Encryption in the Cloud

Who is responsible for data protection in the cloud?

Sponsored by Thales e-Security

Independently conducted by Ponemon Institute LLC

Publication Date: July 2012

THALES

Ponemon INSTITUTE

Encryption in the Cloud[1]

Ponemon Institute, July 2012

Part 1. Executive Summary

For the first time, Ponemon Institute is pleased to present the findings of *Encryption in the Cloud*. This research is a supplementary report that is part of a larger study entitled the *2011 Global Encryption Trends Study* published in February 2012. In this study, we surveyed 4,140 business and IT managers in the United States, United Kingdom, Germany, France, Australia, Japan and Brazil.[2] The purpose of the presented research is to examine how organizations go about protecting a plethora of information assets entrusted to cloud providers.

In our research we consider how encryption is used to ensure sensitive or confidential data is kept safe and secure when transferred to external-based cloud service providers. We believe these findings are important because they demonstrate the relationship between encryption and the preservation of a strong security posture in the cloud environment. As shown in this research, organizations with a relatively strong security posture are more likely to transfer sensitive or confidential information to the cloud. The high-level questions asked and issues sought by this research are specified as follows:

- What percent of organizations currently transfer sensitive or confidential data to external cloud-based services?
- Who is most responsible for protecting sensitive or confidential data transferred to an external cloud-based service provider? Is it the cloud provider, the cloud consumer or is it a shared responsibility?
- Do organizations have the ability to safeguard sensitive or confidential data before or after it is transferred to the cloud?
- Do respondents believe their cloud providers have the ability to safeguard sensitive or confidential data within the cloud?
- In the eyes of respondents, does the adoption of cloud services impact their organization's security posture?
- Where is encryption applied to protect data that is transferred to the cloud?
- Do organizations fully comprehend or even have visibility of the steps or measures taken by the cloud provider to protect sensitive or confidential data?
- Who manages encryption keys when sensitive and confidential data is transferred to the cloud?

Following is a summary of key findings relating to data protection, encryption and key management activities in the cloud.

1. Currently, about half of all respondents say their organizations transfer sensitive or confidential data to the cloud environment. Within the next two years, another one-third of respondents say their organizations are very likely to transfer sensitive or confidential to the cloud. At 56 percent, German companies appear to have the highest rate of sensitive or confidential data transferred to the cloud.

2. Thirty-nine percent of respondents believe cloud adoption has decreased their companies' security posture. However, 44 percent of respondents believe the adoption of cloud services has not increased or decreased their organization's security posture. Only 10 percent of respondents believe the move to the cloud has increased their organization's security posture. With respect to country differences, results suggest that French organizations are most likely to view cloud deployment as diminishing the effectiveness of data protection efforts.

3. Forty-four percent of respondents believe the cloud provider has primary responsibility for protecting sensitive or confidential data in the cloud environment and 30 percent believe it is the cloud consumer. There are also differences among countries as to who is most responsible. Sixty-seven percent of French companies appear to be the most likely to hold the cloud provider responsible for data protection activities. In contrast, 48 percent of Japanese companies hold the cloud consumer primarily responsible for data protection.

---

[1]This research is part of a larger survey project. See 2011 Global Encryption Trends Study. Ponemon Institute, February 2012 for more details about the survey and sampling methods used in the present study.
[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).

4. Companies that currently transfer sensitive or confidential data to the cloud are much more likely to hold the cloud provider primarily responsible for data protection. In contrast, companies that do not transfer sensitive or confidential information to the cloud are more likely to hold the cloud consumer with primary responsibility for data protection.

5. Sixty-three percent of respondents say they do not know what cloud providers are doing to protect the sensitive or confidential data entrusted to them. Once again, French respondents (76 percent) are least likely to say they know what their cloud providers do to safeguard their organization's information assets.

6. In general, respondents who select the cloud provider as the most responsible party for protecting data are more confident in their cloud provider's actual ability to do so (51 percent) compared to only 32 percent of respondents who report confidence in their own abilities to protect data even though they consider their own organization to be primarily responsible for protecting data.

7. Where is data encryption applied? According to 38 percent of respondents, their organizations rely on encryption of data as it is transferred over the network (typically the internet) between the organization and the cloud. Another 35 percent say the organization applies persistent encryption data before it is transferred to the cloud provider. Only 27 percent say they rely on encryption that is applied within the cloud environment.

8. Among the companies that encrypt data inside the cloud, nearly 74 percent believe the cloud provider is most responsible for protecting that data. However, only 34 percent of organizations that encrypt data inside their organization prior to sending it to the cloud hold the cloud provider primarily responsible for data protection.

9. Who manages the encryption keys when sensitive or confidential data is transferred to the cloud? Thirty-six percent of respondents say their organization is most responsible for managing the keys. Twenty-two percent say the cloud provider is most responsible for encryption key management. Another 22 percent says a third party (i.e. another independent service provider) is most responsible for managing the keys. Even in cases where encryption is performed outside the cloud, more than half of respondents hand over control of the keys. With respect to country differences, German organizations appear to be the least likely to relinquish control of encryption keys to the cloud provider. Companies in Australia and Brazil appear to be the most likely to transfer control of encryption keys to the cloud provider.

10. Companies with the characteristics that indicate a strong overall security posture appear to be more likely to transfer sensitive or confidential information to the cloud environment than companies that appear to have a weaker overall security posture. In other words, companies that understand security appear to be willing and able to take advantage of the cloud. This finding appears to be at odds with the common suggestion that more security aware organizations are the more skeptical of cloud security and that it is the less security aware organizations are willing to overlook a perceived lack of security. Here, we use the Security Effectiveness Score (SES) as an objective measure of each organization's security posture.

Part 2. Key Findings

Overall adoption and perceptions about cloud computing

Approximately half of all respondents say their organizations presently transfer sensitive or confidential data to external cloud-based services. Another one-third (33 percent) says their organizations are likely to transfer sensitive or confidential data to the cloud sometime in the next two years. Only 19 percent of respondents say their organizations do not use cloud services for this class of data or have any expectation of doing so in the short-to-medium term.

