2011 Encryption Trends Study United States

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: April 2012

2011 Encryption Trends Study: United States

2011 Encryption Trends Study: United States[1]

Ponemon Institute, May 2012

Part 1. Executive Summary

Ponemon Institute is pleased to present the findings of the *2011 Encryption Trends Study: United States* sponsored by Thales e-Security. In this report, we study a sample of 912 individuals in U.S. organizations. The U.S. sample is part of a larger study involving 4,140 business and IT managers in the United States, United Kingdom, Germany, France, Australia, Japan and Brazil.[2] The findings from this study appear in the *2011 Global Encryption Trends Study* published in February 2012.

The purpose of this research is to examine how the use of encryption has evolved and its impact on the security posture of U.S. 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.

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, *2011 Global Encryption Trends 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 report was performed on independent samples spanning seven years (since 2005).

Summary of key findings:

- **Encryption usage is an indicator of a strong security posture.** The security posture of U.S. organizations participating in this research has steadily increased since 2005. Similarly, the use of encryption has increased at a compound rate of 22 percent over the past seven years. This indicates organizations in the U.S. are more likely to understand and respond to data security risks through the deployment of encryption.

  Encryption spending is increasing. The percentage of U.S. encryption spending relative to the total IT security budget increased from a low of 8 percent in 2006 to 15.9 percent in 2011. The encryption of laptops, desktops and workstations and smart phones and tablets are most likely to be extensively deployed in U.S. organizations

- **Main drivers for using encryption are compliance with privacy and data security regulations.** U.S. organizations are deploying encryption because they are concerned about the financial implications of not complying with regulations and having sensitive data lost or stolen. Of the respondents who say their organizations have a full enterprise encryption strategy, 77 percent rate compliance as the main driver to encryption.

- **Business unit leaders are gaining influence over their company's use of encryption solutions.** Business unit leaders have an increasing role in determining their organization's encryption strategy and the IT leader is no longer the most influential person in determining the organization's approach to encryption. The increasing influence of business leaders in choosing encryption solutions may reflect a broader trend in the consumerization of IT.

- **Since 2005, more U.S. organizations are adopting an overall encryption plan or strategy.** Organizations in the U.S. are most mature in developing an enterprise encryption strategy. Correspondingly, the percentage of respondents who say their companies do not have an encryption strategy is steadily declining.

- **Discovering data at risk followed by protecting sensitive or confidential data in motion on public facing Internet are the top two data protection priorities.** Least important data protection priorities are protecting data in outsourced or cloud-based environments and training and certification of employees.

- **Over 75 percent of U.S. 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 broken business processes.** With respect to data center systems, the most serious threats are third party mistakes and broken business processes.

- **U.S. respondents acknowledge the importance of the 10 crypto development "standards of due care."** The average rating for all crypto standards is above the 50 percent mark, indicating that respondents acknowledge these standards are best practices. The top three are: control access to cryptographic functions and systems using strong authentication, insure each key is only used for one purpose and never allow anyone to come into possession of the full plain text of a private or secret key.

- **U.S. organizations with a strong security posture are most likely to select a single key management solution for the entire enterprise**. For the current year, 25.6 percent of the encryption budget will be allocated to key management solutions and next year the percentage increases to 29.8 percent. Fifty-five percent of respondents say that key management reduces the costs associated with data protection.

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 of 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 seven countries, 37 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 (38 percent) of organizations 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

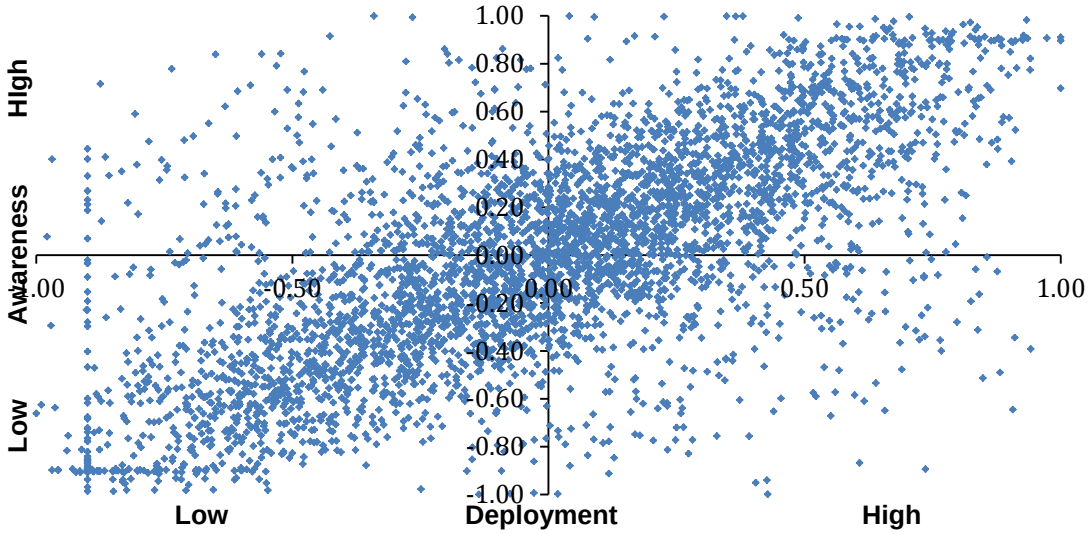


Table 2 describes the business implications for organizations with respect to their location in one of the four quadrants depicted in the scattergram above. Our basic assumption is that awareness (independent variable) drives encryption deployment decisions (dependent variable).

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 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

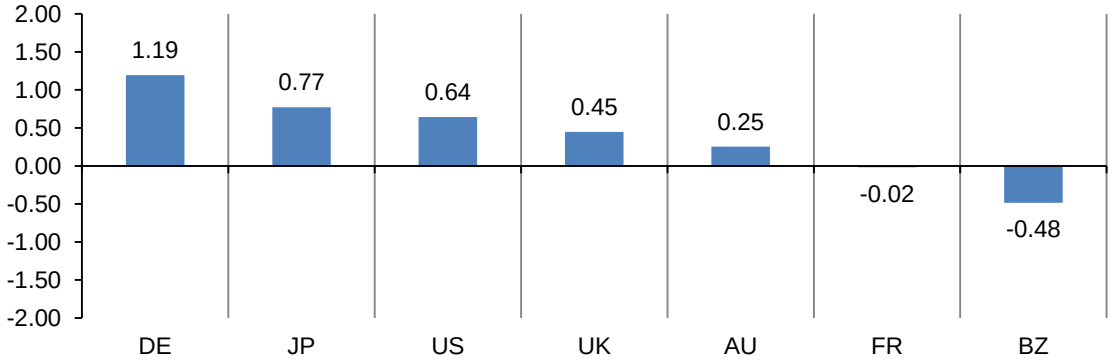
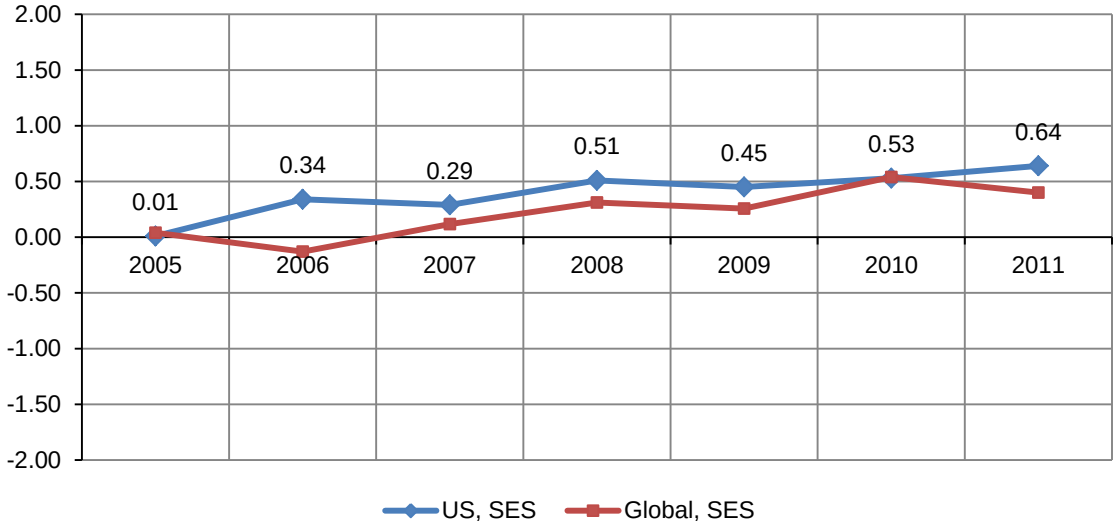


Figure 3 reports the SES results compiled from U.S. encryption trend studies over seven years. The trend line shown below is increasing slightly over time, which suggests that the security posture of participating companies has increased over this time period.

Figure 3. Trends in U.S. average Security Effectiveness Score



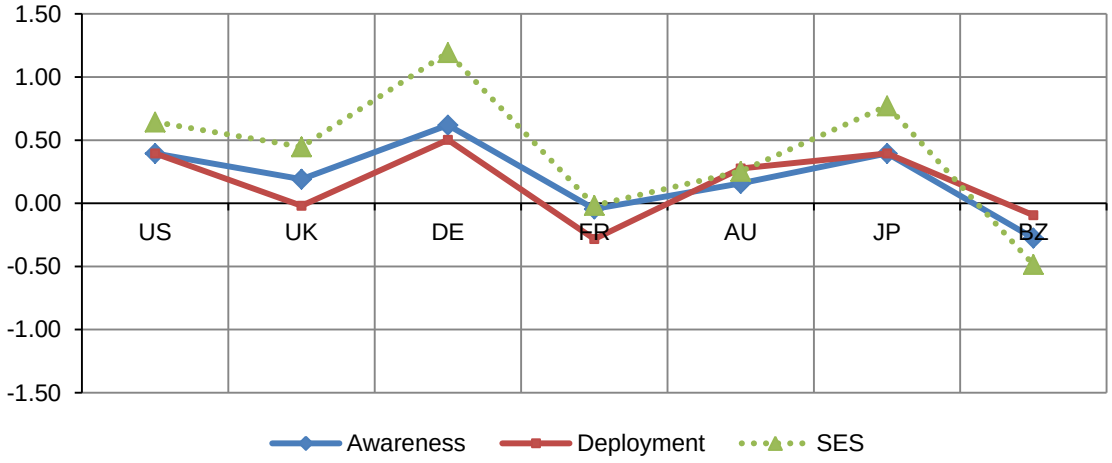
[4] The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent 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 among U.S. respondents are complying with privacy or data security regulations and requirements and lessening the impact of data breaches. The following are the main drivers as presented in Figure 5: To comply with privacy and data security regulations (65 percent), to lessen the impact of data breaches (58 percent), and to protect the company's brand or reputation (43 percent).

