture	45%
Unsure	14%
Total	100%

Q13e. Did you consider the use of tokenization as an alternative to deploying encryption?	Consolidated
Yes	54%
No	31%
Unsure	14%
Total	100%

Q13f. if yes, please specify your reason for adopting tokenization rather than encryption?	Consolidated
Ease of use	30%
Improved security	22%
Improved interoperability	26%
Cost of deployment	18%
Better fit with compliance obligations	41%
Cost of operations	17%
Other (please specify)	4%
Total	157%

Part 4. Budget	
Q15a. Are you responsible for managing all or part of your organization's IT budget in 2010?	Consolidated
Yes	53%
No (Go to Part IV)	47%
Total	100%

Q15b. Removed for failing sanity checks	Deleted

Q15c. Approximately, what percentage of the 2011 IT budget will go to IT security activities?	Consolidated
< 2%	10%
3% to 5%	19%
6% to 10%	28%
11% to 20%	23%
21% to 30%	13%
> 30%	6%
Total	100%
Extrapolated percentage	12%

Q15d. Approximately, what percentage of the 2011 IT security budget will go to data protection activities?	Consolidated
< 5%	6%
6% to 10%	8%
11% to 20%	20%
21% to 30%	23%
31% to 40%	21%
41% to 50%	16%
> 50%	6%
Total	100%
Extrapolated percentage	27%

Q15e. Approximately, what percentage of the 2011 IT security budget will go to encryption activities?	Consolidated
< 5%	13%
6% to 10%	19%
11% to 20%	32%
21% to 30%	21%
31% to 40%	10%
41% to 50%	4%
> 50%	1%
Total	100%
Extrapolated percentage	18%

Q15f. Approximately, what percentage of the 2011 encryption budget will go to key management activities?	Consolidated
< 5%	4%
6% to 10%	11%
11% to 20%	18%
21% to 30%	28%
31% to 40%	24%
41% to 50%	14%
> 50%	2%
Total	100%
Extrapolated percentage	26%

Q16a. Please check the security initiatives that will be earmarked in the 2012 budget? Select all that apply.	Consolidated
Identity & access management	50%
Perimeter controls including intrusion detection and prevention systems	90%
Data loss prevention tools	18%
Encryption solutions	57%
Key and certificate management	39%
Tokenization	18%
Public key encryption (PKI)	37%
Anti-virus, worm and spyware tools	87%
Database security	56%
Endpoint security solutions including laptop encryption	36%
Other	4%
Total	492%

Q16b. Approximately, what percentage of the 2012 IT security budget will go to encryption activities?	Consolidated
< 5%	14%
6% to 10%	22%
11% to 20%	20%
21% to 30%	19%
31% to 40%	16%
41% to 50%	7%
> 50%	1%
Total	99%
Extrapolated percentage	20%

Q16c. Approximately, what percentage of the 2012 encryption budget will go to key management activities?	Consolidated
< 5%	3%
6% to 10%	13%
11% to 20%	23%
21% to 30%	29%
31% to 40%	23%
41% to 50%	9%
> 50%	1%
Total	100%
Extrapolated percentage	24%

Q17. If your organization has budgeted for key management products in 2011, what type of solution is being considered?	Consolidated
Single key management solution for the entire enterprise	18%
Multiple key management solutions from a single vendor that may deployed differently in parts of the enterprise	21%
Multiple key management solutions from potentially different vendors for specific applications (e.g. tape backup, email, etc)	20%
Key management solutions are not budgeted for in 2011	19%
We have sufficient key management solutions	8%
Our organization is building its own key management solution	14%
Total	100%

Q18: Does your organization's key management product expenditures:	Consolidated
Reduce the operations costs associated with data protection by more than 10%	15%
Reduce the operations costs associated with data protection by less than 10%	35%
Does not impact the operations costs associated with data protection	40%
Increases the operational costs associated with data protection by less than 10%	8%
Increases the operational costs associated with data protection by more than 10%	3%
Total	100%

Part 5. Data breach	
Q19a. Did your experience a data breach in the past 12-month period?	Consolidated
Yes, only one incident	29%
Yes, two to five incidents	24%
Yes, more than five incidents	15%
No	32%
Total	100%

Q18b. If you said yes, did you publicly disclose the data breach?	Consolidated
Yes, for all data breach incidents experienced	11%
Yes, for some data breach incidents experienced	22%
No, disclosure was not necessary	67%
Total	100%

Q19. What do you see as emerging data security threats that may affect your organization over the next 12 to 24 months?	Consolidated
Loss or theft of confidential or sensitive information	44%
Economic espionage	25%
Social engineering	33%
Malicious employee attacks	34%
Cyber security attacks	45%
Surreptitious download of malware, virus, worm or Trojan that penetrates your company's network or enterprise system	59%
Use of insecure cloud computing applications or platform	41%
Virtualization opens access to unauthorized parties	29%
Insecure mobile devices connect to your company's network or enterprise system	63%
Average	38%

Q20. How severe are the data security threats mentioned above with respect to your organization ability to succeed or fulfill its mission?	Consolidated
Loss or theft of confidential or sensitive information	56%
Economic espionage	68%
Social engineering	40%
Malicious employee attacks	57%
Cyber security attacks	61%
Surreptitious download of malware, virus, worm or Trojan that penetrates your company's network or enterprise system	30%
Use of insecure cloud computing applications or platform	48%
Virtualization opens access to unauthorized parties	42%
Insecure mobile devices connect to your company's network or enterprise system	58%
Average	50%

Part 7: Security Effectiveness Score (SES)	
Q22. The following matrix lists 24 attributes that describe an effective IT security environment. Please assess the effectiveness of your company's IT security and data protection infrastructure using the scale provided to the right of each attribute. The scale requires you to rate each item based on your level of confidence in being able to accomplish the stated attribute. The full questionnaire will be provided upon request.	Consolidated
Average SES computed from attributes	40%

Part 8. Organizational and respondent characteristics	
What organizational level best describes your current position?	Consolidated
Senior executive	1%
Vice President	1%
Director	15%
Manager/supervisor	42%
Associate/staff	35%
Other	7%
Total	100%

Check the Primary Person you or your IT security leader reports to within the organization.	Consolidated
CEO/Executive Committee	1%
Chief Financial Officer	4%
General Counsel	1%
CIO, CTO or IT leader	61%
Compliance leader	7%
CMO or marketing leader	0%
Human resources leader	3%
CISO or CSO	14%
Chief Risk Officer	10%
Other	0%
Total	100%

Experience levels	Consolidated
Total years of business experience	12.23
Total years of security experience	10.20
Total years in current position	5.98

Gender:	Consolidated
Female	27%
Male	73%
Total	100%

What industry best describes your organization's industry focus?	Consolidated
Financial services	16%
Public sector	13%
Technology & software	8%
Healthcare & pharmaceutical	8%
Manufacturing	11%
Communications	5%
Consumer products	4%
Hospitality & leisure	4%
Transportation	6%
Retailing	7%
Professional services	7%
Defense	1%
Education & research	4%
Energy	3%
Entertainment & Media	4%
Other	1%
Total	100%

Where are your employees located? (check all that apply):	Consolidated
United States	79%
Canada	65%
EMEA	79%
APJ	59%
LATAM	36%

What is the worldwide headcount of your organization?	Consolidated
Less than 500	8%
500 to 1,000	15%
1,001 to 5,000	25%
5,001 to 25,000	28%
25,001 to 75,000	16%
More than 75,000	7%
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.