Figure 1. Does your organization currently transfer (or plan to transfer) sensitive or confidential data to the cloud?
Consolidated view

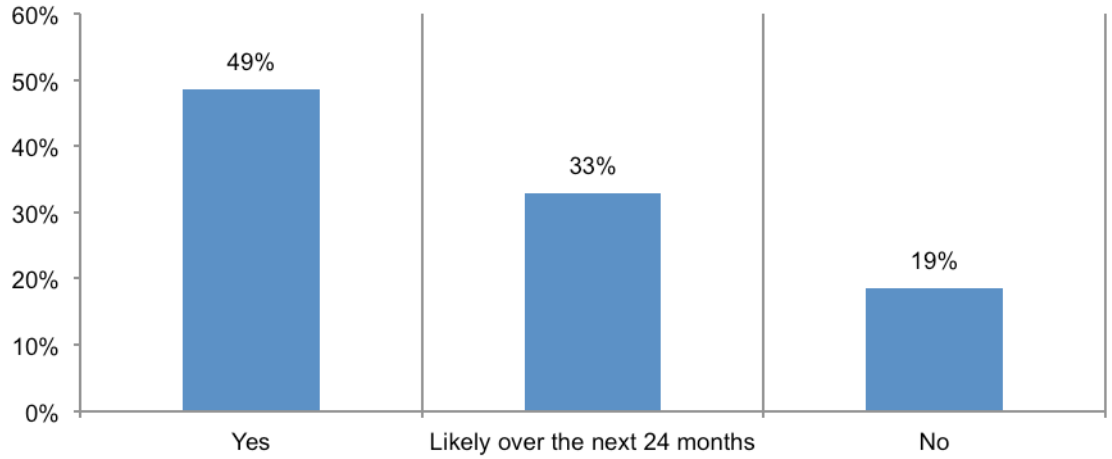
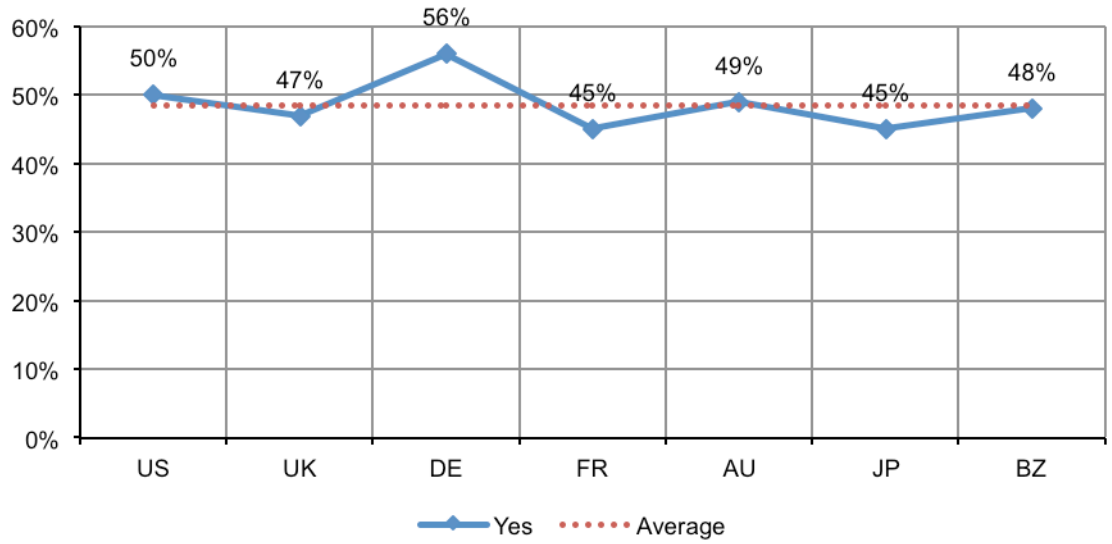


Figure 2 shows the breakout by country on the issue of sensitive or confidential data transferred to the cloud. It shows a constant pattern across country samples, wherein German companies are most likely to transfer sensitive or confidential data (56 percent yes response). In contrast, France and Japan are least likely to transfer sensitive or confidential data to the cloud (both with a 45 percent yes response).

Figure 2. Does your organization currently transfer sensitive or confidential data to the cloud?
Yes response by country



Who is most responsible for protecting sensitive or confidential data in the cloud? According to respondents who say their organizations transfer sensitive or confidential data to the cloud, the entity that is perceived to be most responsible for protecting that data is the cloud provider (44 percent), followed by the cloud consumer (30 percent). Only 24 percent of respondents say the responsibility is shared between providers and consumers of cloud resources.

Figure 3. Who is most responsible for protecting data in the cloud?
Consolidated view

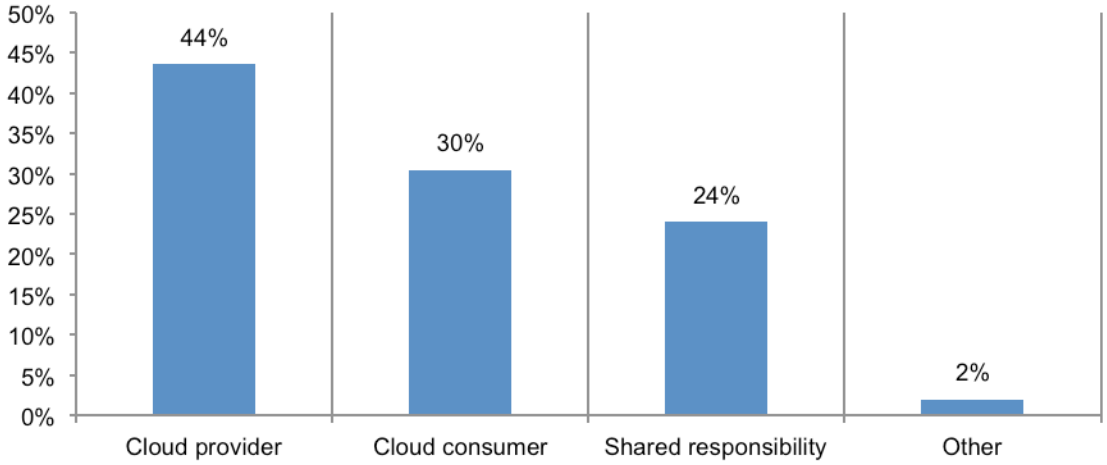


Figure 4 shows that there is marked variation among countries on the question of who is perceived to be the most responsible for protecting sensitive or confidential data transferred to the cloud. Among the seven countries studied in this research, French organizations are most likely to see the cloud provider, and least likely to see the cloud consumer, as the party most responsible for protecting data (67 percent vs.12 percent). In contrast, the cloud consumer is held most responsible in the UK, Australia and Japan.