Figure 5. The main drivers for using encryption technology solutions in U.S. organizations

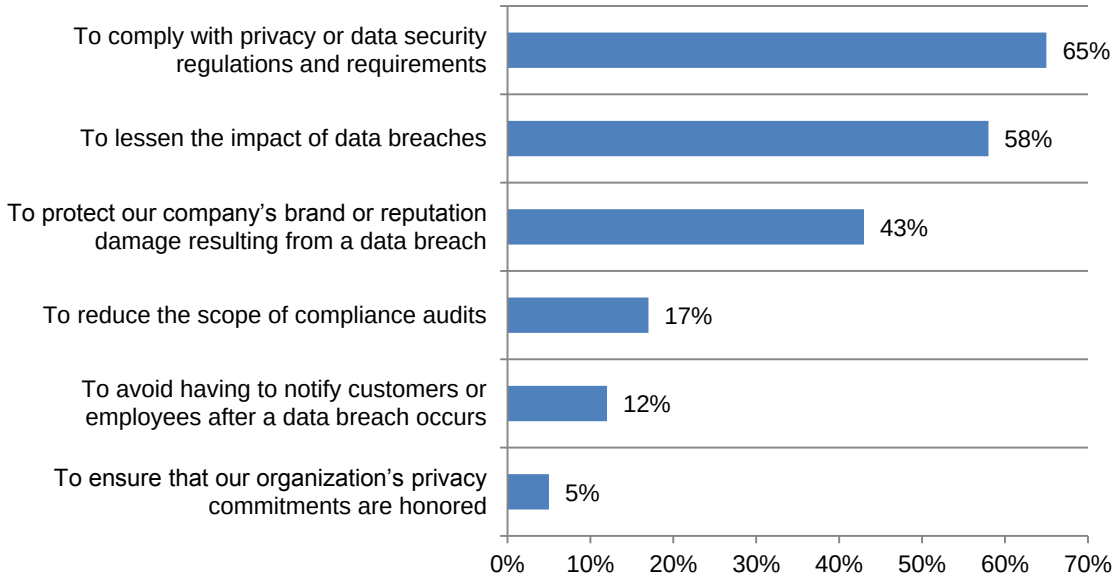
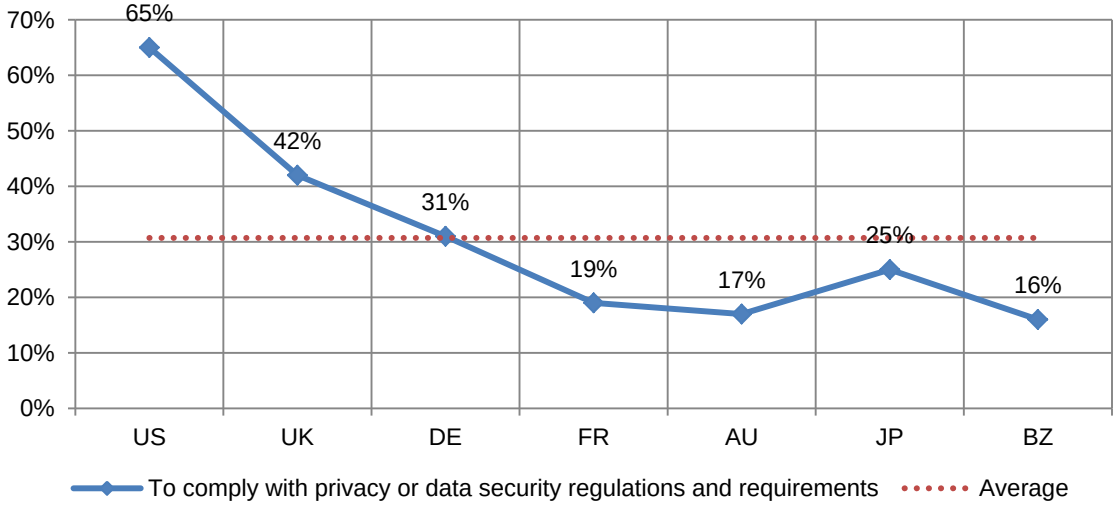


Figure 6 shows responses for seven countries to the top choice – "to comply with privacy or data security regulations and requirements." As can be seen, the issue of compliance as a main reason for deploying encryption solutions appears to be most important in the U.S. and least important in Brazil.

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



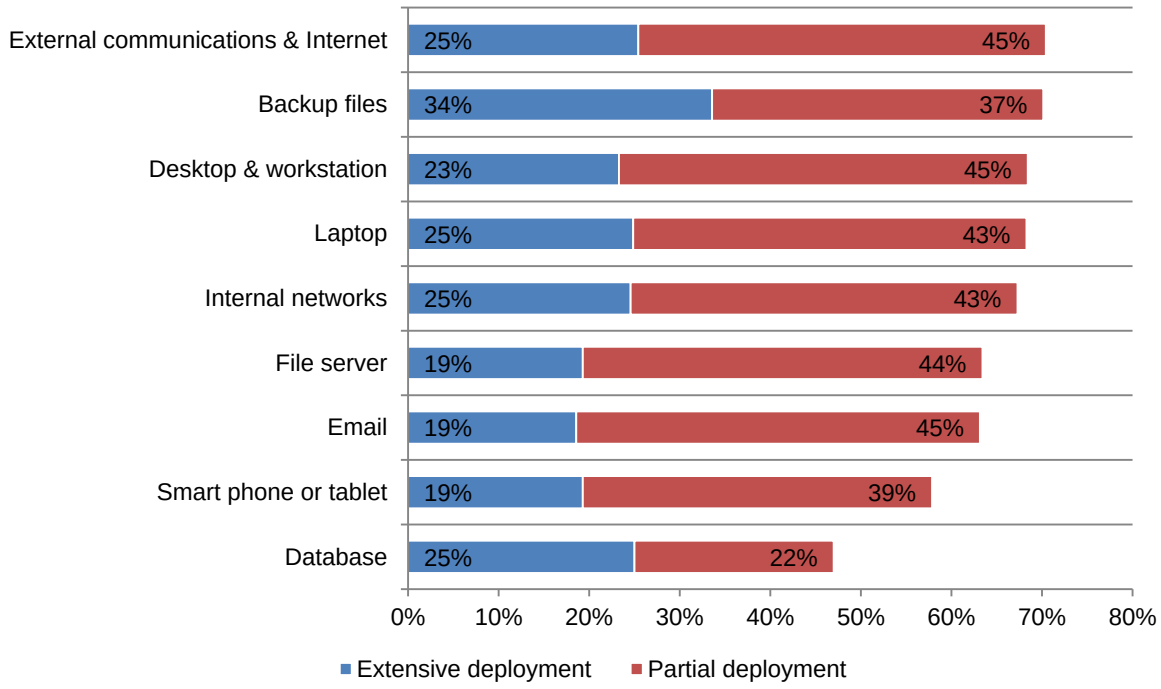
`

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.

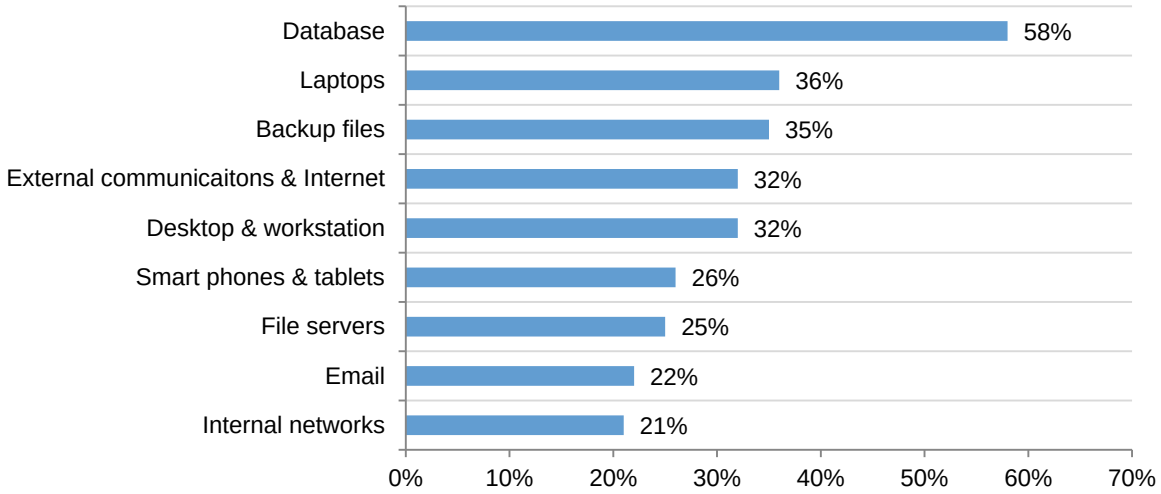
As shown in Figure 7, encryption of backup files, internal networks, external communications and laptops are most likely to be extensively deployed. In contrast, smart phone, email and file server encryption solutions are the least likely to see extensive deployment.

Figure 7. Global view on the use of encryption technologies



U.S. rate of deployment differs from global view. Figure 8 reports the enterprise deployment for nine encryption technologies in the U.S. As shown, database encryption is most widely deployed. Email and internal networks are least deployed

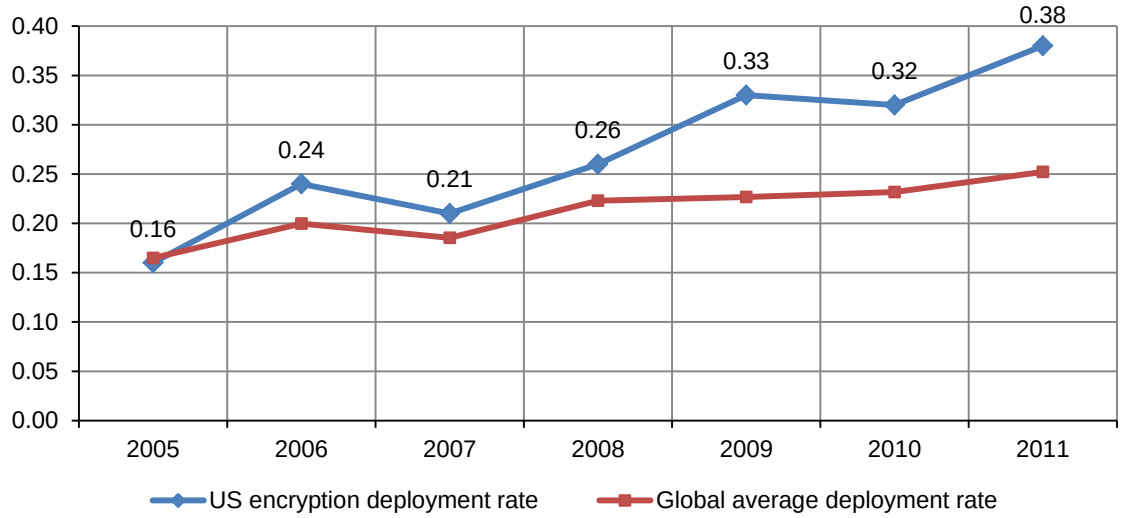
Figure 8. U.S. rates of extensive deployment for nine encryption categories



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 U.S. organizations (i.e., a compound increase of 22 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.

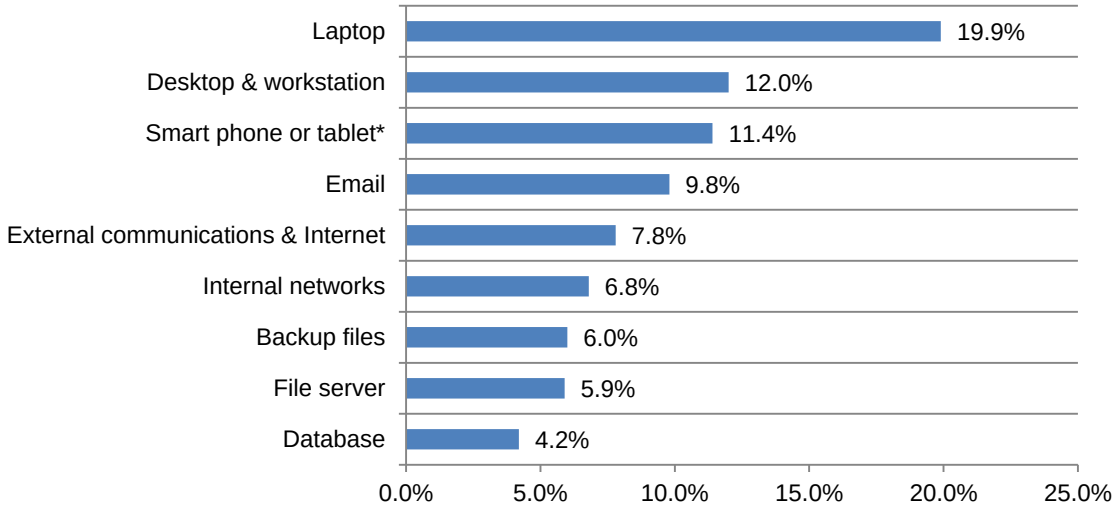
Figure 9. U.S. trends on the extensive use of encryption technologies



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

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 encryption.

