Data Breach: The Cloud Multiplier Effect in European Countries

Sponsored by Netskope

Independently conducted by Ponemon Institute LLC

Publication Date: September 2014

Data Breach: The Cloud Multiplier Effect in European Countries

Ponemon Institute, September 2014

Part 1. Introduction

Data Breach: The Cloud Multiplier Effect in European Companies[1] sponsored by Netskope reveals how the risk of a data breach in the cloud is multiplying. This can be attributed to the proliferation of mobile and other devices with access to cloud resources and more dependency on cloud services without the support of a strengthened cloud security posture and visibility of end user practices.

We surveyed 1,059 IT and IT security practitioners in Europe who are familiar with their company's usage of cloud services. The majority of respondents (54 percent) say on-premise IT is equally or less secure than cloud-based services. However, 64 percent of respondents say their organisation's use of cloud resources diminishes its ability to protect confidential or sensitive information and 59 percent believe it makes it difficult to secure business-critical applications.

A lack of knowledge about the number of computing devices connected to the network and enterprise systems, software applications in the cloud and business critical applications used in the cloud workplace could be creating a cloud multiplier effect. Other uncertainties identified in this research include how much sensitive or confidential information is stored in the cloud.

Can a data breach in the cloud result in a larger and more costly incident? The cloud multiplier calculates the increase in the frequency and cost of data breach based on the growth in the use of the cloud and uncertainty as to how much sensitive data is in the cloud.

As shown in more detail in this report, we consider two types of data breach incidents to determine the cloud multiplier effect. We found that if the data breach involves the loss or theft of 100,000 or more customer records, instead of a baseline cost of €1.63 million it could be as much as €4.58 million. Data breaches involving the theft of high value information could increase from a baseline of €1.30 million to a high of €3.51 million.

For the first time, we attempt to quantify the potential scope of a data breach based on typical use of cloud services in the workplace or what can be described as the cloud multiplier effect. The report describes nine scenarios involving the loss or theft of more than 100,000 customer records and a material breach involving the loss or theft of high value[2] IP or business confidential information.

In contrast to the U.S. study,[3] respondents in European companies are more confident about their security capabilities in the cloud. When asked to rate their organisations' effectiveness in securing data and applications used in the cloud, only 25 percent of respondents say it is low. In the U.S. study, 51 percent said it was low.

Fifty-two percent of European respondents rate the effectiveness as high in contrast to 26 percent in the U.S. Despite having more confidence, 53 percent of European respondents say the likelihood of a data breach increases due to the cloud. In the U.S. study, 51 percent said the cloud increases the risk of a data breach.

---

[1] Countries represented in this research are: Austria, Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Netherlands, Poland, Russian Federation, Slovakia, Spain, Sweden, Switzerland and the United Kingdom. A separate report on Germany is also available.

[2] High value IP refers to information assets that in the wrong hands could seriously diminish the reputation and the economic viability of an enterprise. Examples include product designs, legal documents, source code, strategic plans, market analyses, formulas, financial information and much more.

[3] Data Breach: The Cloud Multiplier Effect, conducted by Ponemon Institute and sponsored by Netskope, June 2014.

Key takeaways from this research include the following:

- **Cloud security is an oxymoron for many companies**. Fifty-five percent of respondents do not agree or are unsure that cloud services are thoroughly vetted before deployment. Forty-seven percent believe there is a failure to be proactive in assessing information that is too sensitive to be stored in the cloud.

- **Certain activities increase the cost of a breach when customer data is lost or stolen.** An increase in the backup and storage of sensitive and/or confidential customer information in the cloud can cause the most costly breaches. Less costly activities occur when the organisation's use of IaaS or cloud infrastructure increases.

- **Certain activities increase the cost of a breach when high value IP and business confidential information is lost or stolen**. The increase in the use of cloud services (SaaS) and the increase in the backup and storage of sensitive and/or confidential information results in the most costly data breaches involving high value IP.

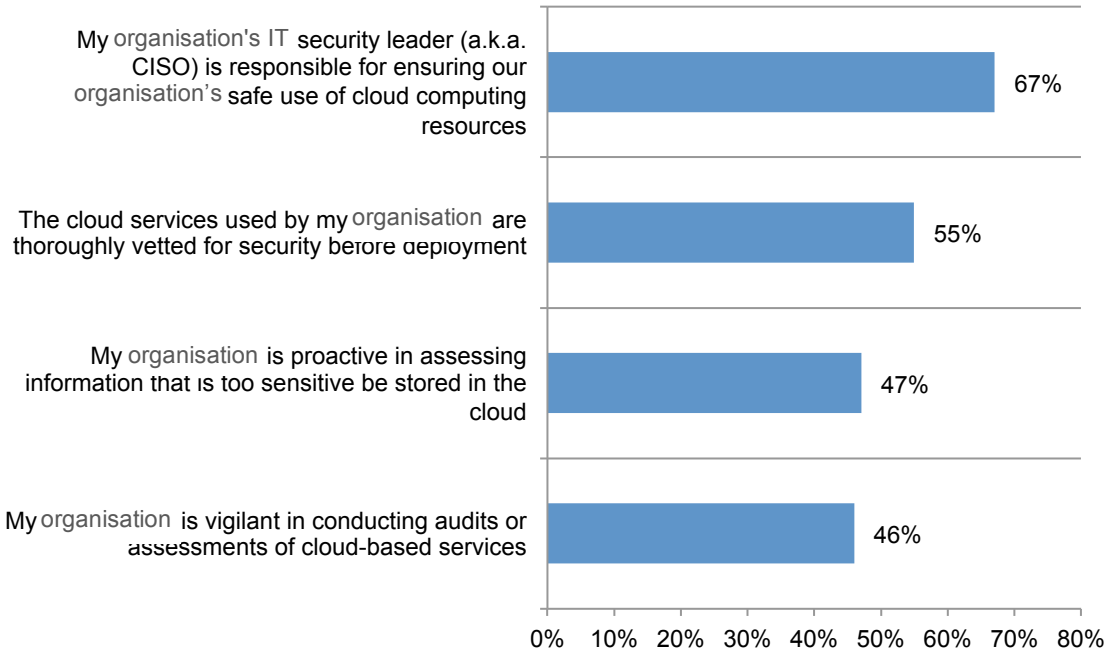
Part 2. Key Findings

Why is the likelihood of a data breach in the cloud increasing? Ideally, the right security procedures and technologies need to be in place to ensure sensitive and confidential information is protected when using cloud resources. According to Figure 1, the majority of companies are circumventing important practices such as vetting the security practices of cloud service providers and conducting audits and assessment of the information stored in the cloud.

As shown below, 55 percent of respondents do not agree or are unsure that cloud services are thoroughly vetted for security before deployment, 46 percent believe there is a lack of vigilance in conducting audits or assessments of cloud-based services and almost half (47 percent of respondents) believe there is a failure to be proactive in assessing information that is too sensitive to be stored in the cloud.