Figure 4. Who is most responsible for protecting data in the cloud?
Respondents who selected cloud providers and cloud consumers by country

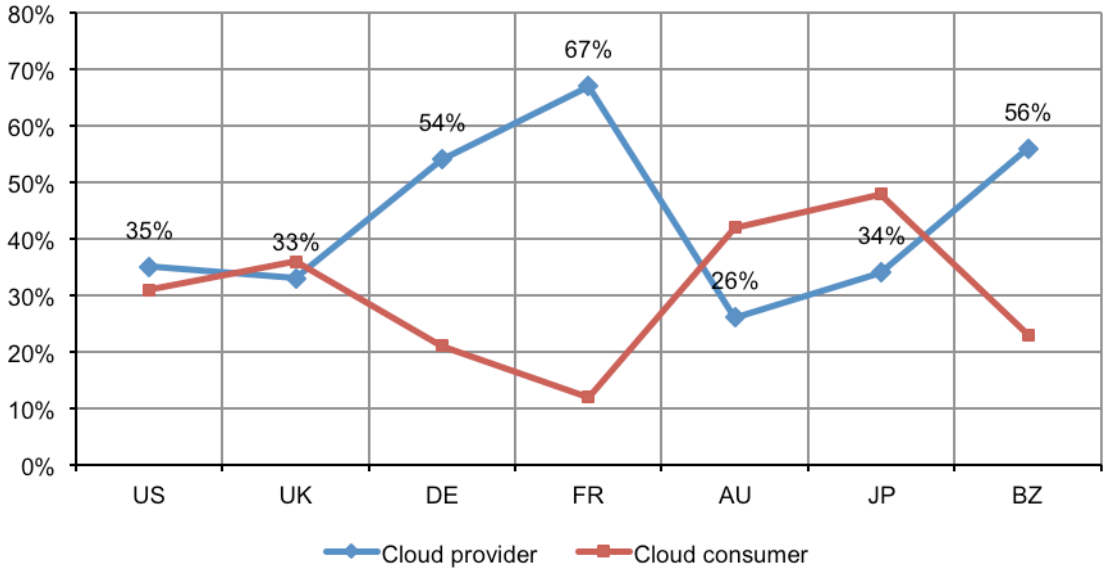
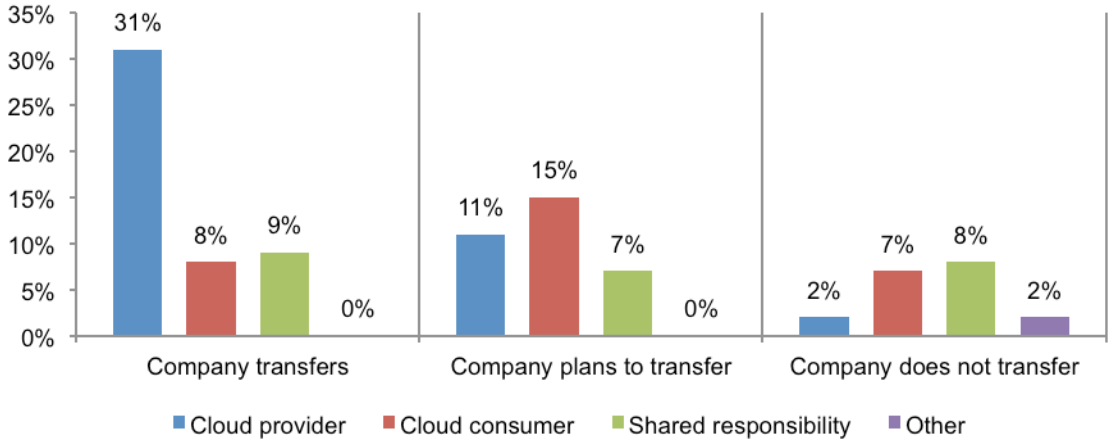


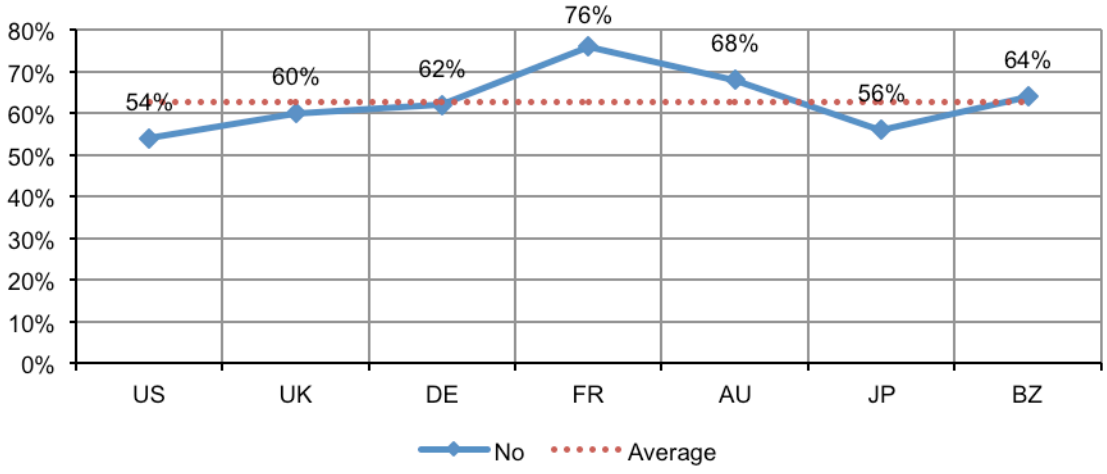
Figure 5 provides the results of a cross-tabulation between two questions: (1) Who is responsible for data protection? (2) Does the company transfer sensitive or confidential data to the cloud? In general, our findings suggest that respondents who currently transfer sensitive data to the cloud have a strong bias towards the cloud provider in terms of where responsibility lies for protecting that data.

Figure 5. Who is most responsible for protecting data transferred to the cloud for three subsamples: (1) companies that transfer, (2) companies than plan to transfer and (3) companies that do not transfer sensitive or confidential data to the cloud. Consolidated view



Having looked at the question of perceived responsibility, we then consider the question of whether organizations actually know what steps or measures are taken by their cloud provider to ensure sensitive or confidential data is protected. Only 29 percent of respondents (in the consolidated sample) say "Yes." Another 72 percent say "No" (63 percent) or were "Unsure" (9 percent). Figure 6 reports the "No" response by country sample. At 76 percent, France reports the highest "No" response. On the other hand, respondents in the U.S. sample record the lowest "No" response (54 percent).

Figure 6. Do you know what your cloud providers are doing to protect your organization's data? "No" response by country



We now turn our attention to assessing levels of confidence, the perceived ability to deliver against those responsibilities. The next two figures summarize confidence ratings for two groups of respondents; namely, those selecting the cloud provider as being primarily responsible for data protection and those selecting themselves, the cloud consumers, as the most responsible parties for protecting sensitive or confidential data. Confidence in this analysis is defined as the percentage agreement to two statements or attributions about data protection contained in our survey instrument.