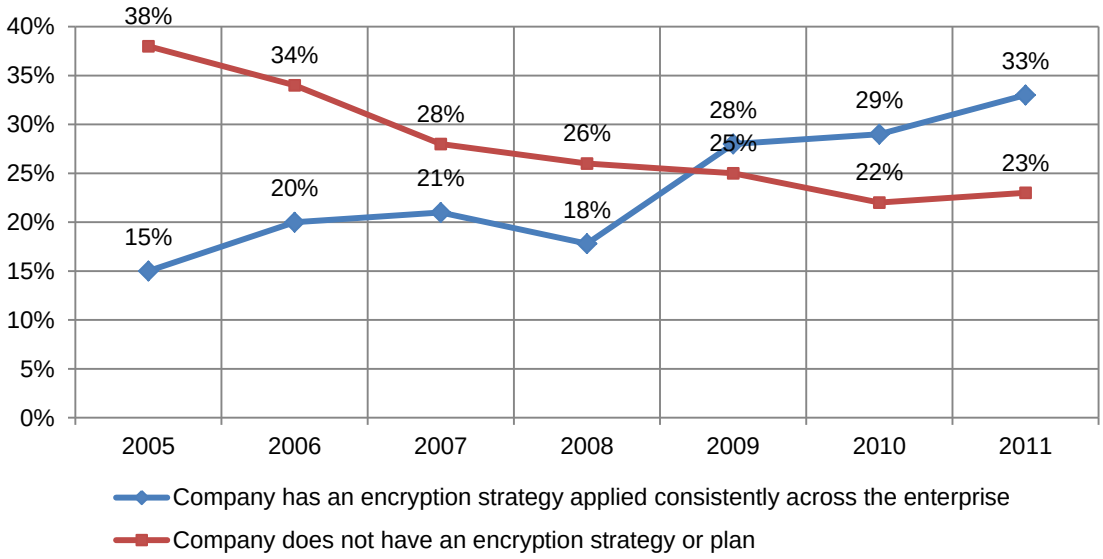
Figure 10. U.S. growth rates for enterprise encryption by technology category
Percentages are calculated from average rates over a seven-year period from 2005 to 2011
*The growth rate for smart phone or tablet technologies was calculated over two years



Trends in strategy

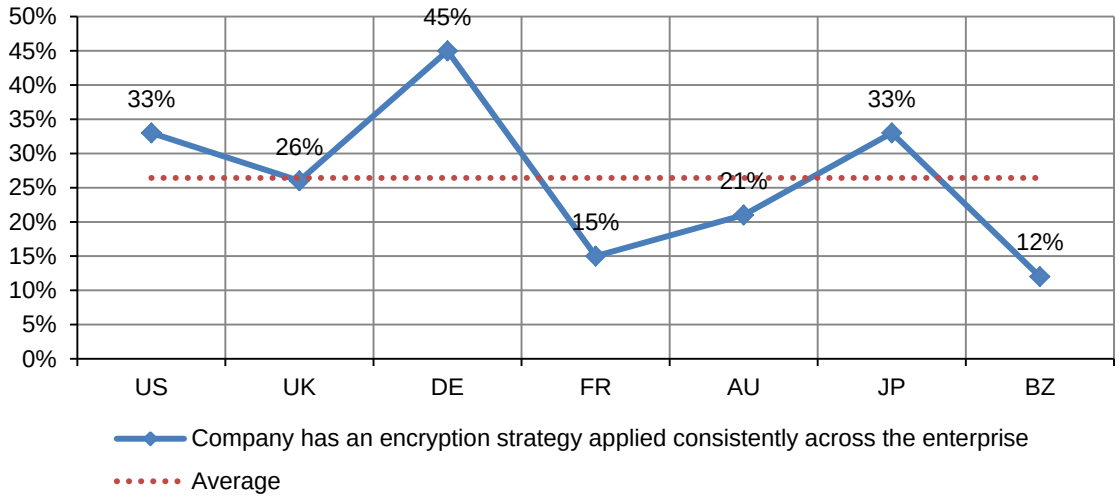
There has been a steady increase in organizations with an overall encryption plan or strategy that is applied consistently across the entire enterprise and a steady decline in not having an encryption plan or strategy. Figure 11 shows how the response has changed over the past seven years. It is clear 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 U.S.encryption strategy



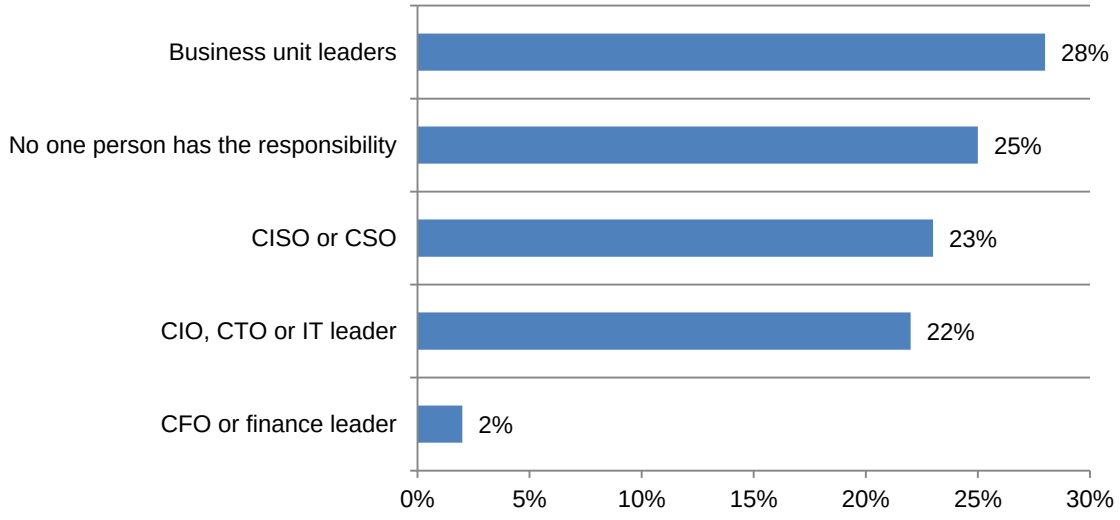
According to Figure 12, the prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany followed by the US and Japan. Respondents in France and Brazil report the lowest prevalence 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 view of U.S. respondents. The chart shows that business unit leaders are most influential in framing the organization's approaches to encryption.

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



Business unit leaders have been steadily gaining influence over their company's encryption strategy since we began studying trends in encryption usage. The U.S. trend in Figure 14 shows that the company's IT leader is no longer the most influential person in determining the organization's approaches to encryption. As mentioned earlier, the increasing influence of business unit leaders in choosing encryption solutions may reflect a broader trend in the consumerization of IT.

Figure 14. U.S. trends in the influence IT and business unit leaders have on encryption strategy

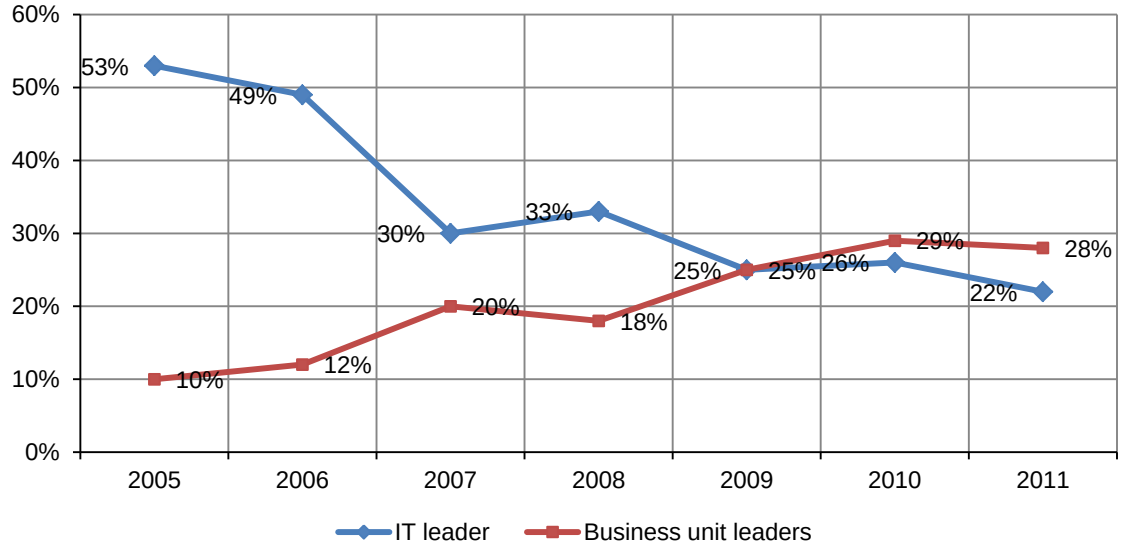


Figure 15 shows the distribution of respondents who rate business unit leaders as the most influential in determining their organization's encryption strategy. The business unit leader is most influential in the U.S. (28 percent), Japan (26 percent) and Germany (25 percent). In contrast, the business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