The findings also reveal that 67 percent do not believe that the IT security leader is responsible for ensuring the organisation's safe use of cloud computing resources. In other words, respondents believe their organisations are relying on functions outside security to protect data in

Figure 1. A lack of cloud confidence within the organisation
Strongly disagree, disagree and unsure response combined

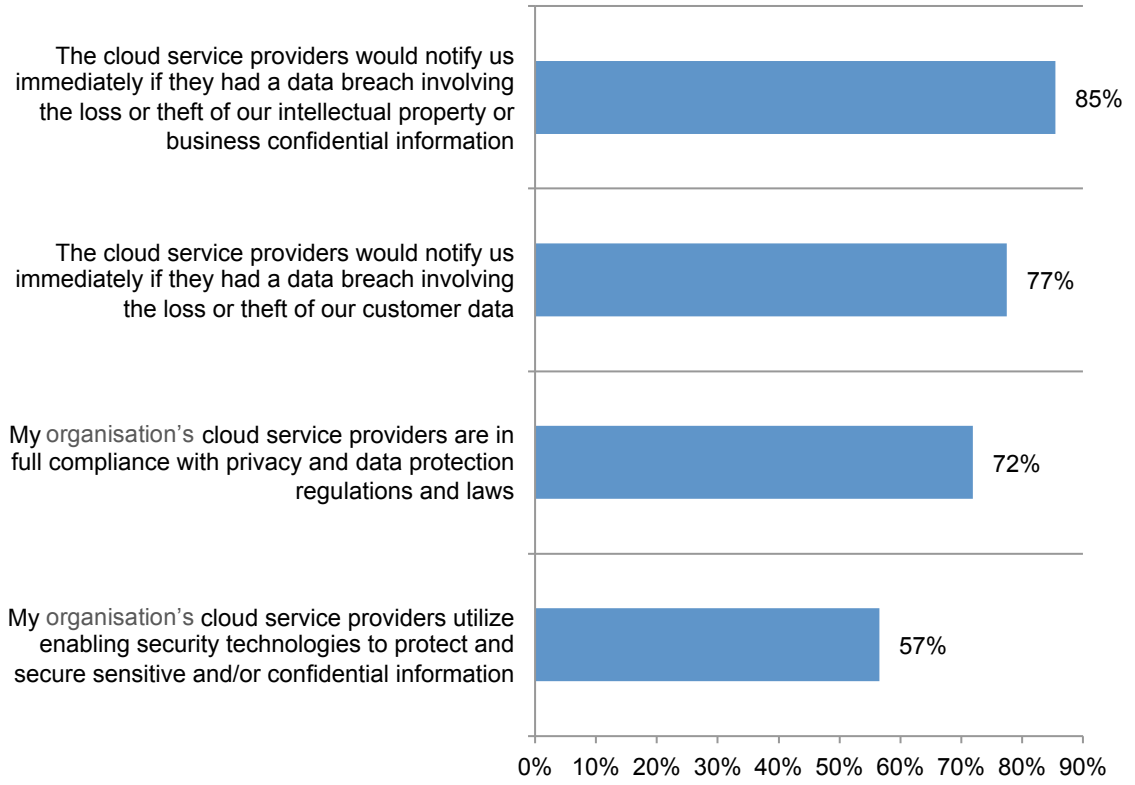


There is a lack of confidence in the security practices of cloud providers. Respondents are critical of their cloud providers' security practices. First, they do not believe they would be notified that the cloud provider lost their data in a timely manner. Second, they do not think the cloud provider has the necessary security technologies in place.

Figure 2 shows 85 percent of respondents do not agree their cloud service provider would notify them immediately if they had a data breach involving the loss or theft of their intellectual property or business confidential information. Similarly, 77 percent of respondents fear their cloud service provider would not notify their organisation immediately if they had a data breach involving the loss or theft of customer data.

Further, 57 percent of respondents do not agree that their organisation's cloud service use enabling security technologies to protect and secure sensitive and confidential information and 72 percent say these cloud service providers are not in full compliance with privacy and data protection regulations and laws.

Figure 2. Security practices of cloud service providers
Strongly disagree, disagree and unsure response combined



Lack of visibility of what's in the cloud puts confidential and sensitive information at risk. The number of computing devices in the typical workplace is making it more difficult than ever to determine the extent of cloud use. According to estimates provided by respondents, an average of 16,704 computing devices such as desktops, laptops, tablets and smartphones are connected to their organisation's networks and/or enterprise systems.

We asked respondents to estimate the percentage of their organisations' applications and information that is stored in the cloud. They were also asked to estimate the percentage of these applications and information that are not known, officially recognised or approved by the IT function (a.k.a. shadow IT). The range of responses is shown in Figure 3.

Figure 3. Software applications in the cloud
Estimated percentage of software applications

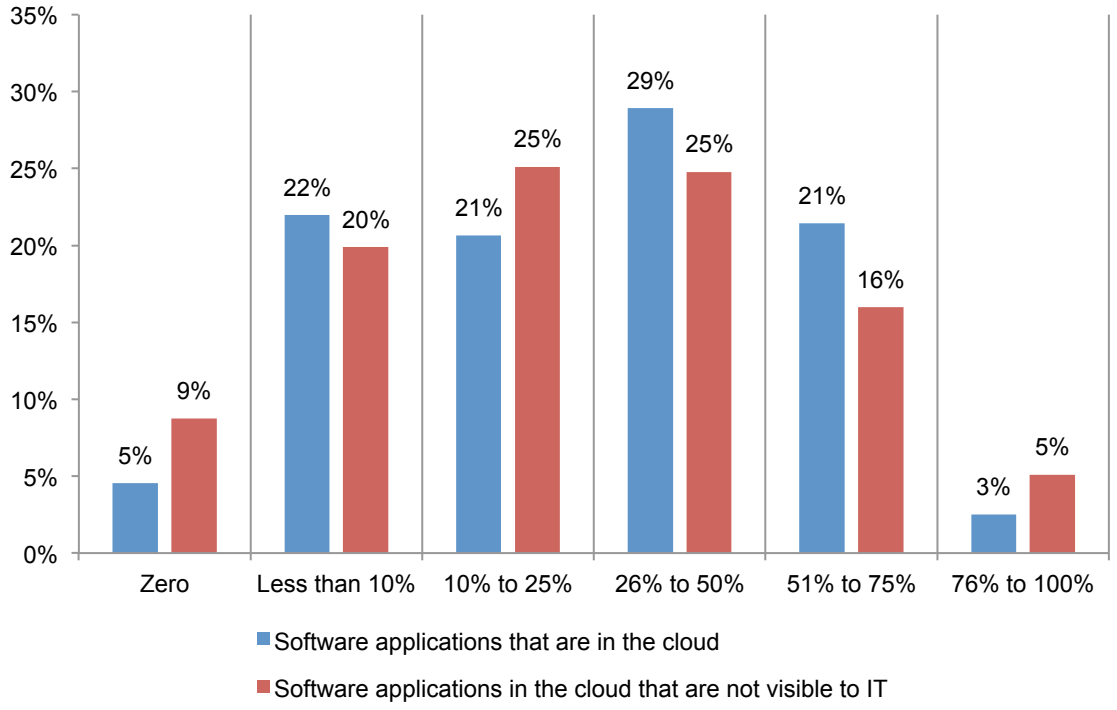
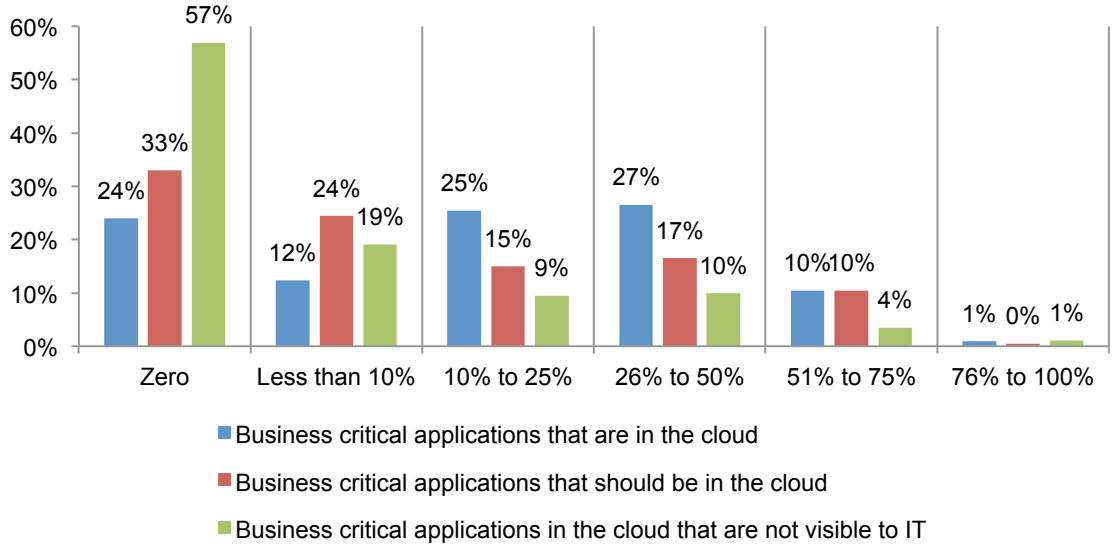


