Data Breach: The Cloud Multiplier Effect

Sponsored by Netskope

Independently conducted by Ponemon Institute LLC

Publication Date: June 2014

Data Breach: The Cloud Multiplier Effect

Ponemon Institute, June 2014

Part 1. Introduction

Data Breach: The Cloud Multiplier Effect 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 613 IT and IT security practitioners in the United States who are familiar with their company's usage of cloud services. The majority of respondents (51 percent) say on-premise IT is equally or less secure than cloud-based services. However, 66 percent of respondents say their organization's use of cloud resources diminishes its ability to protect confidential or sensitive information and 64 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 an average cost of $2.37 million it could be as much as $5.32 million. Data breaches involving the theft of high value information could increase from $2.99 million to $4.16 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[1] IP or business confidential information.

When asked to rate their organizations' effectiveness in securing data and applications used in the cloud, the majority (51 percent) of respondents say it is low. Only 26 percent rate the effectiveness as high. Based on their lack of confidence, 51 percent say the likelihood of a data breach increases due to the cloud.

Key takeaways from this research include the following:

- **Cloud security is an oxymoron for many companies**. Sixty-two percent of respondents do not agree or are unsure that cloud services are thoroughly vetted before deployment. Sixty-nine 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. The second most costly occurs when one of the organization's primary cloud services provider expands operations too quickly and

[1]High value IP refers to information assets that in the wrong hands could seriously diminish the reputation

experiences financial difficulties. The least costly is when the use of IaaS or cloud infrastructure services increases.

- **Certain activities increase the cost of a breach when high value IP and business confidential information is lost or stolen**. Bring Your Own Cloud (BYOC) results in the most costly data breaches involving high value IP. The second most costly is the backup and storage of sensitive or confidential information in the cloud increases. The least costly occurs when one of the organization's primary cloud providers fails an audit failure that concerns the its inability to securely manage identity and authentication processes.

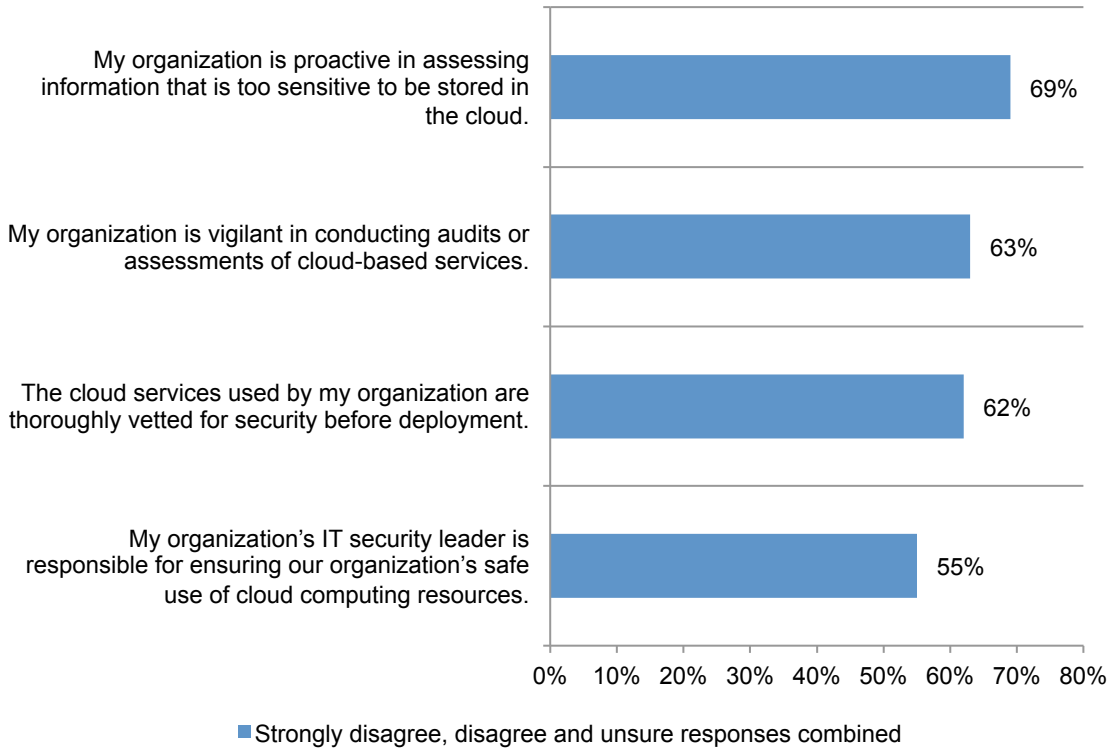
Part 2. Key Findings

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.