Figure 15. Influence of business leader by country samples

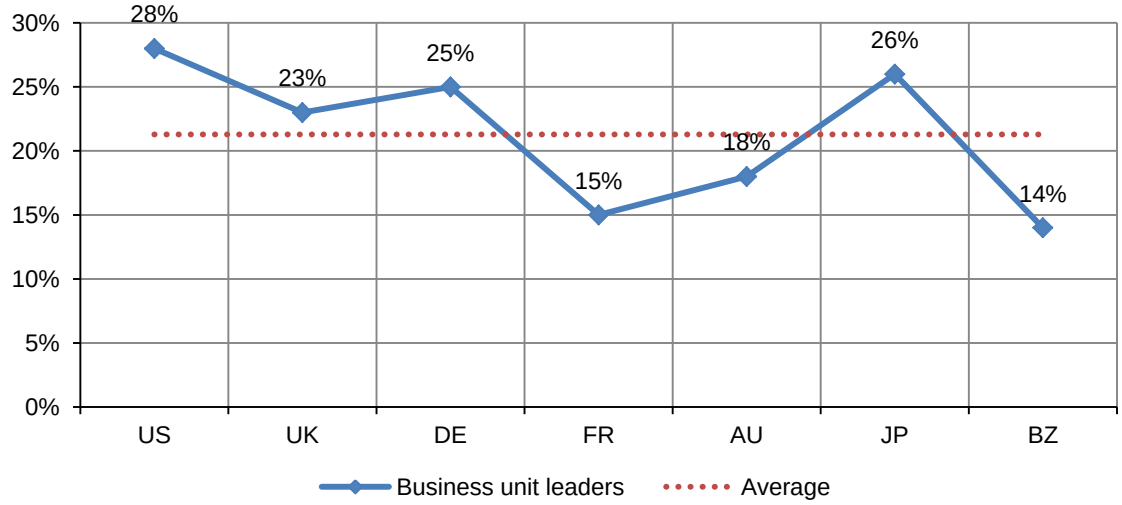
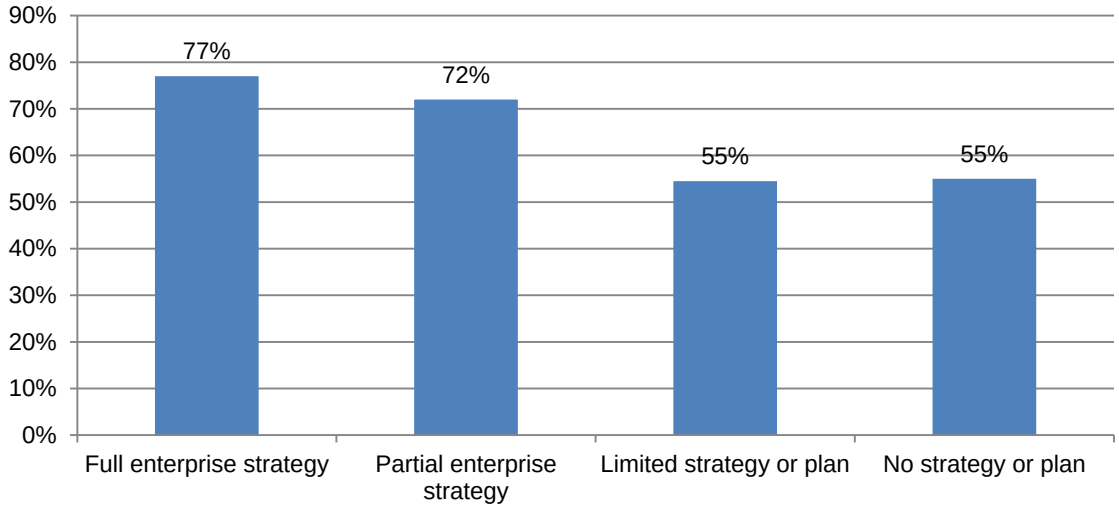


Figure 16 illustrates a cross-tabulation on the affect of compliance on encryption strategy. One question asked respondents to select the main drivers to encryption deployment.[6] The other question asked respondents to place their organization into one of four possible encryption strategy groups. Among the respondents who say their organizations have a full enterprise

[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, 65 percent of respondents selected the "compliance with privacy and data security regulations" option (which is the highest rated response).

strategy, 77 percent rate compliance as a main driver to encryption. In contrast, those who say their organizations do not have a strategy or plan, only 55 percent rate compliance as the main driver.

Figure 16. U.S. compliance orientation and encryption strategy



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, discovering data at risk, protecting data in motion on public facing Internet applications and identity and access management were viewed as top priorities for participants in the U.S. study. Lower priorities are protecting data in outsourced or cloud environments and training and certification of employees.

Figure 17. U.S. ranking of data protection priorities
Highest rank = 13, lowest rank = 1

Encryption features considered most important. U.S. respondents were asked to rate nine encryption technology features considered most important as shown in Figure 18. According to the consolidated findings, automated encryption policy enforcement and encryption on mobile data-bearing devices used by employees were the two top rated features.

Figure 18. U.S. ranking of encryption technology solutions
Very important & important responses combined

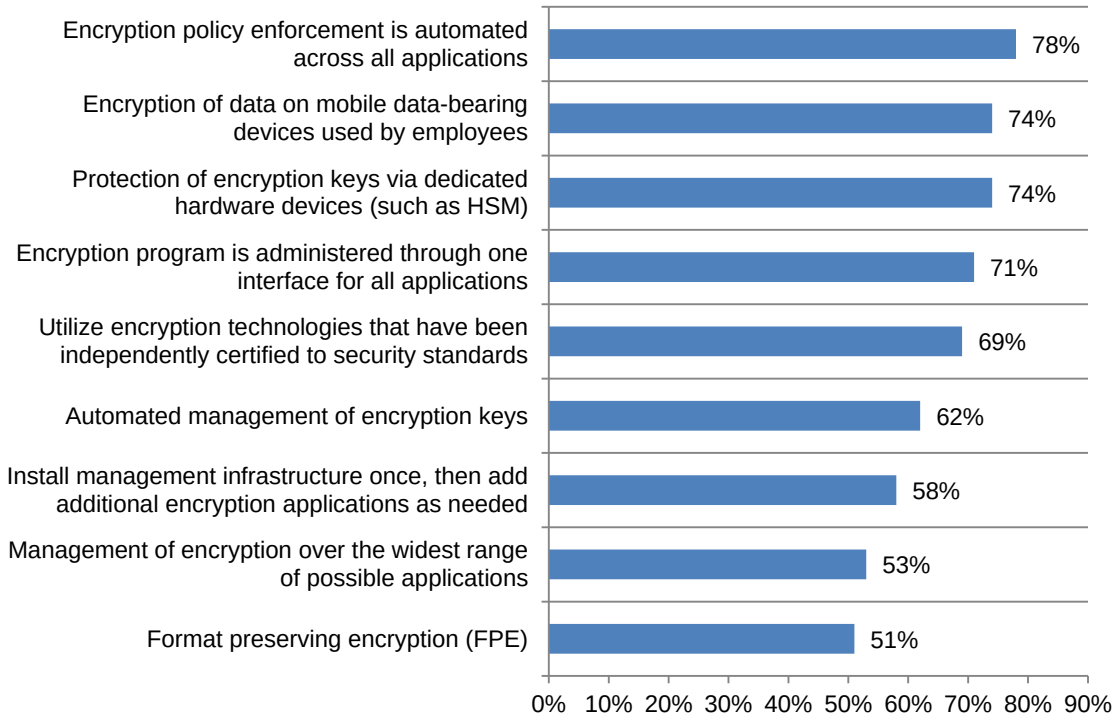
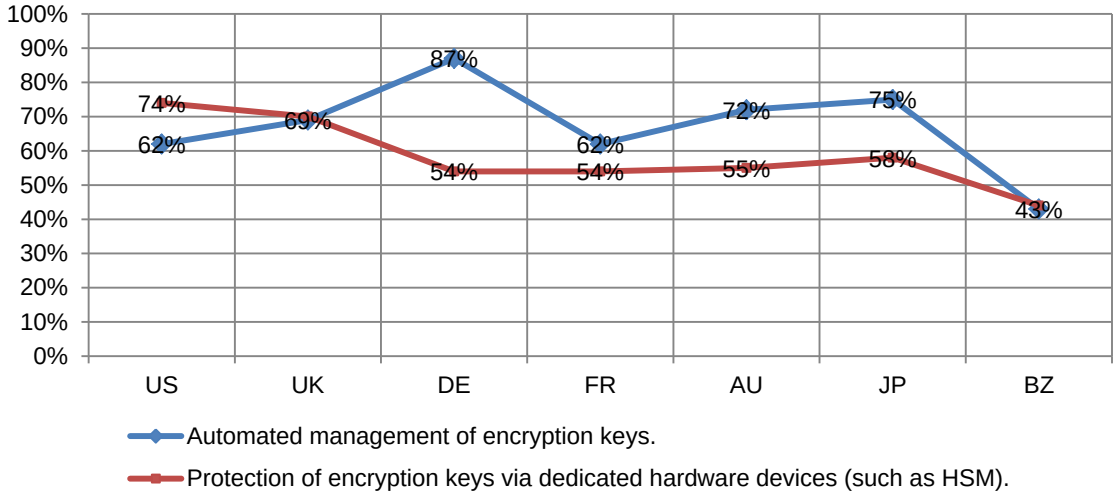


Figure 19 reports the two aspects relating to key management by country samples. With the exception of Brazil, respondents in all other countries attach a high level of importance (above 50 percent) to key management. The protection of encryption keys via dedicated hardware devices (such as HSM) is also 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. U.S. findings reveal that data protection is a critical part of organizations' risk management efforts. As shown in Figure 20, 75 percent say data protection is very important and 21 percent say it is important to their organization's risk management efforts.

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

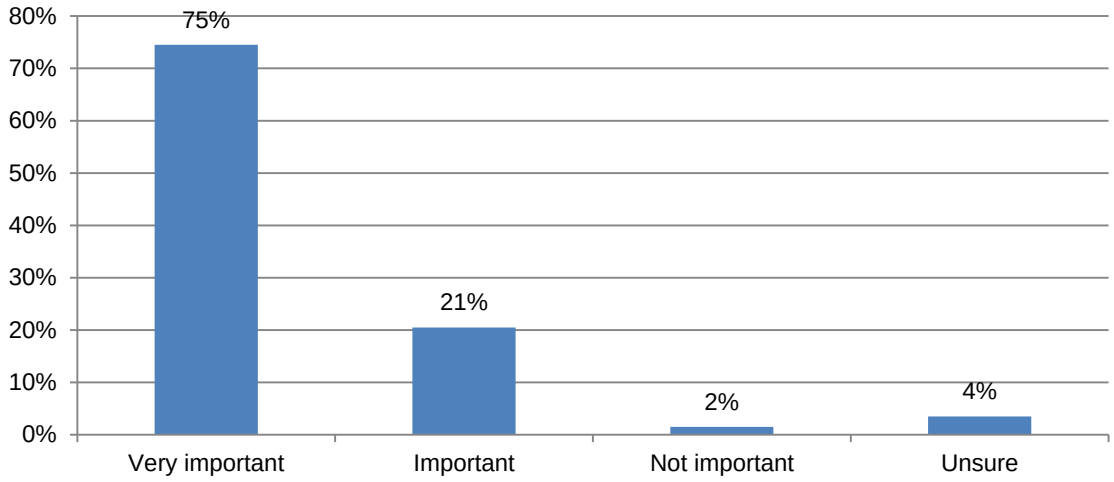
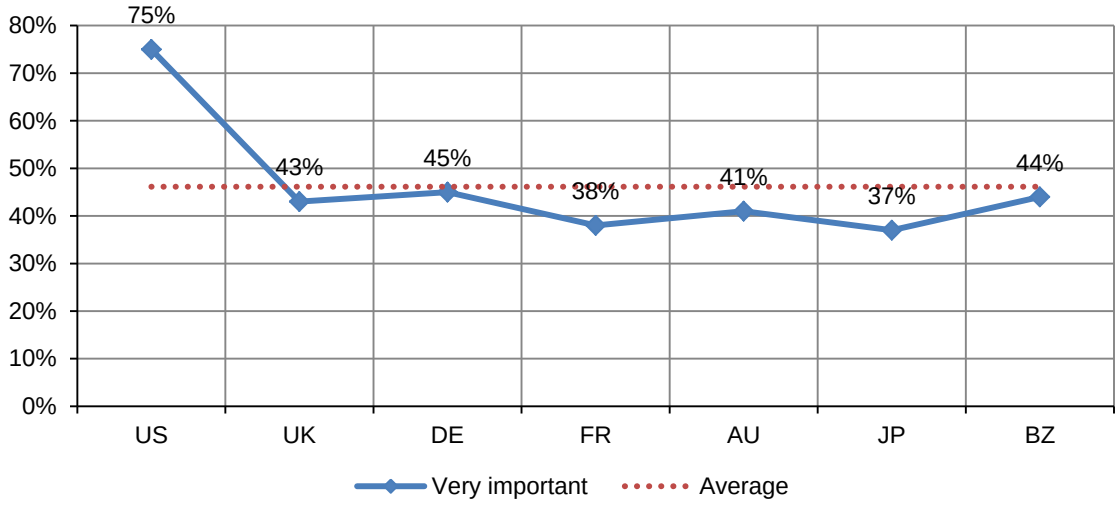


Figure 21 reports the very important response across seven countries. With an average very important rating of 75 percent, the US appears as an outlier when compared to other countries. In contrast, the other country ratings are closely aligned between 38 and 45 percent.