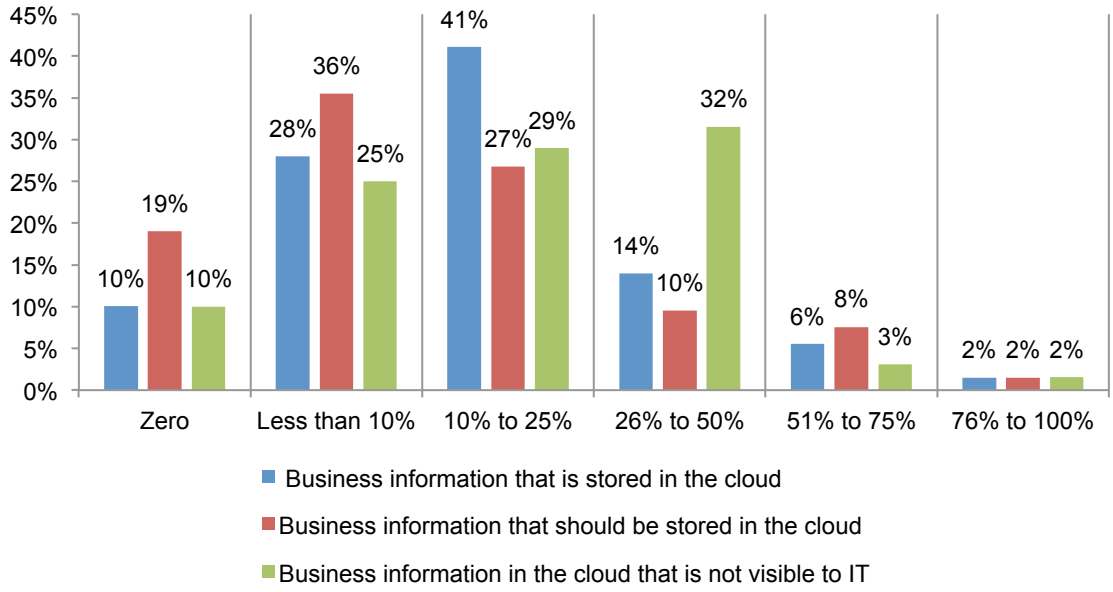
Figure 4 shows the range of business-critical applications in the cloud. On average, only 23 percent of these applications used in organisations are estimated to be in the cloud, which is evidence that the cloud is still not mature. According to respondents, only 18 percent of business critical applications should be in the cloud. Respondents estimate that 10 percent are not visible to IT.

Figure 4. Business-critical applications in the cloud
Estimated percentage of business-critical applications



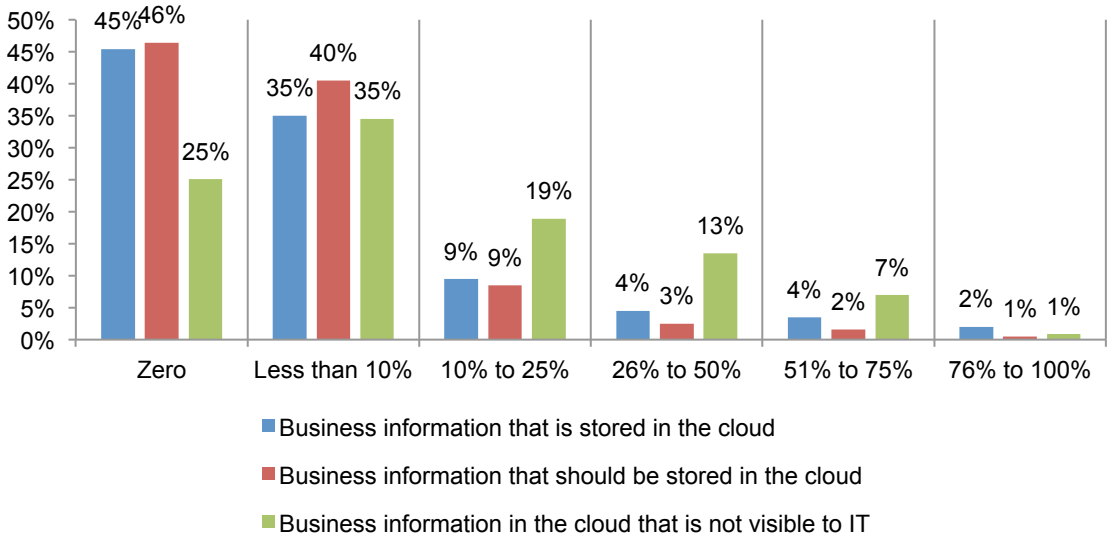
According to Figure 5, an average of 20 percent of business information is stored in the cloud but respondents believe an average of 18 percent of business information should be stored in the cloud. Respondents estimate 23 percent is not visible to IT. This suggests that many organisations are at risk because they do not know what business information is in the cloud.

Figure 5. Business information in the cloud
Estimated percentage of business information



According to Figure 6, 10 percent of sensitive or confidential business information is stored in the cloud but respondents believe an average of 8 percent of business information should be stored in the cloud. Respondents estimate 17 of sensitive or confidential information percent is not visible to IT. This suggests that many organisations are at risk because they do not know what sensitive or confidential information such as IP is in the cloud.

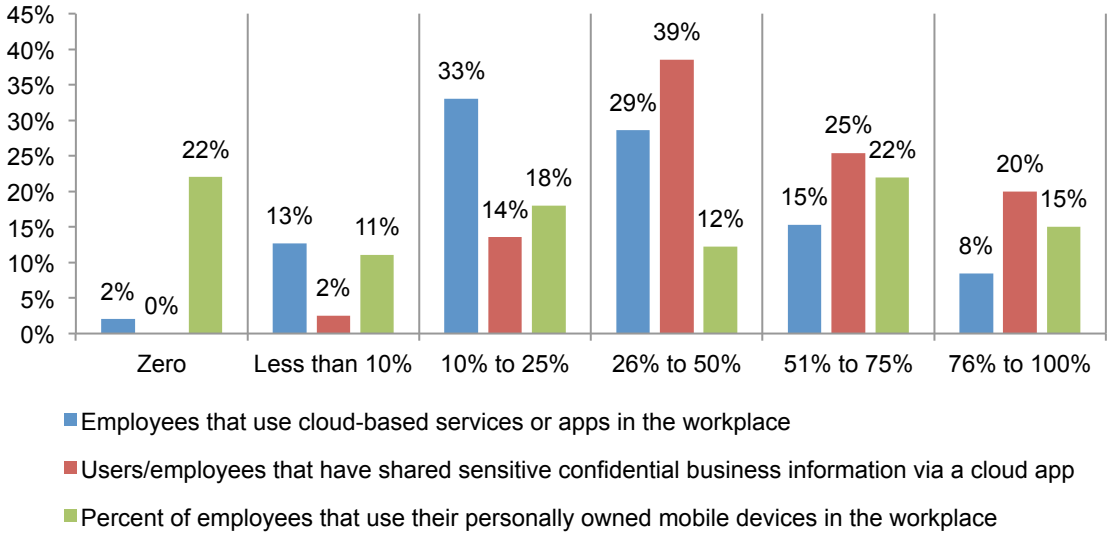
Figure 6. Sensitive or confidential business information stored in the cloud



What employees do in the cloud. On average, 35 percent of employees in organisations use cloud-based services or apps in the workplace and approximately 36 percent use their personally owned mobile devices (BYOD) in the workplace.