Figure 7a focuses on the perceived ability of cloud consumers to protect data. Forty-eight (28+20) percent of respondents who believe the cloud provider is most responsible for protecting data, agree that their organization also has the ability to safeguard sensitive or confidential data before being transferred to the cloud (effectively creating an additional layer of protection). In contrast, only 32 (17+15) percent of respondents who say the cloud consumer (typically their own organization) is most responsible, agree with the statement that they have the ability to safeguard sensitive or confidential data before it is transferred to the cloud.

Figure 7a. Rating of the following statement
"My organization has the ability to safeguard sensitive or confidential data before being transferred to the cloud"

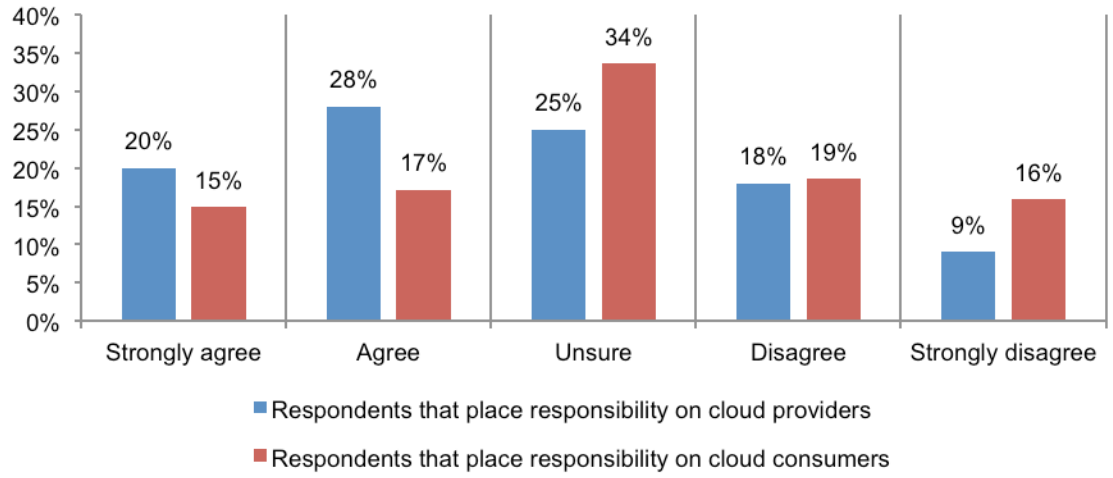
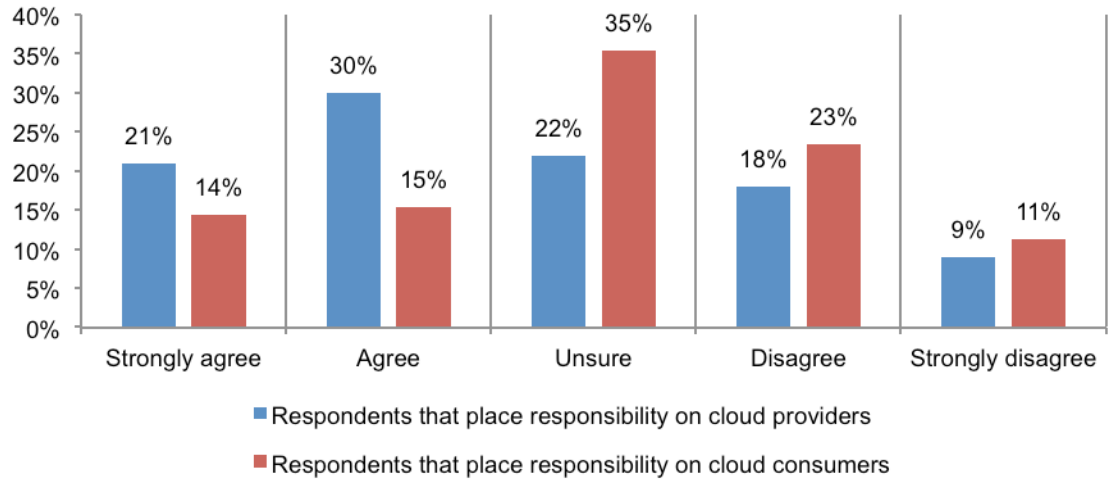


Figure 7b focuses on the perceived abilities of cloud providers to protect data in the cloud. Fifty-one percent of respondents who say the cloud provider is primarily responsible for protecting data agree that their cloud provider has the ability to safeguard sensitive or confidential data within the cloud. However, only 31 percent of respondents who say the cloud consumer is responsible for data protection have confidence that their cloud provider has the ability to protect data.

Figure 7b. Rating of the following statement
"My organization's cloud providers have the ability to safeguard sensitive or confidential data within the cloud"



How does the adoption of cloud services affect the organization's security posture? Figure 8 reports the combined results for seven countries on how the transfer of sensitive or confidential data has changed the organization's security posture. According to 44 percent of respondents, the move from on-premises IT to the cloud has not changed their organizations' security posture. Another 39 percent say the adoption of cloud services has decreased the security posture of the organization. Only 10 percent of respondents believe the adoption of cloud services has actually increased or improved the security of posture of their organizations.

Figure 8. How has the adoption of cloud services changed your organization's security posture?
Consolidated view