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 rates the highest among U.S. respondents for client-controlled devices. In the data center systems environment, the two highest threats to sensitive or confidential data are third party mishaps and broken business processes**.**

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

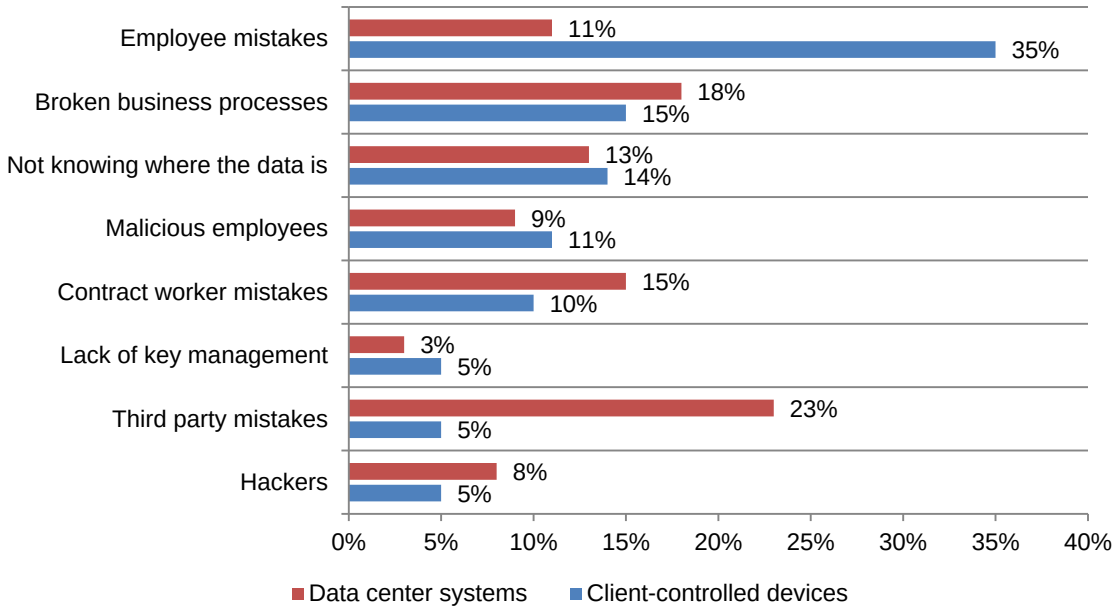


Figure 23 reports the top three threats for client-controlled devices by country, which are employee mistakes, not knowing where the data is and broken business processes. Employee mistakes are rated highest in France, Australia and the U.S. The inability to locate data is rated highest in Australia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

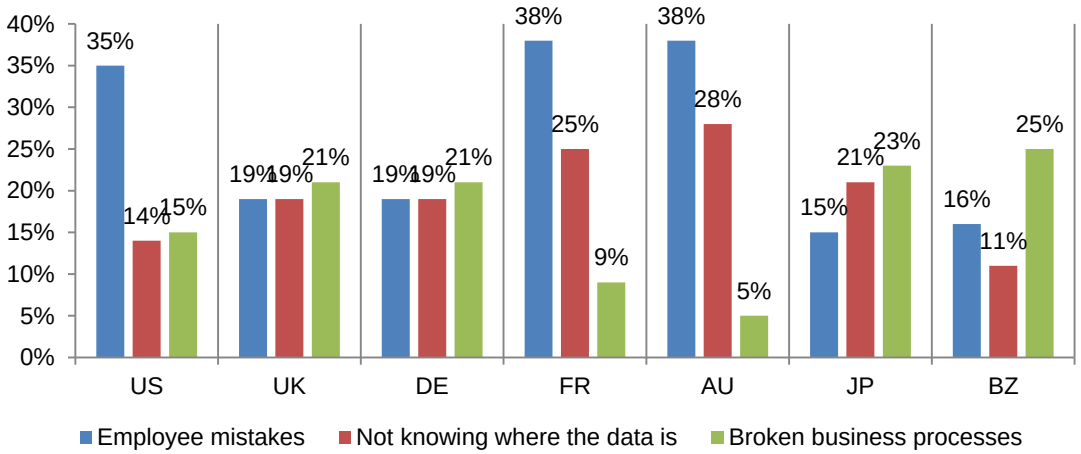
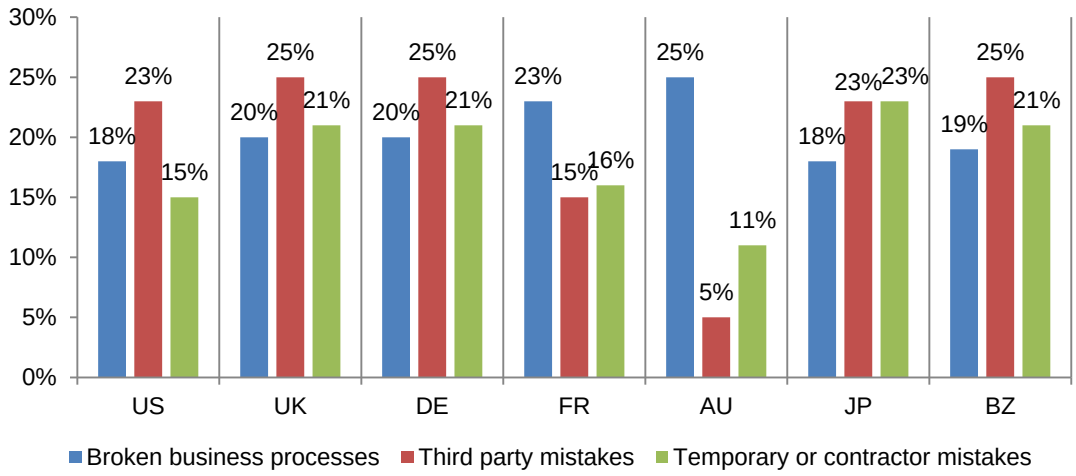


Figure 24 reports the top three threats for data center systems by country, which are broken business processes, third party mistakes and temporary or contractor mishaps. Respondents in Australia and France are most likely to rate broken business processes as a top threat to sensitive or confidential 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

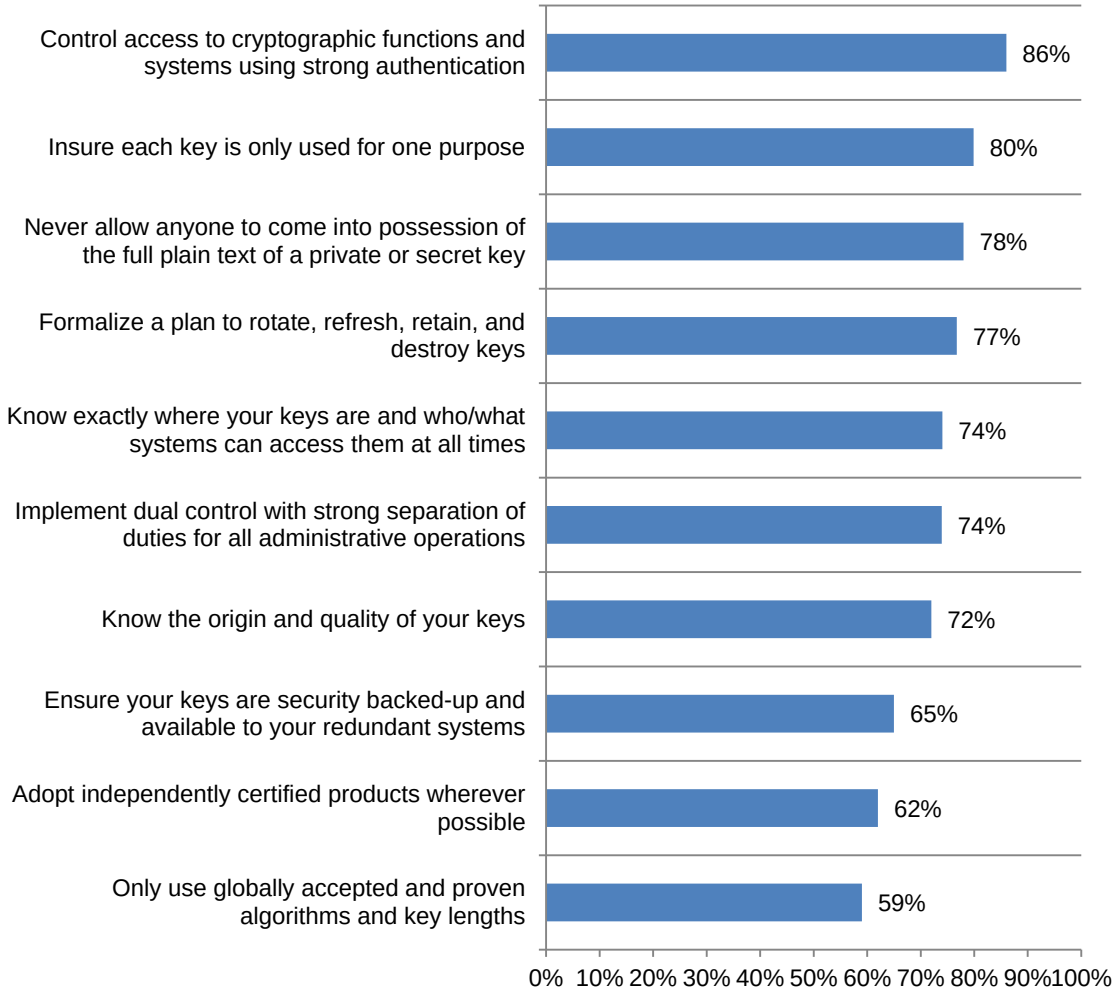


“Standards of due care” for crypto deployment

These are well-established best practices for 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 U.S. respondents, The fact that the average rating for all crypto standards is above the 50 percent mark is strong evidence that respondents acknowledge these standards as best practices.

The top three standards as shown are: control access to cryptographic functions and systems using strong authentication, insure each key is only used for one purpose and never allow anyone to come into possession of the full plain text of a private or secret key.

Figure 25. U.S. 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 57 percent of respondents in the U.S. sample. Figure 26a reports 32 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 37 percent say they use an external tokenization service. The most common class of data tokenized is credit cardholder information, as shown in Figure 26b.

Figure 26a
Types of tokenization deployed (U.S.)