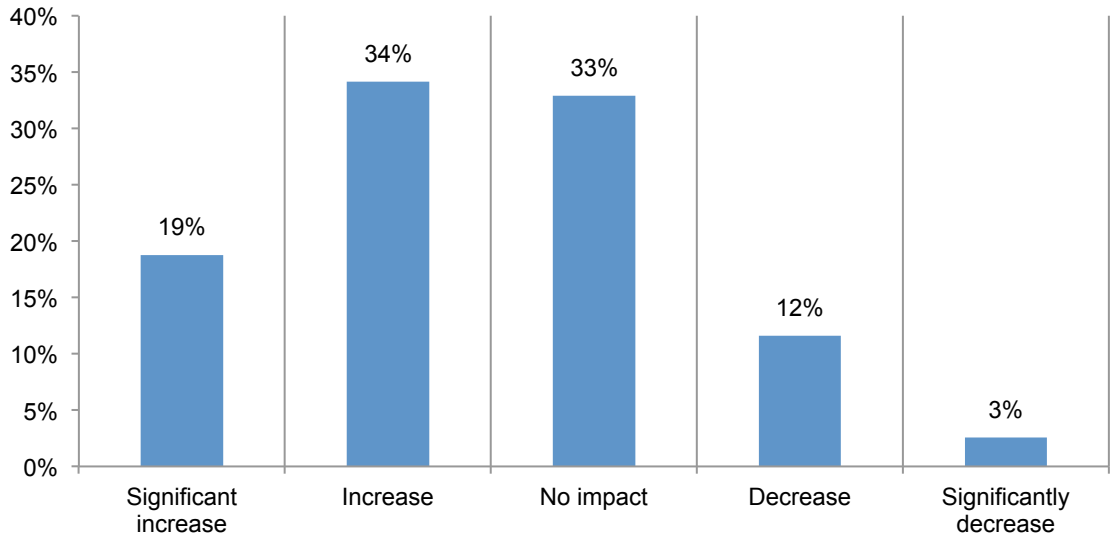
About 35 percent of these employees use their own devices to connect to cloud-based services or apps. Respondents also estimate that an average of 51 percent of employees have sent or shared sensitive, confidential business via a cloud application.

Figure 7. Employee use of cloud services
Estimated percentage of cloud services



Do certain changes in an organisation's use of cloud services affect the likelihood of a data breach? As shown in Figure 8, 19 percent say the use of cloud-based services significantly increases and 34 percent say it increases the likelihood of a data breach. In this study, we define a material data breach as one that involves the loss or theft of more than 100,000 customer records or one that involves the theft of high value IP or business confidential information.

Figure 8. Does the use of cloud-based services affect the likelihood of a data breach?



Cloud security and the multiplier effect: scenario analysis

Respondents were asked to estimate the probability of a data breach affecting both customer data and the theft of high value information assets[4] for nine typical cloud scenarios. We refer to these as nine cloud multiplier scenarios. As described in Table 1 below, each scenario has the ability to exacerbate or multiply the risk of a data breach if the use of the cloud service increases or if the cloud provider experiences a change that affects its operations.

Table 1 reports the percentage of respondents who believe each scenario increases the likelihood or probability of a data breach for their organisation. As shown, 86 percent of respondents say their organisation is most likely to experience scenario (S4), which involves an increase by 50 percent of the backup and storage of sensitive and/or confidential information in the cloud over a 12-month period. Fewer respondents (65 percent) say they are likely to have a breach if the use of cloud infrastructure services increases by 50 percent.

Table 1. Summary of nine cloud multiplier scenarios	Does this scenario increase the probability of a data breach for your organisation?
S1. The number of network-connected mobile devices with access to cloud services increases by 50 percent within your organisation over a 12-month period.	82%
S2. The use of cloud services increases by 50 percent within your organisation over a 12-month period.	77%
S3. The use of cloud infrastructure services increases by 50 percent within your organisation over a 12-month period.	65%
S4. The backup and storage of sensitive and/or confidential information in the cloud increases by 50 percent within your organisation over a 12-month period.	86%
S5. The number of employee-owned mobile devices with access to cloud services increases by 50 percent within your organisation over a 12-month period.	74%
S6. The number of employees that use their own cloud apps in the workplace for sharing sensitive or confidential data increases by 50 percent within your organisation over a 12-month period.	74%
S7. One of your organisation's primary cloud services provider moves their data centre operations from their country (domicile) to an offshore location.	81%
S8. One of your organisation's primary cloud services provider expanded operations too quickly and is now experiencing financial difficulties.	67%
S9. One of your organisation's primary cloud providers fails a compliance audit. The audit failure concerns the provider's inability to securely manage identity and authentication processes.	69%

[4]Respondents were ask to treat each scenario as an independent (non-overlapping) incident.

Calculating the economic impact of a data breach in the cloud.

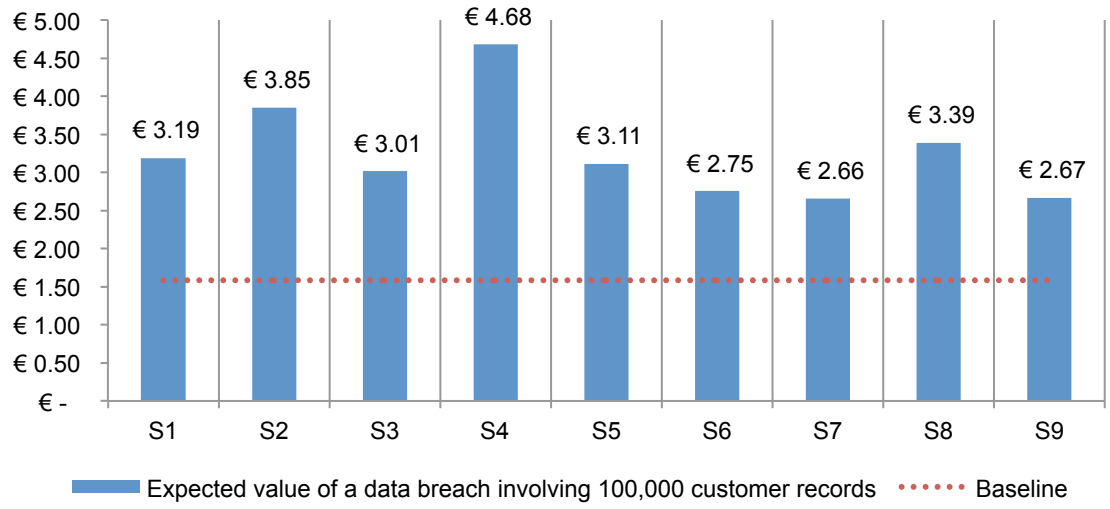
In this section, we calculate what it might cost an organisation to deal with a data breach in the cloud involving customer records. These calculations are based on Ponemon Institute's recent cost of data breach research and the estimated likelihood or probability of a data breach based on cloud use. The calculation involves the following four steps:

- First, drawing upon Ponemon Institute's most recent cost of data breach study, we compiled a pan-European[5] data breach cost estimate of of €136 per compromised record.[6]
- Second, based on a data breach size of 100,000 or more compromised records in the survey and using the unit cost of €136 times 100,000 records, we calculate a total cost of €13.6 million
- Third, from the survey results we extrapolate the average likelihood of a data breach involving 100,000 or more questions at approximately 12 percent over a two-year period.
- Fourth, multiplying the estimated likelihood or probability of a data breach at 12 percent times the total cost of €13.6 million we calculate a baseline expected value of €1.63 million as the average of what an organisation would have to spend if it had a data breach involving customer records lost or stolen in the cloud.