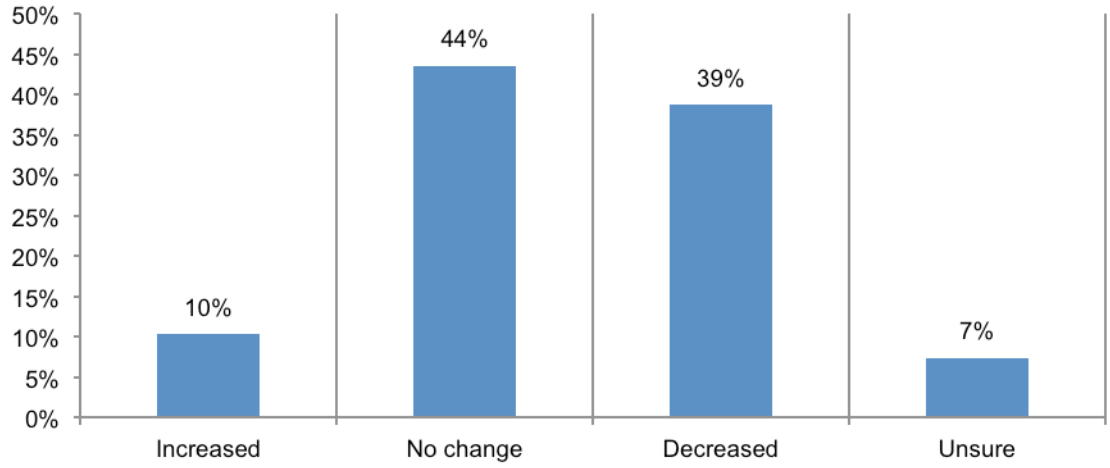
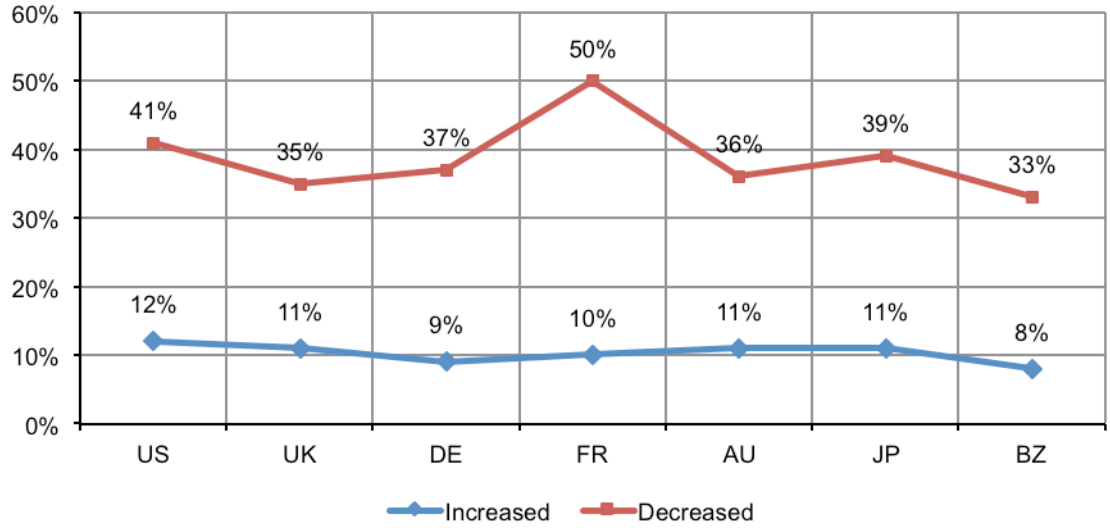


Figure 9 shows that respondents in all seven countries believe the move from in-premise IT to the cloud has weakened or decreased the security posture of the organizations. French companies (50 percent) are most likely to perceive cloud adoption as decreasing the organizations' security posture, while Brazilian companies (33 percent) are least likely to see this negative impact.

Figure 9. How has the adoption of cloud services changed your organization's security posture?
Increased and decreased choices by country



Actual cloud deployment choices

Figure 10 provides various deployment options for encryption in the cloud environment. Respondents were asked to select the practices their organizations presently implement. As can be seen, 38 percent of respondents say the organization encrypts data during its initial transfer over the network between the enterprise and the cloud (typically the internet). Thirty-five percent says their organization encrypts data before it is transferred to the cloud provider, such that it remains encrypted within the cloud. Only 27 (16+11) percent say their organizations perform encryption within the cloud environment.

Figure 10. Where is encryption applied to protect data in the cloud environment?
Consolidated view

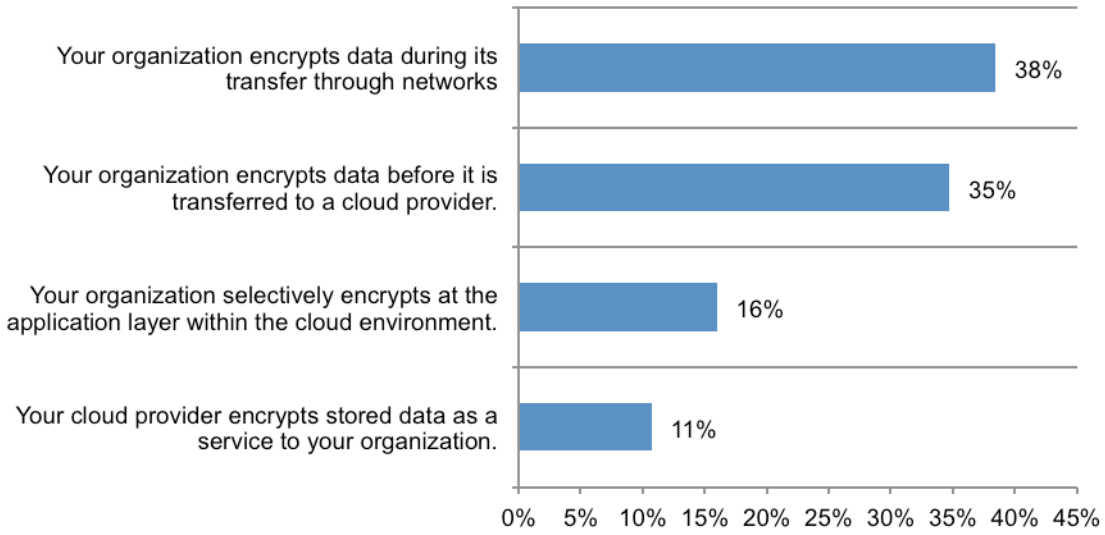
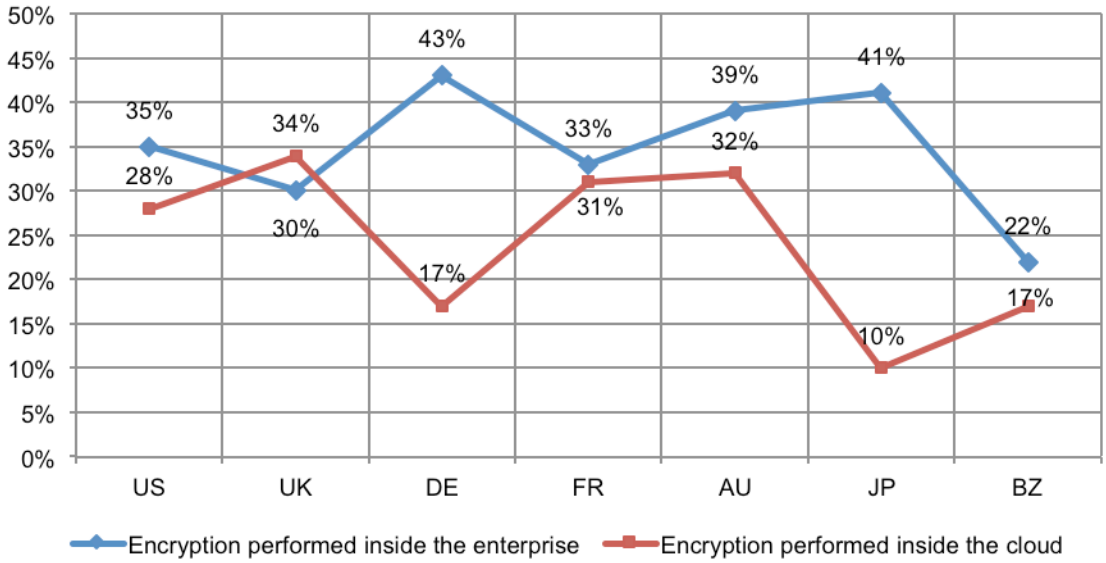


Figure 11 summarizes for each country whether encryption is applied within the enterprise, before being sent to the cloud, or inside the cloud environment. At 43 percent, German companies are most likely to encrypt sensitive or confidential data inside their enterprise environment. In contrast, UK companies (34 percent) are most likely to encrypt data inside the cloud environment.