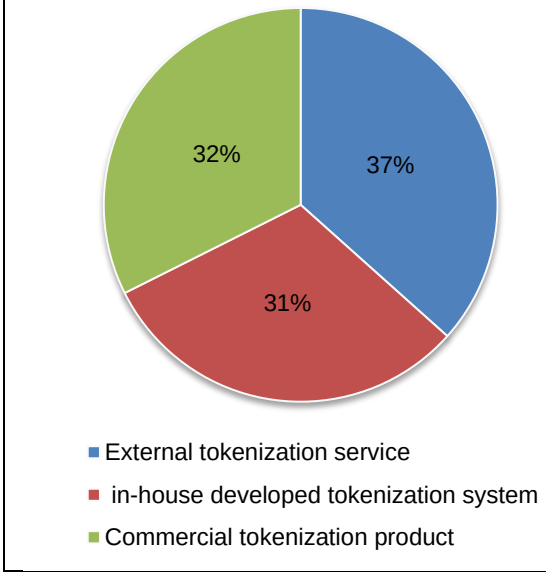
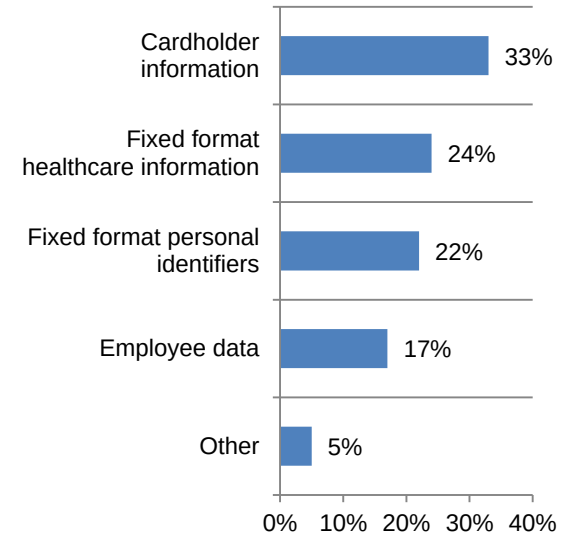
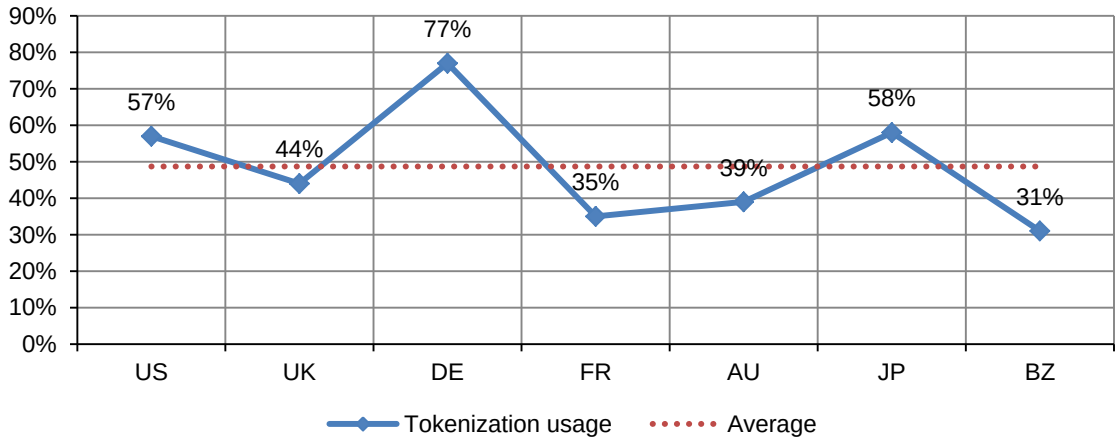


Figure 26b
Classes of data tokenized (U.S.)



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 53 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 and ease of use.

Figure 28a
Is tokenization an alternative to encryption (U.S.)?

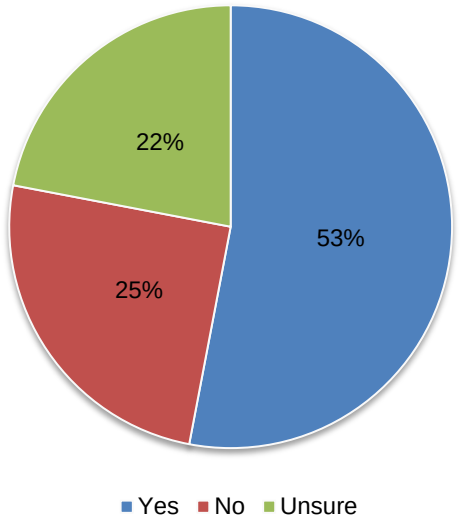


Figure 28b
Reasons for deploying tokenization (U.S.)

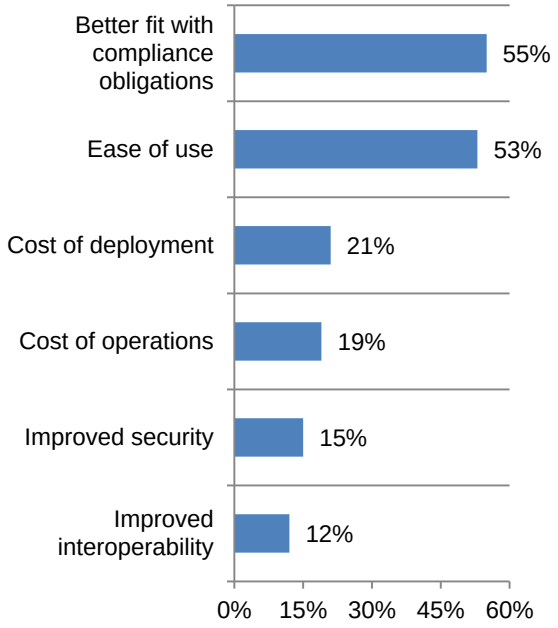
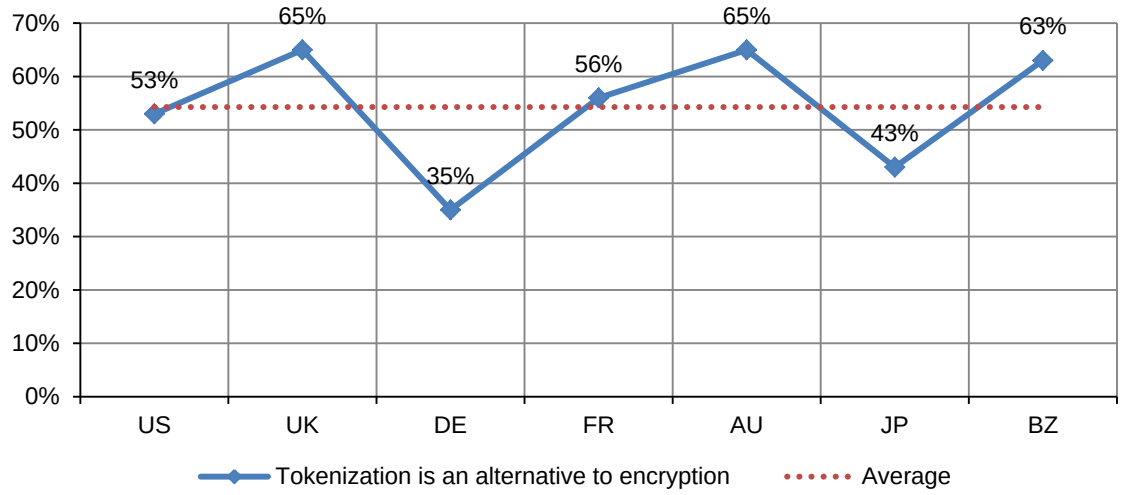


Figure 29 reports the average results by country to the question, "Is tokenization an alternative to encryption deployment?" Despite the fact that Germany reports the highest percentage usage of tokenization, respondents in this country are least likely to see tokenization as an alternative to encryption. 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

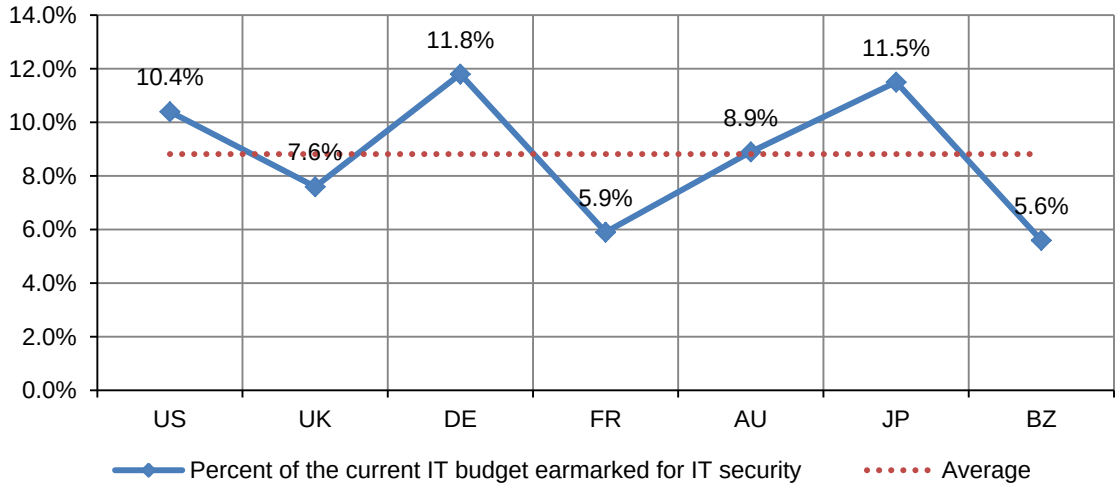


Figure 31 reports the average percent of current IT security relative to total IT over seven years for the U.S. sample. As shown, the trend appears to be upward sloping, which suggests the proportion of IT spending dedicated to security activities including encryption is increasing over time.

Figure 31. U.S. trends in the percent of current IT security relative to the total IT budget

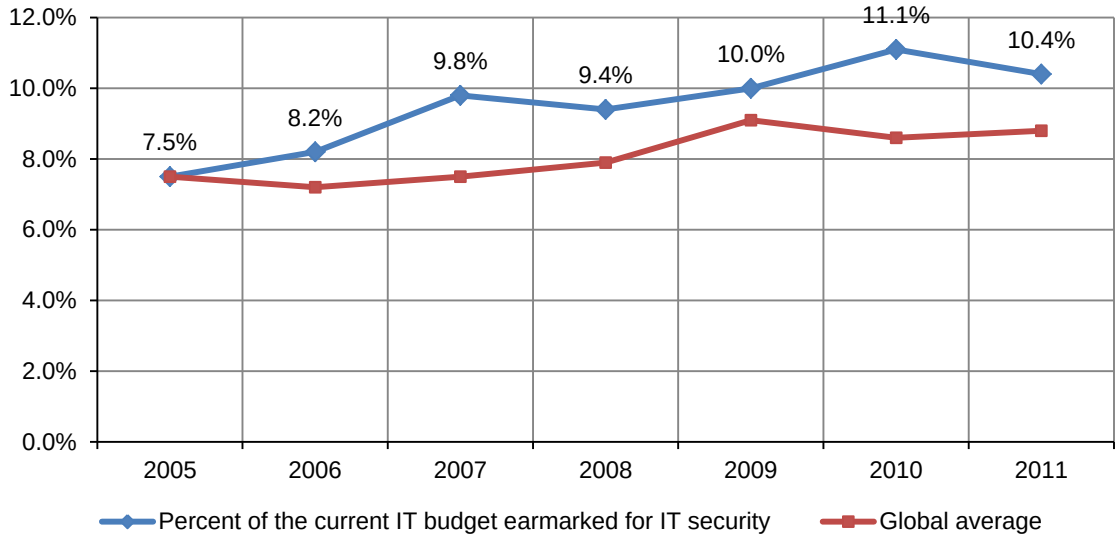


Figure 32 shows the average percent of current IT security spending dedicated to data protection spending by country sample. As shown, the percentage of data protection spending relative to total IT security is highest in the U.S. and France, and lowest in Brazil. Perhaps more important is the consistency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

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

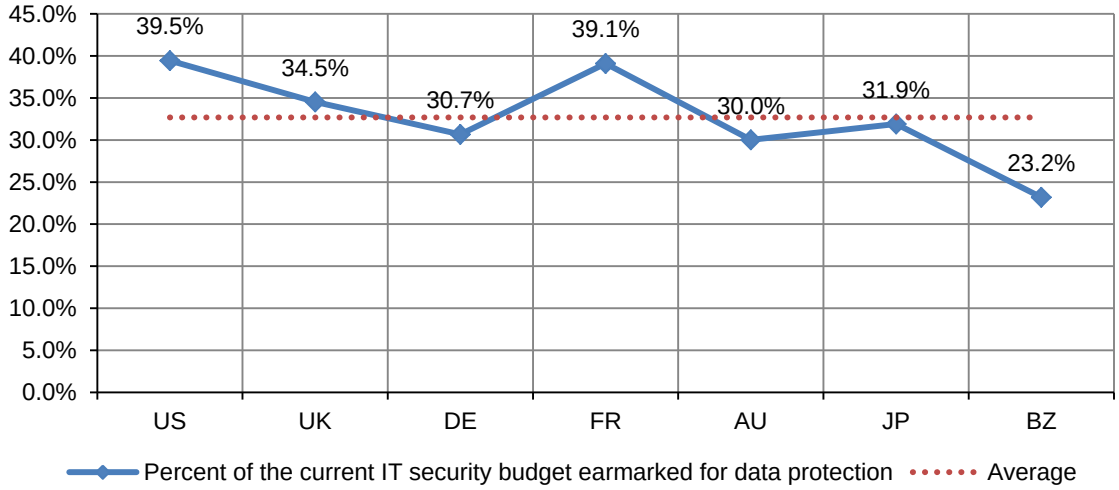


Figure 33 reports the percentage of data protection spending relative to the total IT security budget over seven years for the U.S. sample. Again, this trend appears to be upward sloping, which suggests data protection spending as a proportion of total IT security is on the rise.