As discussed above, we asked respondents to consider nine different scenarios involving the increased use of cloud in their organisations or a change in the cloud provider's operations over a 12-month period. Figure 9 shows the expected value of a data breach involving 100,000 customer records for these nine scenarios**.** As can be seen, all nine scenarios are above the baseline value of €1.63 million. This means that all nine scenarios accelerate data breach costs.

What can cost an organisation the most? A 50 percent increase in the backup and storage of sensitive customer data in the cloud could cost an average of €4.58 million if this data was lost or stolen. Another expensive data breach at an average of €3.97 million could result when the use of cloud services expands quickly (i.e., by more than 50 percent).

Figure 9. Expected value of data breach costs involving the loss or theft of 100,000 or more customer records for nine scenarios. (000,000 omitted)



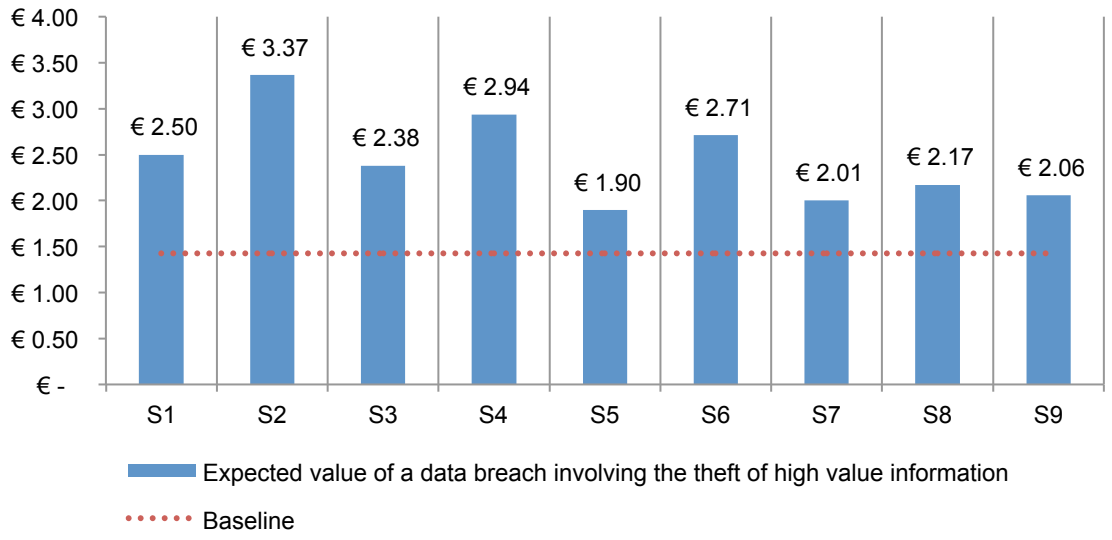
[5]The pan-European cost estimate of €136 per compromised record is based upon the weighted average data breach costs for the U.K., Italy, France and Germany.
[6]See the 2014 Cost of Data Breach Study: Germany, Ponemon Institute (sponsored by IBM), May 2014.

In this section, we calculate what it might cost an organisation to deal with a data breach in the cloud involving high value IP. Once again, these calculations are based on Ponemon Institute's recent cost of data breach research and the estimated likelihood or probability of a data breach based on cloud use. The calculation involves the following three steps:

- First, drawing upon Ponemon Institute's IT security benchmark database consisting of 1,281 companies compiled over a 10-year period, we estimate an expected value of €8.49 million.[7]
- Second, based upon the estimates provided by respondents we extrapolate the likelihood of a data breach involving the theft of high value information at 15.3 percent.
- Third, multiplying the estimated likelihood or probability of a data breach at 15.3 percent times the total cost of €8.49 million we calculate a baseline expected value of €1.30 million as the average economic impact for organisations in our study.

What can cost an organisation the most when it has a data breach involving the loss or theft of IP? Figure 10 shows that the most costly scenarios involve: (1) the growth in the number of employees using their own cloud apps in the workplace for sharing sensitive or confidential information (a.k.a. BYOC), (2) an increase in the backup and storage of IP or business confidential information in the cloud and (3) the rapid growth in the use of cloud services. The average costs to deal with these three data breach scenarios are €2.57 million, €3.15 million and €3.51 million, respectively.

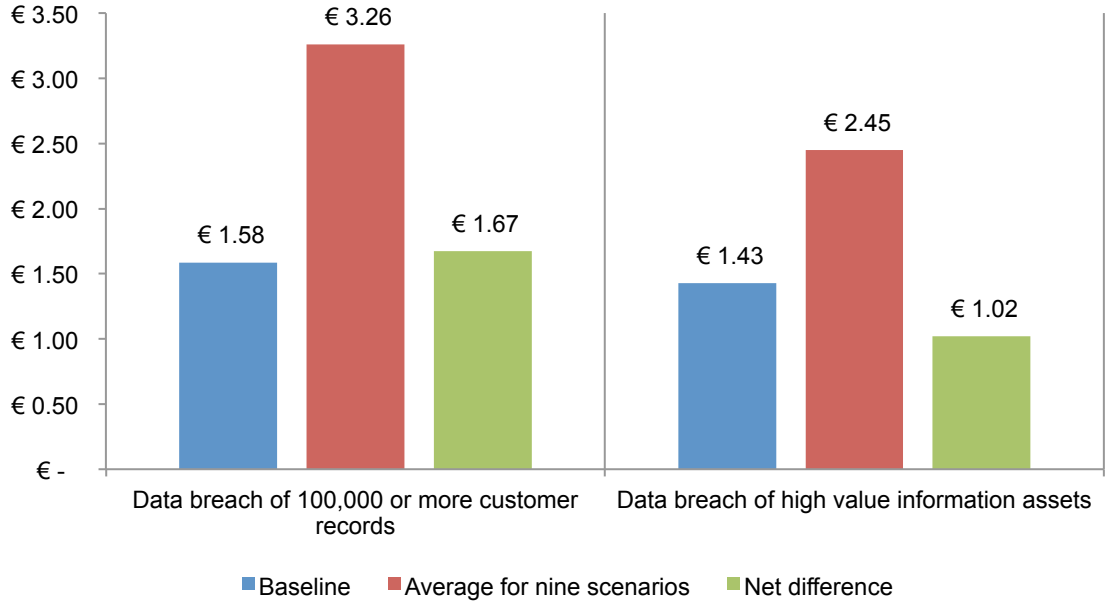
Figure 10. Expected value of data breach costs involving the theft of high value information for nine scenarios. (000,000 omitted)



[7]With the assistance of Ponemon Institute Fellows we performed a validity check to corroborate this value.

Figure 11 summarizes the total costs for two data breach incidents on average for nine scenarios. It is clear that respondents in this study recognize a multiplier effect of cloud usage within their organisation. The net difference in data breach costs involving the loss or theft of 100,000 or more customer records is €1.63 million on average. Similarly, the net difference in data breach costs involving the theft of high value information is expected to increase by €1.20 million as a result of the multiplier effect.