Figure 11. Where is encryption applied to protect data in the cloud environment?
Inside the enterprise or inside the cloud choices by country



Figures 12a and 12b report who is most responsible for protecting data according to those deploying encryption inside the enterprise or inside the cloud environment. For companies deploying encryption inside the cloud, 74 percent believes the cloud provider is the most responsible entity for protecting sensitive or confidential data. In contrast, for companies deploying encryption inside the enterprise, only 34 percent believes the cloud provider is the most responsible entity.

Figure 12. Who is most responsible for protecting data transferred to the cloud for two subsamples: (1) companies that perform encryption inside the cloud and (2) companies that perform encryption inside the enterprise. Consolidated view

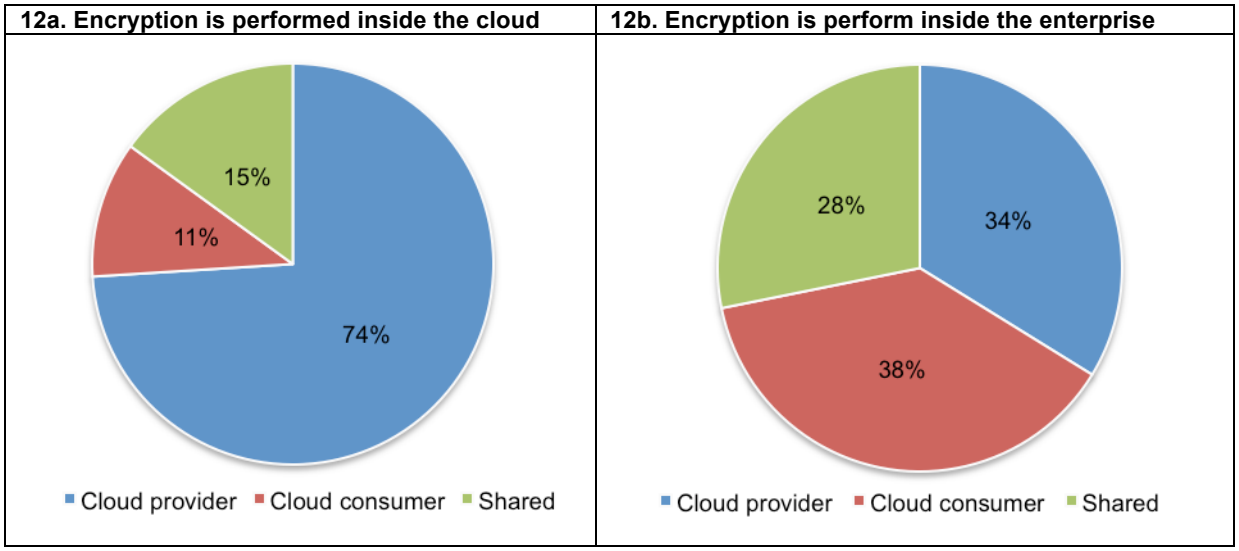


Figure 13 reports which entities are responsible for managing encryption keys when sensitive or confidential data is transferred to the cloud. The organization (a.k.a. cloud consumer) is the most likely to manage encryption keys. Third-party service providers and cloud providers are tied in second place, both at 22 percent for the consolidated sample.

Figure 13. Who manages encryption keys when data is transferred to the cloud?
Consolidated view

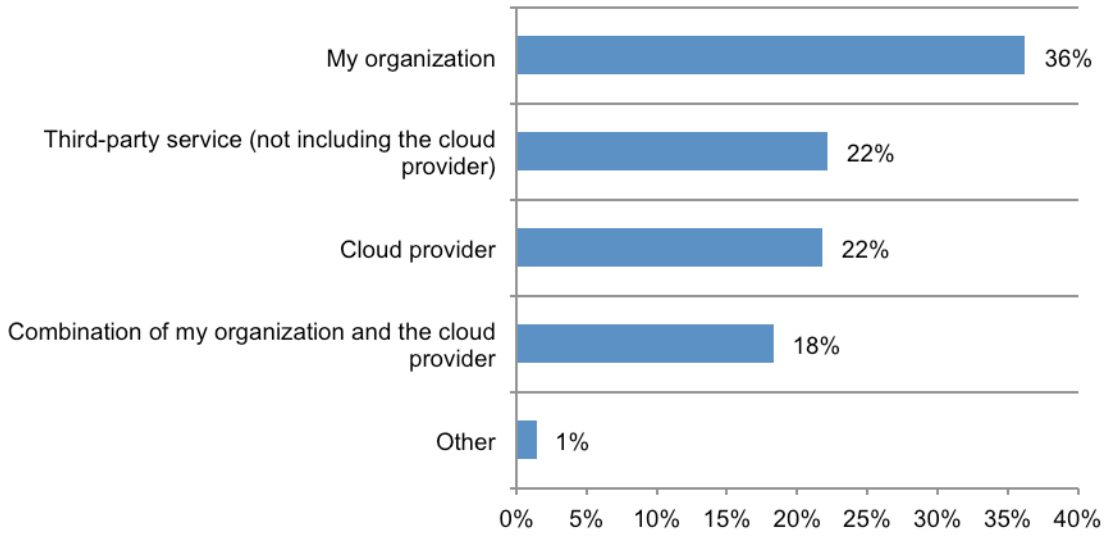
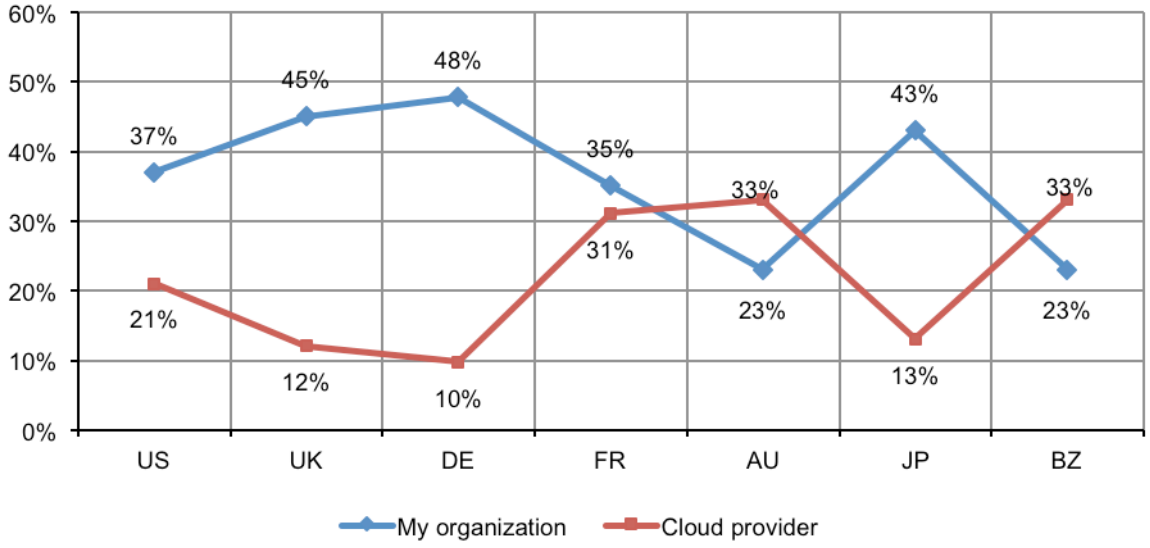