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

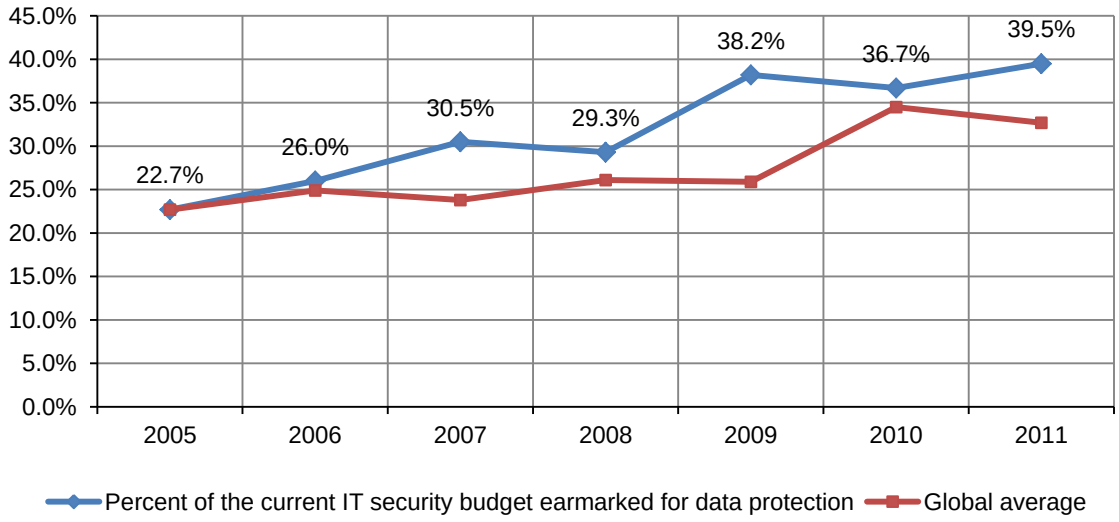


Figure 34 reports the percentage of IT security spending dedicated to encryption.[7] This figure also reports the forecasted proportion of encryption spending next year. The pattern shown below by country clearly shows next year's spending at a higher percentage than the current year's spending on encryption.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

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

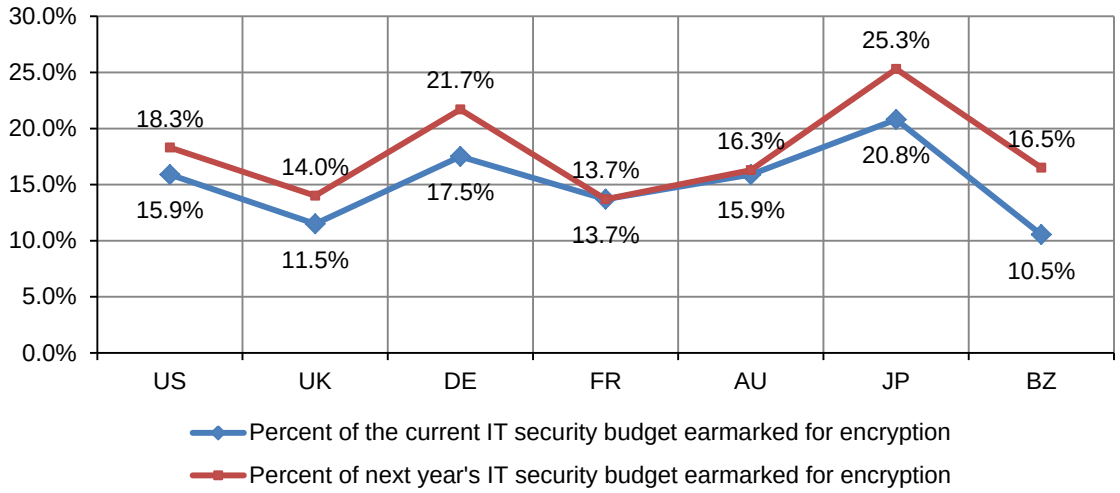
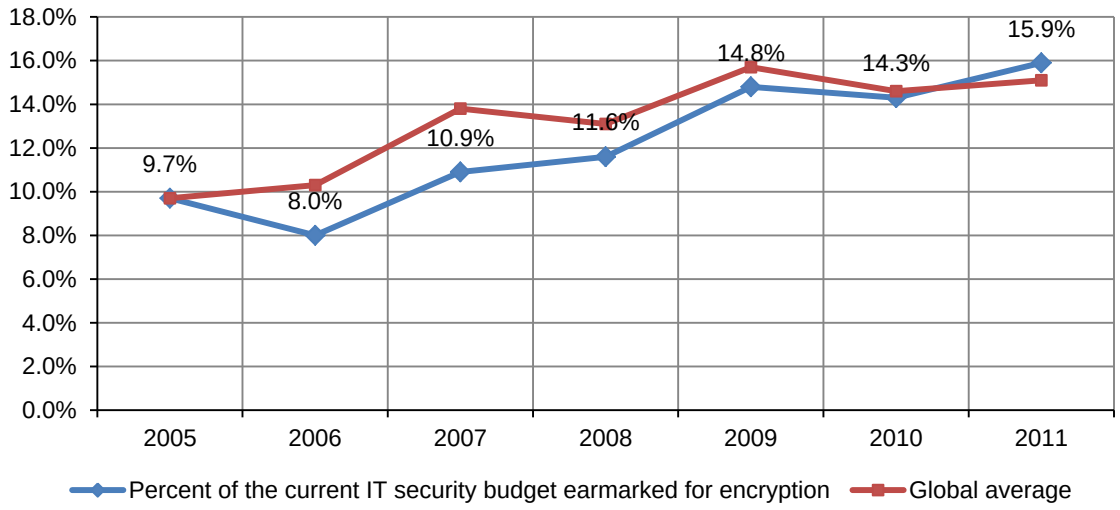


Figure 35 reports the seven-year trend in the percentage of U.S. encryption spending relative to the total IT security budget. Again, the trend appears to be increasing from a low of eight percent in 2006 to 15.9 percent in the present year's encryption trends study.

Figure 35. U.S. trends in the percent of IT security budget dedicated to encryption



[7]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.

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

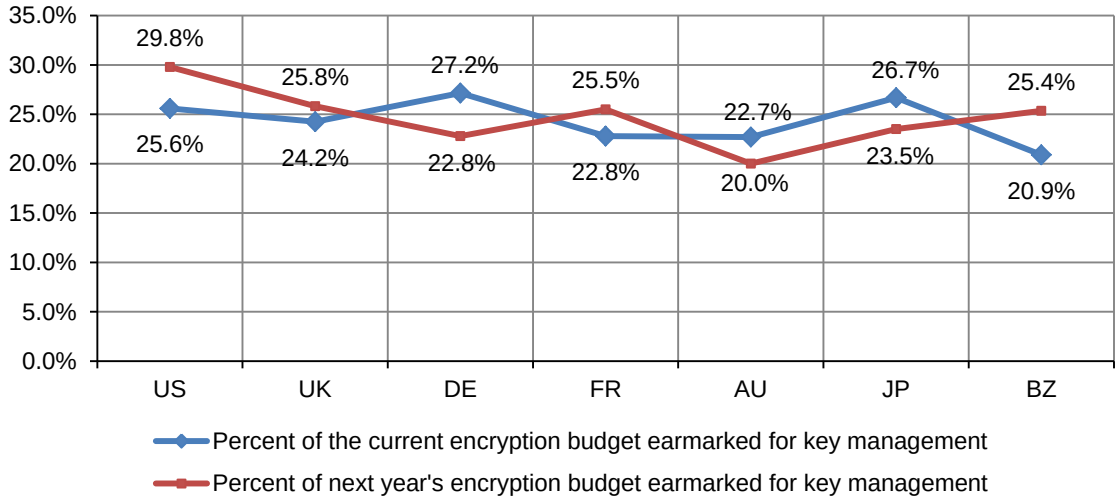


Figure 37 reports the types of key management solutions already deployed or being considered by respondents. The top two choices are multiple key management solutions either from a single vendor (26 percent) or key management solutions are not budgeted (26 percent). Only six percent believe their organization's existing key management solutions are sufficient.

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

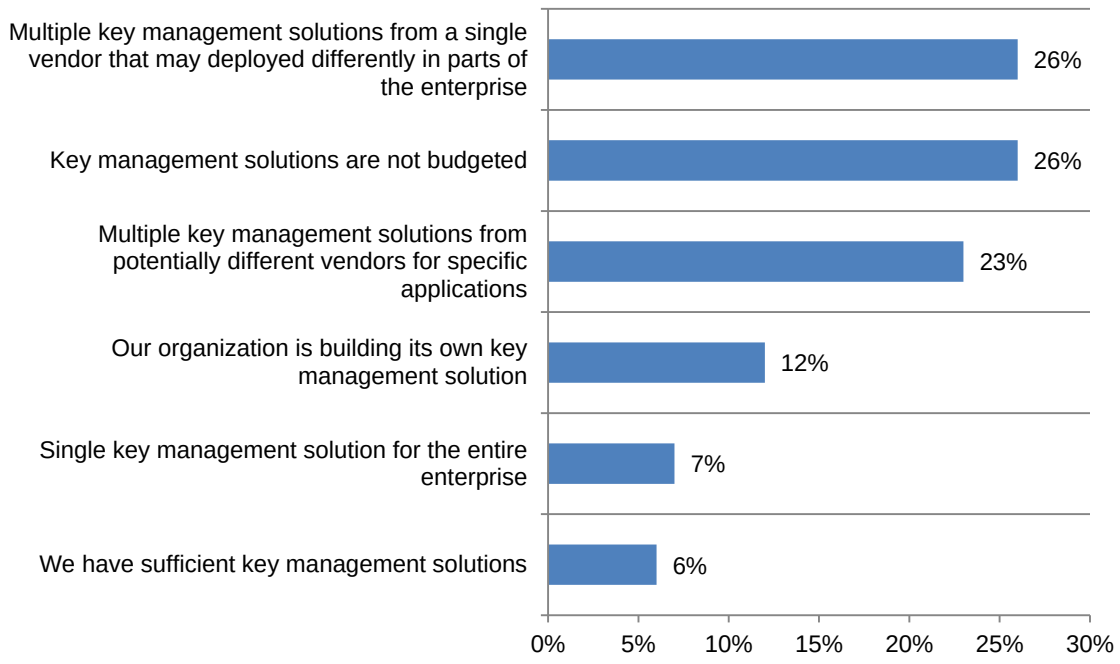


Figure 38 provides a deeper analysis to the response "single key management solution for the entire enterprise" by the calculated SES. As previously mentioned, we use the SES as a measure of each organization's security posture. As can be seen, respondents within the first quartile (highest SES group) 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. U.S. analysis of the response "single key management solution for the entire enterprise" by sample quartiles defined by SES