Figure 11. Average total cost for two types of data breach incidents
Consolidated for nine scenarios (000,000 omitted)



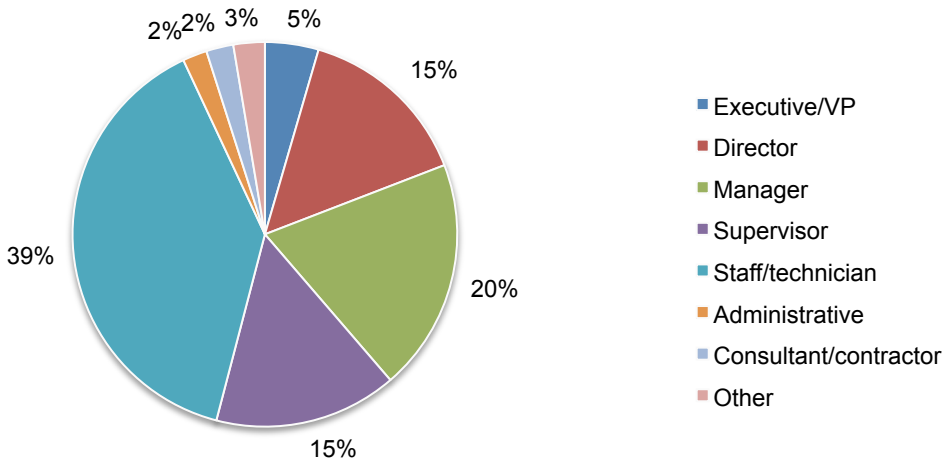
Part 4. Methods

A sampling frame of 26,900 experienced IT and IT security practitioners located in 16 European countries were selected as participants to this survey.[8] To ensure knowledgeable responses, all participants in this research are familiar with their company's cloud-based services. Table 2 shows 1,140 total returns. Screening and reliability checks required the removal of 48 surveys. Our final sample consisted of 1,059 surveys or a 3.9 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	26,900	100.0%
Total returns	1,140	4.2%
Rejected or screened surveys	81	0.3%
Final sample	1,059	3.9%

Pie Chart 1 reports the respondent's organisational level within participating organisations. By design, 55 percent of respondents are at or above the supervisory levels.

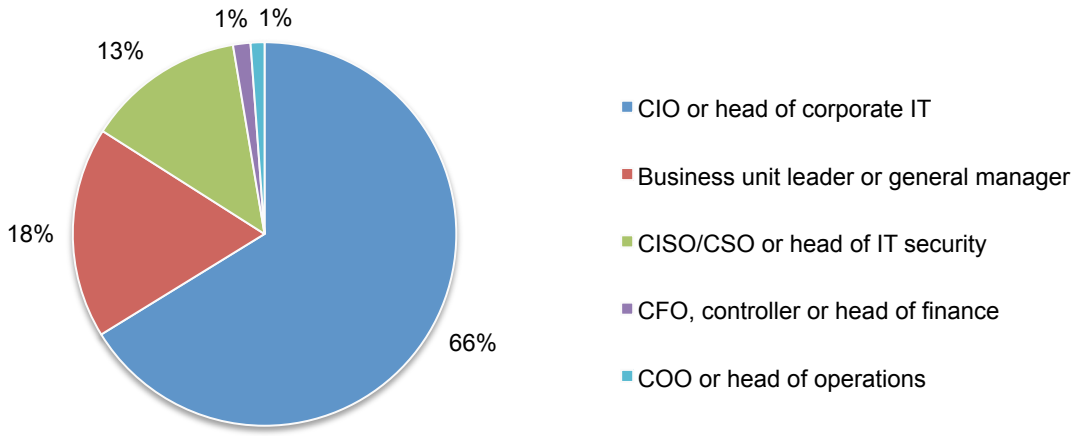
Pie Chart 1. Current position within the organisation
Sample size = 1,059



[8]The European cluster sample contains results from one dedicated German sample consisting of 514 bona fide respondents (or 49 percent of the total European sample).

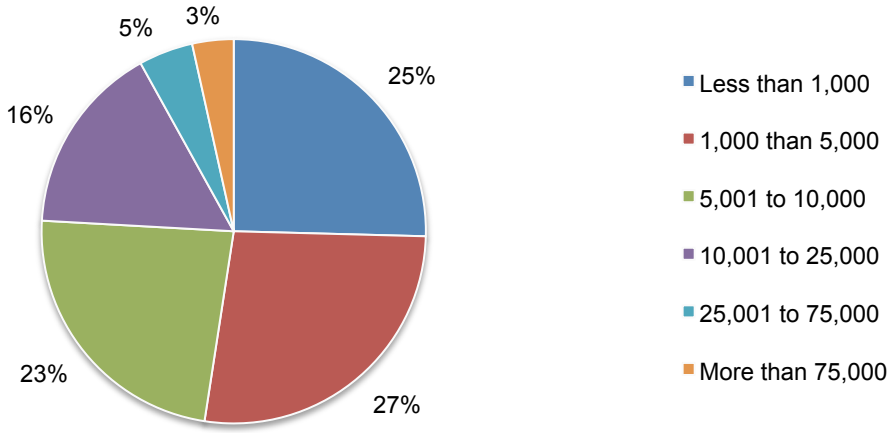
Pie Chart 2 reports that 66 percent of respondents report directly to the CIO or head of corporate IT, 18 percent report to the business unit leader or general manager and 13 percent report to the CISO/CSO or head of IT security.

Pie Chart 2. Direct reporting channel
Sample size = 1,059



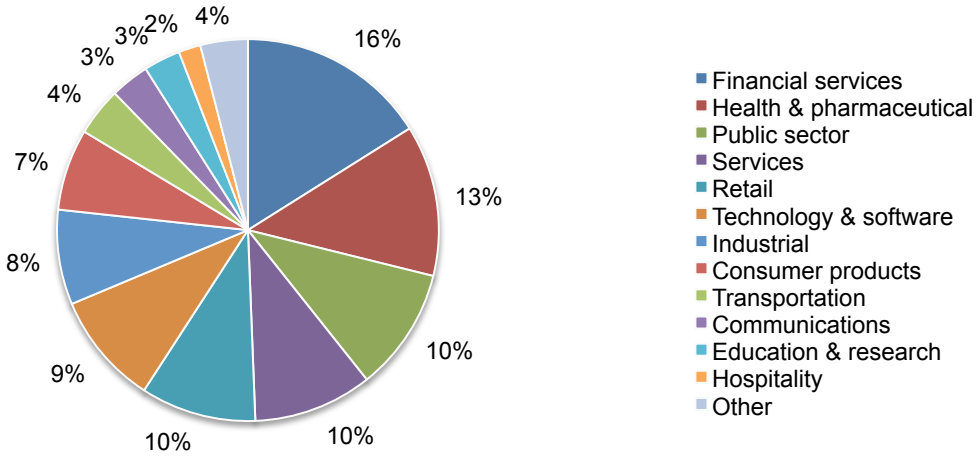
As shown in Pie Chart 3, 75 percent of respondents are from organisations with a global headcount of 1,000 or more employees.

Pie Chart 3. The full-time headcount of the global organisation
Sample size = 1,059



Pie Chart 4 reports the industry classification of respondents' organisations. This chart identifies financial services (16 percent) as the largest segment, followed by health and pharmaceuticals (13 percent), public sector (10 percent) and services (10 percent).

Pie Chart 4. Primary industry classification
Sample size = 1,059



Part 5. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, 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 instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in July 2014.