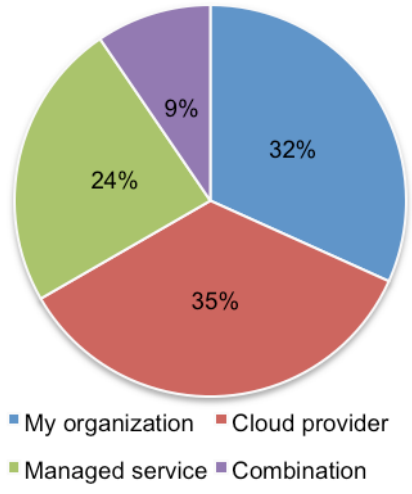
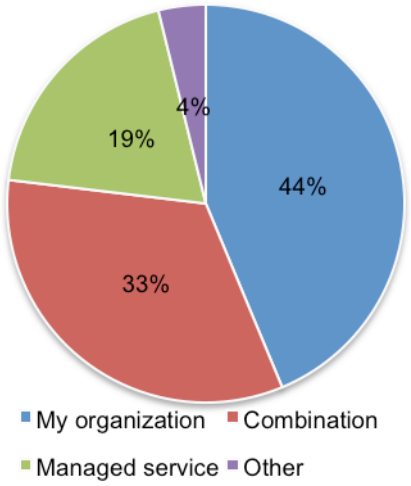
Figure 14 reports two ratings within each country for respondents selecting “my organization” or “cloud provider” as the most likely entity to manage encryption keys for data in the cloud. With the exception of Australia and Brazil, “my organization” is more likely to be selected than “cloud provider.” At 48 percent, German organizations are most likely to select “my organization.” Respondents in Australia and Brazil are most likely to select the cloud provider as the most likely entity to manage encryption keys.

Figure 14. Who manages encryption keys when data is transferred to the cloud?
My organization and cloud provider choices by country



Next we looked at how the responsibility for performing key management depends on where encryption was taking place – namely, inside the enterprise or inside the cloud environment. For companies deploying encryption inside the cloud (Figure 15b), 35 percent see the cloud provider as the most likely entity for managing encryption keys. In contrast, for companies deploying encryption inside the enterprise, 44 percent see the cloud consumer (their own organization) as the most likely entity to manage encryption keys.

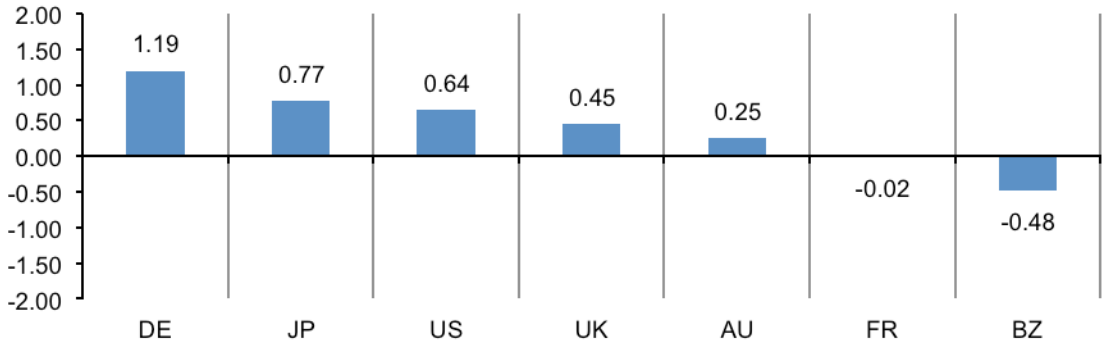
Figure 15. Who manages encryption keys when data is transferred to the cloud for two subsamples:
(1) companies that perform encryption inside the cloud and (2) companies that perform encryption inside the enterprise. Consolidated view

15a. Encryption inside the cloud	15b. Encryption inside the enterprise
	

To estimate the security posture of organizations, we used the Security Effectiveness Score or SES as part of the survey process.[3] 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.

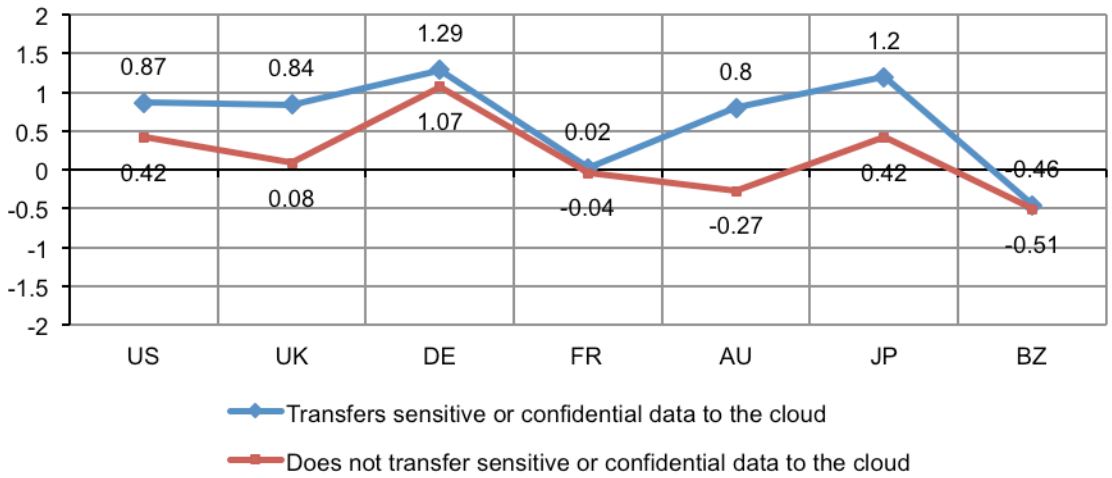
Figure 16 summarizes the average SES for each country. As shown, Germany achieves the highest score (SES = +1.19), while Brazil has the lowest score (SES = -.48)

Figure 16. Average security effectiveness score (SES) in ascending order by country



The average SES for the consolidated sample is 0.40. For those organizations that transfer sensitive or confidential data to the cloud the average SES is 0.65, and for those saying No it is 0.17. Figure 14 shows the individual results by country. The pattern suggests companies with a strong security posture (high SES) are more likely to transfer sensitive or confidential data to the cloud than those with a relatively weak security posture (low SES). This chart also shows the gap in SES scores by country, which appears to be negligible for the French and Brazilian samples.