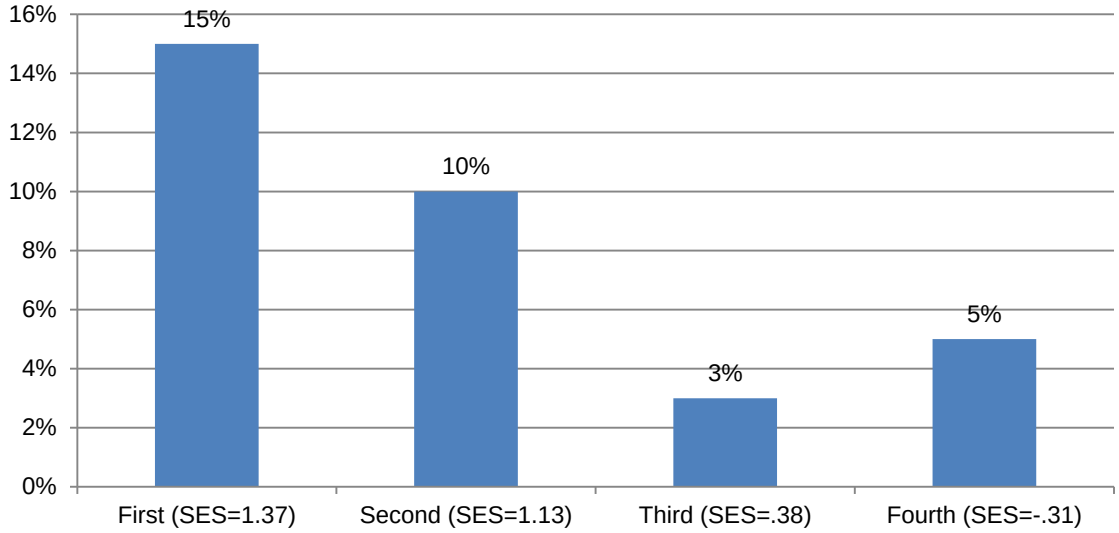
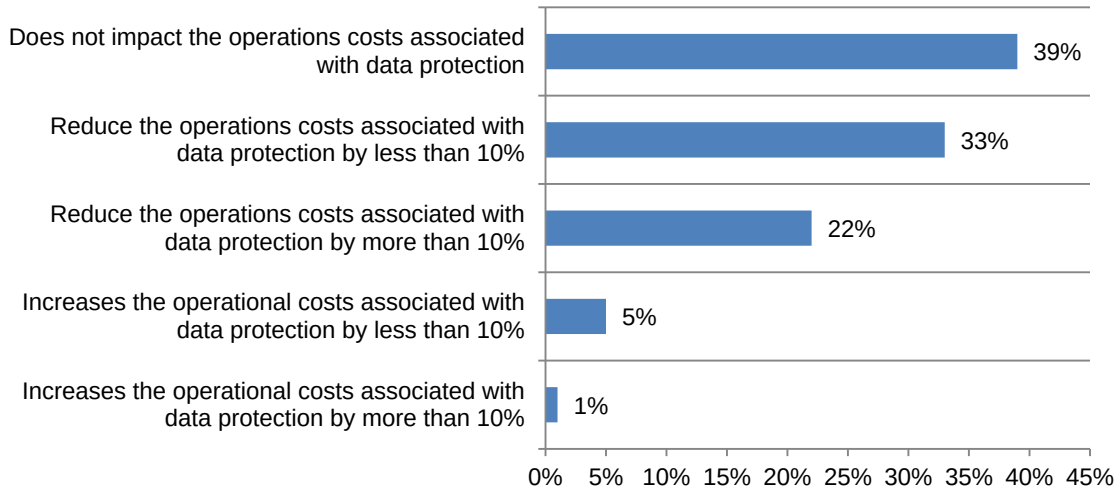


Figure 39 summarizes what respondents perceive as the economic impact of key management solutions on operating costs. A majority of U.S. respondents hold a favorable view – wherein 33 percent see a cost decrease by less than 10 percent and 22 percent see a cost decrease by more than 10 percent. Thirty-nine percent of respondents do not see any cost impact resulting from new key management expenditures.

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



Part 3. Methods & Limitations

The sample response for this study was 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 and Japan in 2011.

Table 3 reports the sample response for the U.S. study. As shown, 26,501 individuals were selected for participation, of which 24,562 received invitations to join this web-based survey. A total of 1,016 individuals completed the survey and 104 of these returns were rejected on the basis of objective reliability criteria. The final sample of U.S. respondents is 912 individuals, which represents a 3.4 percent response rate.

Table 3. U.S. sample response	**Freq,**	**Pct%**
Total sampling frame	26,501	100.0%
Invitations	24,562	92.7%
Total returns	1,016	3.8%
Rejected surveys	104	0.4%
Final sample	912	3.4%

As noted in Table 4, the respondents' average (mean) experience in IT, IT security or related fields is 11.9 years. Approximately 29 percent of respondents are female and 71 percent male.[9]

Table 4. Other characteristics of respondents			
Experience levels	Mean	Gender	Pct%
Overall experience	12.92	Female	29%
IT or security experience	11.9	Male	71%
Years in present position	5.51	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 U.S. respondents. As can be seen, the majority (65 percent) of respondents are at or above the supervisory level.

Figure 37. Distribution of respondents according to position level
U.S. national sample

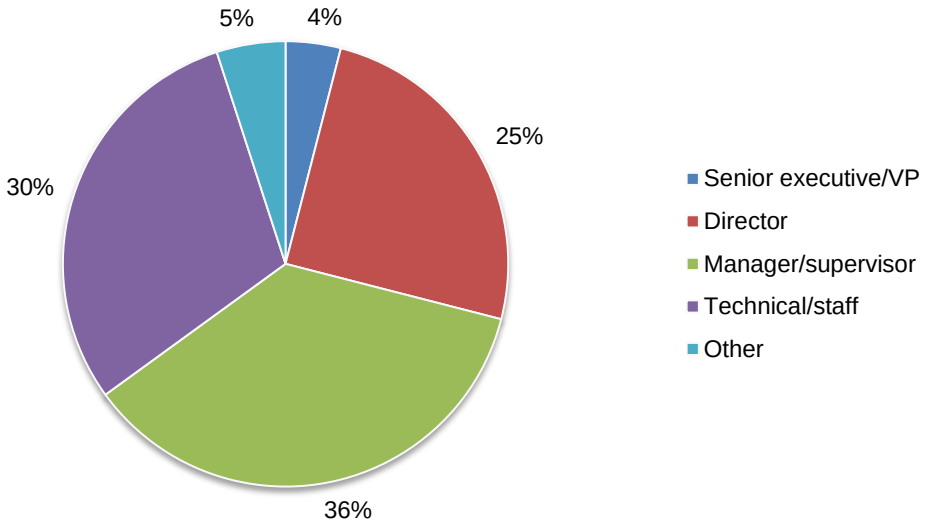
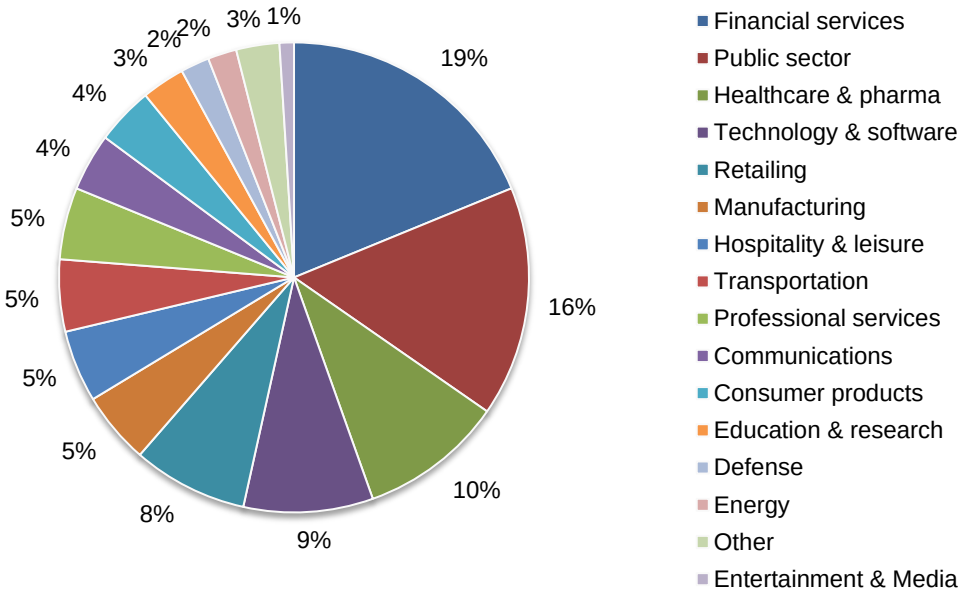


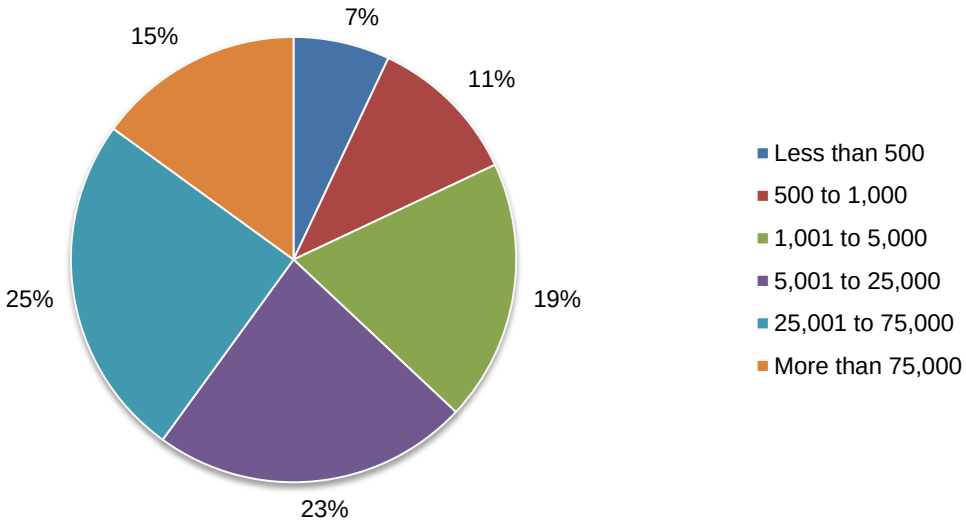
Figure 38 reports the U.S. respondents' organizations primary industry segments. As shown, 19 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 16 percent are located in public sector organizations, including central and local government.

Figure 38. Distribution of respondents according to primary industry classification
U.S. national sample



According to Figure 39, the majority of U.S. respondents (63 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
U.S. national sample



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 companies 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.

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.