Survey response	EU Cluster
Total sampling frame	26,900
Total returns	1,140
Rejected or screened surveys	81
Final sample	1,059
Response rate	3.9%

Part 1. Screening

S1. Does your organisation use cloud-based services?	EU Cluster
Yes	100%
No (stop)	0%
Total	100%

S2. What best defines your familiarity with the cloud-based services used by your organisation today?	EU Cluster
Very familiar	33%
Familiar	47%
Somewhat familiar	20%
Not familiar or no knowledge (stop)	0%
Total	100%

Part 2. Sizing the current state

Q1. Using the 10-point scale below, please rate your organisation's level of effectiveness in securing data and applications used in the cloud.	EU Cluster
1 to 2	7%
3 to 4	18%
5 to 6	23%
7 to 8	26%
9 to 10	26%
Total	100%
Extrapolated value	6.41

Q2. What one statement best describes your opinion about the security of cloud-based services in comparison to on-premise IT security?	EU Cluster
On-premise IT is more secure than cloud-based services	43%
On-premise IT and cloud-based services are equally secure	36%
On-premise IT is less secure than cloud-based services	18%
Cannot determine	3%
Total	100%

Q3. Approximately, how many computing devices such as desktops (home and office), laptops, tablets and smart phones are connected to your organisation's networks and/or enterprise systems?	EU Cluster
Less than 1,000	9%
1,001 to 5,000	28%
5,001 to 10,000	28%
10,001 to 25,000	15%
25,001 to 50,000	11%
50,001 to 75,000	5%
75,001 to 100,000	3%
100,001 to 200,000	1%
More than 200,000	0%
Total	100%
Extrapolated value	16,704

Q4a. Approximately, what percent of all software applications used by your organisation are in the cloud?	EU Cluster
Zero	5%
Less than 10%	22%
10% to 25%	21%
26% to 50%	29%
51% to 75%	21%
76% to 100%	3%
Total	100%
Extrapolated value	32%

Q4b. Approximately, what percent of software applications in the cloud are not known, officially recognised or approved by your organisation's IT function (i.e., shadow IT)?	EU Cluster
Zero	9%
Less than 10%	20%
10% to 25%	25%
26% to 50%	25%
51% to 75%	16%
76% to 100%	5%
Total	100%
Extrapolated value	30%

Q5a. Approximately, what percent of business critical applications used by your organisation are in the cloud?	EU Cluster
Zero	24%
Less than 10%	12%
10% to 25%	25%
26% to 50%	27%
51% to 75%	10%
76% to 100%	1%
Total	100%
Extrapolated value	23%

Q5a-2. Approximately, what percent of business critical applications used by your organisation should be in the cloud?	EU Cluster
Zero	33%
Less than 10%	24%
10% to 25%	15%
26% to 50%	17%
51% to 75%	10%
76% to 100%	0%
Total	100%
Extrapolated value	18%

Q5b. Approximately, what percent of business critical applications in the cloud are not known, officially recognised or approved by your organisation's IT function (i.e., shadow IT)?	EU Cluster
Zero	57%
Less than 10%	19%
10% to 25%	9%
26% to 50%	10%
51% to 75%	4%
76% to 100%	1%
Total	100%
Extrapolated value	10%

Q6a. Approximately, what percent of business information used by your organisation is stored in the cloud?	EU Cluster
Zero	10%
Less than 10%	28%
10% to 25%	41%
26% to 50%	14%
51% to 75%	6%
76% to 100%	2%
Total	100%
Extrapolated value	20%

Q6a-2. Approximately, what percent of business information used by your organisation should be stored in the cloud?	EU Cluster
Zero	19%
Less than 10%	36%
10% to 25%	27%
26% to 50%	10%
51% to 75%	8%
76% to 100%	2%
Total	100%
Extrapolated value	18%

Q6b. Approximately, what percent of business information in the cloud is not known, officially recognised or approved by your organisation's IT function (i.e., shadow IT)?	EU Cluster
Zero	10%
Less than 10%	25%
10% to 25%	29%
26% to 50%	32%
51% to 75%	3%
76% to 100%	2%
Total	100%
Extrapolated value	23%

Q7a. Approximately, what percent of sensitive or confidential business information used by your organisation is stored in the cloud?	EU Cluster
Zero	45%
Less than 10%	35%
10% to 25%	9%
26% to 50%	4%
51% to 75%	4%
76% to 100%	2%
Total	100%
Extrapolated value	10%

Q7a-2. Approximately, what percent of sensitive or confidential business information used by your organisation should be stored in the cloud?	EU Cluster
Zero	46%
Less than 10%	40%
10% to 25%	9%
26% to 50%	3%
51% to 75%	2%
76% to 100%	1%
Total	100%
Extrapolated value	8%

Q7b. Approximately, what percent of sensitive or confidential business information in the cloud is not known, officially recognised or approved by your organisation's IT function (i.e., shadow IT)?	EU Cluster
Zero	25%
Less than 10%	35%
10% to 25%	19%
26% to 50%	13%
51% to 75%	7%
76% to 100%	1%
Total	100%
Extrapolated value	17%

Q8. Approximately, what percent of employees in your organisation use cloud-based services or apps in the workplace?	EU Cluster
Zero	2%
Less than 10%	13%
10% to 25%	33%
26% to 50%	29%
51% to 75%	15%
76% to 100%	8%
Total	100%
Extrapolated value	35%

8b. Approximately, what percent of users/employees in your organisation have sent or shared sensitive confidential business information via a cloud app?	EU Cluster
Zero	0%
Less than 10%	2%
10% to 25%	14%
26% to 50%	39%
51% to 75%	25%
76% to 100%	20%
Total	100%
Extrapolated value	51%

Q9. Approximately, what percent of employees use their personally owned mobile devices (a.k.a. BYOD) in the workplace?	EU Cluster
Zero	22%
Less than 10%	11%
10% to 25%	18%
26% to 50%	12%
51% to 75%	22%
76% to 100%	15%
Total	100%
Extrapolated value	36%

Q10. Approximately, what percent of employees who use their personally owned mobile devices connect to cloud-based services or apps (a.k.a. BYOC) in the workplace?	EU Cluster
Zero	7%
Less than 10%	20%
10% to 25%	26%
26% to 50%	18%
51% to 75%	17%
76% to 100%	13%
Total	100%
Extrapolated value	35%

Part 3. The fragile cloud ecosystem

Q11. In your opinion, does the use of cloud-based services affect the likelihood of a data breach?	EU Cluster
Significant increase	19%
Increase	34%
No impact	33%
Decrease	12%
Significantly decrease	3%
Total	100%

Data breach type 1: A material data breach involving the loss or theft of more than 100,000 customer records.	
Q12. In your opinion, what is the likelihood that your company will experience one or more data breach incidents of this type sometime over the next 24 months?	EU Cluster
1% to 10%	72%
11% to 30%	20%
31% to 50%	5%
51% to 70%	2%
71% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	12%

Data breach type 2: A material data breach involving the theft of high value IP or business confidential information.	
Q13. In your opinion, what is the likelihood that your company will experience one or more data breach incidents of this type sometime over the next 24 months?	EU Cluster
1% to 10%	63%
11% to 30%	19%
31% to 50%	10%
51% to 70%	6%
71% to 90%	2%
91% to 100%	0%
Total	100%
	17%

Scenario 1. The number of network-connected mobile devices with access to cloud services increases by 50 percent within your organisation over a 12-month period.	
Q14a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	82%
No	13%
Cannot determine	4%
Total	100%

Q14b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	50%
11% to 30%	19%
31% to 50%	15%
51% to 70%	8%
71% to 90%	7%
91% to 100%	1%
Total	100%
Extrapolated value	23%