Figure 17. Relationship between security posture (SES score) and the use of cloud services
Comparison between those responding Yes or No to the question of whether or not they transfer sensitive or confidential data to an external cloud service



[3]The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. While an important factor in the SES calculus, encryption usage is only a small part of the total computation. 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.

Part 3. Methods & Limitations

Table 1 reports the sample response for seven separate country samples. 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 sample before screening was 4,140, thus resulting in a 3.6 percent response rate. In total, the sample size used in this paper represents approximately 49 percent of respondents who say their organization uses cloud resources (n=2011).

Table 1. 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%

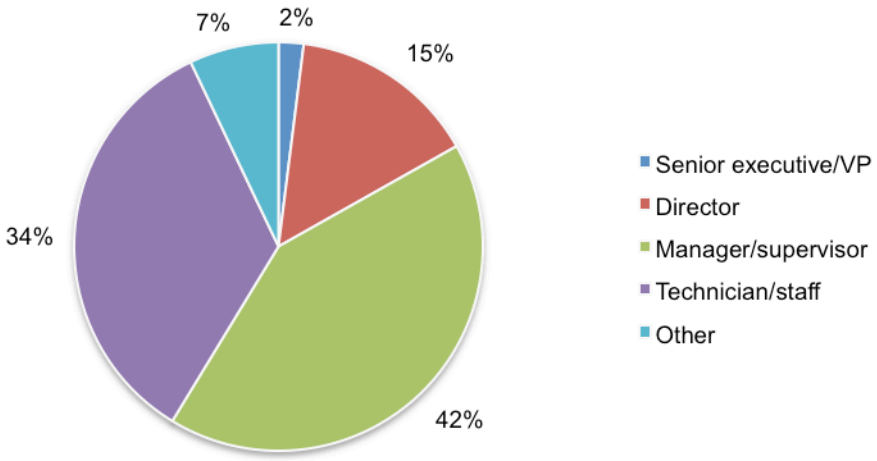
As noted in Table 2, the respondents' average (mean) experience in IT, IT security or related fields is 10.2 years. Approximately 27 percent of respondents are female and 73 percent male.[4]

Table 2. 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%

Figure 18 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.

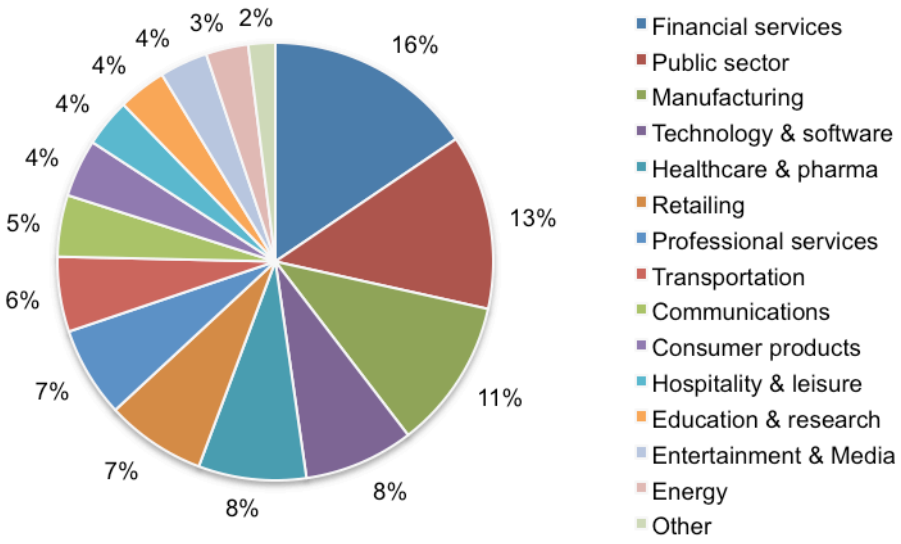
Figure 18. Distribution of respondents according to position level
Consolidated view



[4]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.

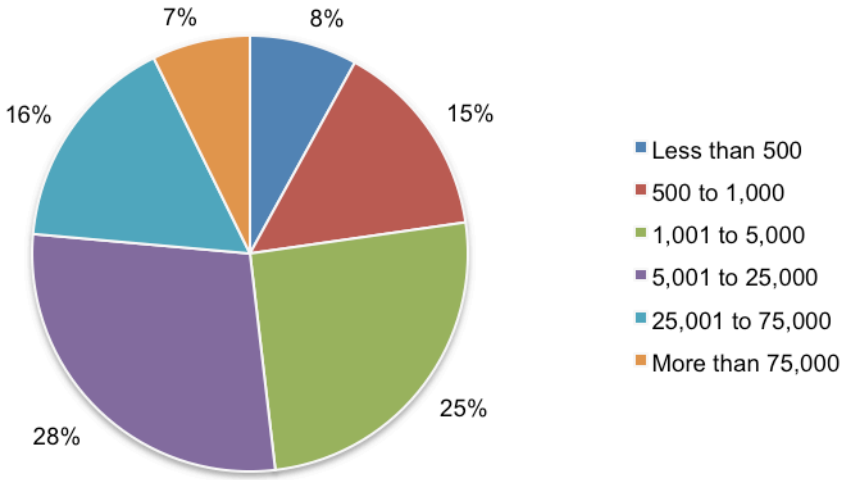
Figure 19 reports the respondents' organizations primary industry segments. As shown, 16 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 13 percent are located in public sector organizations, including central and local government.

Figure 19. Distribution of respondents according to primary industry classification
Consolidated view



According to Figure 20, the majority of respondents (52 percent) are located in larger-sized organizations with a global headcount of more than 5,000 employees.

Figure 20. Distribution of respondents according to organizational headcount
Consolidated view



Part 4. 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.

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.