Q14c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	38%
11% to 30%	22%
31% to 50%	14%
51% to 70%	16%
71% to 90%	7%
91% to 100%	3%
Total	100%
Extrapolated value	29%

Scenario 2. The use of cloud services (SaaS) increases by 50 percent within your organisation over a 12-month period.	
Q15a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	77%
No	22%
Cannot determine	1%
Total	100%

Q15b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	34%
11% to 30%	25%
31% to 50%	20%
51% to 70%	16%
71% to 90%	4%
91% to 100%	1%
Total	100%
Extrapolated value	28%

Q15c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	26%
11% to 30%	20%
31% to 50%	18%
51% to 70%	13%
71% to 90%	16%
91% to 100%	7%
Total	100%
Extrapolated value	40%

Scenario 3. The use of cloud infrastructure services (IaaS) increases by 50 percent within your organisation over a 12-month period.	
Q16a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	64%
No	27%
Cannot determine	9%
Total	100%

Q16b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	41%
11% to 30%	29%
31% to 50%	20%
51% to 70%	8%
71% to 90%	2%
91% to 100%	0%
Total	100%
Extrapolated value	22%

Q16c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	35%
11% to 30%	24%
31% to 50%	20%
51% to 70%	18%
71% to 90%	3%
91% to 100%	1%
Total	100%
Extrapolated value	28%

Scenario 4. The backup and storage of sensitive and/or confidential information in the cloud increases by 50 percent within your organisation over a 12-month period.	
Q17a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	86%
No	10%
Cannot determine	3%
Total	100%

Q17b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	22%
11% to 30%	27%
31% to 50%	24%
51% to 70%	18%
71% to 90%	8%
91% to 100%	1%
Total	100%
Extrapolated value	34%

Q17c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	26%
11% to 30%	21%
31% to 50%	23%
51% to 70%	22%
71% to 90%	5%
91% to 100%	3%
Total	100%
Extrapolated value	35%

Scenario 5. The number of employee-owned mobile devices (a.k.a. BYOD) with access to cloud services increases by 50 percent within your organisation over a 12-month period.	
Q18a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	81%
No	13%
Cannot determine	6%
Total	100%

Q18b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	43%
11% to 30%	26%
31% to 50%	16%
51% to 70%	14%
71% to 90%	2%
91% to 100%	0%
Total	100%
Extrapolated value	23%

Q18c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	37%
11% to 30%	34%
31% to 50%	17%
51% to 70%	11%
71% to 90%	0%
91% to 100%	0%
Total	100%
Extrapolated value	22%

Scenario 6. The number of employees that use their own cloud apps in the workplace for sharing sensitive or confidential data (a.k.a. BYOC) increases by 50 percent within your organisation over a 12-month period.	
Q19a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	74%
No	22%
Cannot determine	4%
Total	100%

Q19b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	48%
11% to 30%	29%
31% to 50%	13%
51% to 70%	8%
71% to 90%	3%
91% to 100%	0%
Total	100%
Extrapolated value	20%

Q19c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	20%
11% to 30%	33%
31% to 50%	25%
51% to 70%	19%
71% to 90%	2%
91% to 100%	1%
Total	100%
Extrapolated value	32%

Scenario 7. One of your organisation's primary cloud services provider moves their data centre operations from your country (domicile) to an offshore location.	
Q20a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	81%
No	12%
Cannot determine	7%
Total	100%

Q20b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	46%
11% to 30%	28%
31% to 50%	22%
51% to 70%	4%
71% to 90%	0%
91% to 100%	0%
Total	101%
Extrapolated value	20%

Q20c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	33%
11% to 30%	34%
31% to 50%	26%
51% to 70%	6%
71% to 90%	1%
91% to 100%	1%
Total	100%
Extrapolated value	24%

Scenario 8. One of your organisation's primary cloud services provider expanded operations too quickly and is now experiencing financial difficulties.	
Q21a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	67%
No	28%
Cannot determine	4%
Total	100%

Q21b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	39%
11% to 30%	23%
31% to 50%	23%
51% to 70%	14%
71% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	25%

Q21c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	31%
11% to 30%	32%
31% to 50%	25%
51% to 70%	9%
71% to 90%	3%
91% to 100%	0%
Total	100%
Extrapolated value	26%

Scenario 9. One of your organisation's primary cloud providers fails a compliance audit conducted by a bona fide security expert. The audit failure concerns the provider's inability to securely manage identity and authentication processes.	
Q22a. In your opinion, would this scenario increase the probability of a data breach for your organisation?	EU Cluster
Yes	69%
No	29%
Cannot determine	2%
Total	100%

Q22b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	EU Cluster
1% to 10%	40%
11% to 30%	39%
31% to 50%	13%
51% to 70%	5%
71% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	20%

Q22c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	EU Cluster
1% to 10%	34%
11% to 30%	30%
31% to 50%	27%
51% to 70%	9%
71% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	24%

Part 4. Attributions used for cloud confidence index (11 items)	EU Cluster
Q25a. My organisation's use of cloud resources does not diminish its ability to protect confidential or sensitive information.	36%
Q25b. My organisation's use of cloud resources does not diminish its ability to secure business-critical applications.	41%
Q25c. The cloud services used by my organisation are thoroughly vetted for security before deployment.	45%
Q25d. My organisation is vigilant in conducting audits or assessments of cloud-based services.	54%
Q25e. My organisation is proactive in assessing information that is too sensitive be stored in the cloud.	53%
Q25f. My organisation's IT security leader (a.k.a. CISO) is responsible for ensuring our organisation's safe use of cloud computing resources.	33%
Q25g. The cloud service providers used by my organisation would notify us immediately if they had a data breach involving the loss or theft of our customer data.	23%
Q25h. The cloud service providers used by my organisation would notify us immediately if they had a data breach involving the loss or theft of our intellectual property or business confidential information.	15%
Q25i. My organisation's cloud service providers utilise enabling security technologies to protect and secure sensitive and/or confidential information.	43%
Q25j. My organisation's cloud service providers are in full compliance with privacy and data protection regulations and laws.	28%
Q25k. My organisation's cloud service providers are financially stable (i.e., good financial health).	45%

Part 5. Organisation and respondents' demographics

D1. What best describes your position level within the organisation?	EU Cluster
Executive/VP	5%
Director	15%
Manager	20%
Supervisor	15%
Staff/technician	39%
Administrative	2%
Consultant/contractor	2%
Other	3%
Total	100%

D2. What best describes your direct reporting channel?	EU Cluster
CEO/executive committee	0%
COO or head of operations	1%
CFO, controller or head of finance	1%
CIO or head of corporate IT	66%
Business unit leader or general manager	18%
Head of compliance or internal audit	0%
CISO/CSO or head of IT security	13%
Other	0%
Total	100%

D3. What range best describes the full-time headcount of your global organisation?	EU Cluster
Less than 1,000	25%
1,000 than 5,000	27%
5,001 to 10,000	23%
10,001 to 25,000	16%
25,001 to 75,000	5%
More than 75,000	3%
Total	100%
Extrapolated value	10784

D4. What best describes your organisation's primary industry classification?	EU Cluster
Agriculture & food services	1%
Communications	3%
Consumer products	7%
Defence & aerospace	1%
Education & research	3%
Energy & utilities	1%
Entertainment & media	1%
Financial services	16%
Health & pharmaceutical	13%
Hospitality	2%
Industrial	8%
Public sector	10%
Retail	10%
Services	10%
Technology & software	9%
Transportation	4%
Other	0%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

As a member of the **Council of American Survey Research Organisations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.