The findings also reveal that 55 percent do not believe that the IT security leader is responsible for ensuring the organization's safe use of cloud computing resources. In other words, respondents believe their organizations are relying on functions outside security to protect data in the cloud.

As shown below, 62 percent of respondents do not agree or are unsure that cloud services are thoroughly vetted for security before deployment, 63 percent believe there is a lack of vigilance in conducting audits or assessments of cloud-based services and the highest percentage (69 percent of respondents) believe there is a failure to be proactive in assessing information that is too sensitive to be stored in the cloud.

Figure 1. A lack of cloud confidence within the organization

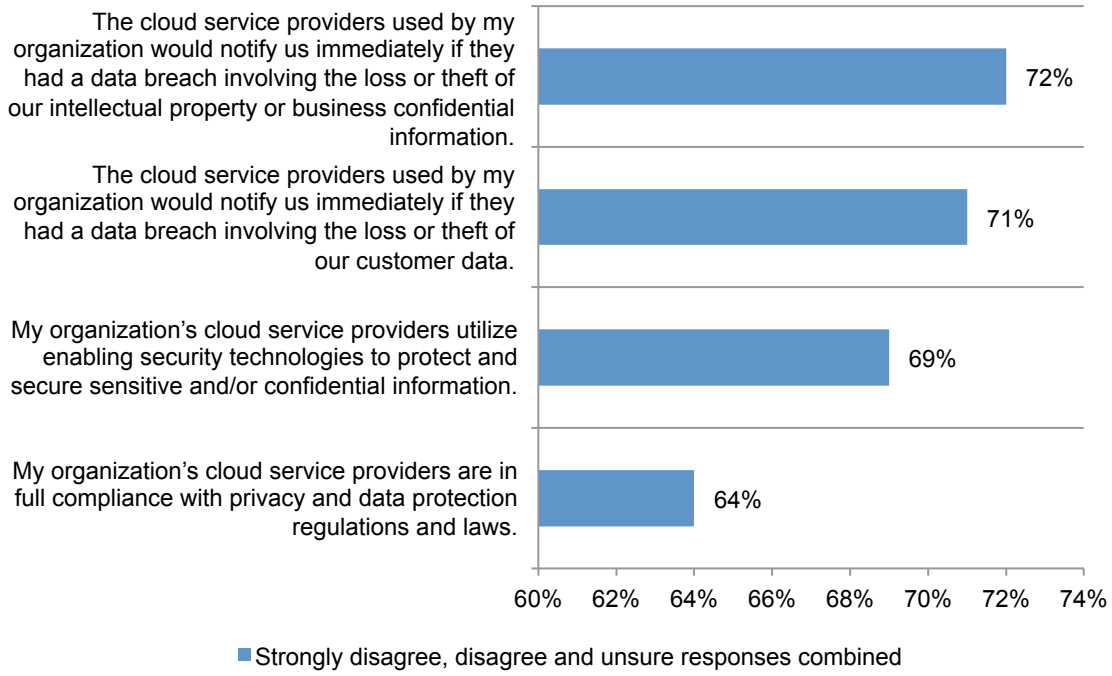


There is a lack of confidence in the security practices of cloud providers. Respondents are critical of their cloud providers' security practices. First, they do not believe they would be notified that the cloud provider lost their data in a timely manner. Second, they do not think the cloud provider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

Figure 2 shows 72 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, 71 percent of respondents fear their cloud service provider would not notify their organization immediately if they had a data breach involving the loss or theft of customer data.

Further, 69 percent of respondents do not agree that their organization's cloud service use enabling security technologies to protect and secure sensitive and confidential information and 64 percent say these cloud service providers are not in full compliance with privacy and data protection regulations and laws.

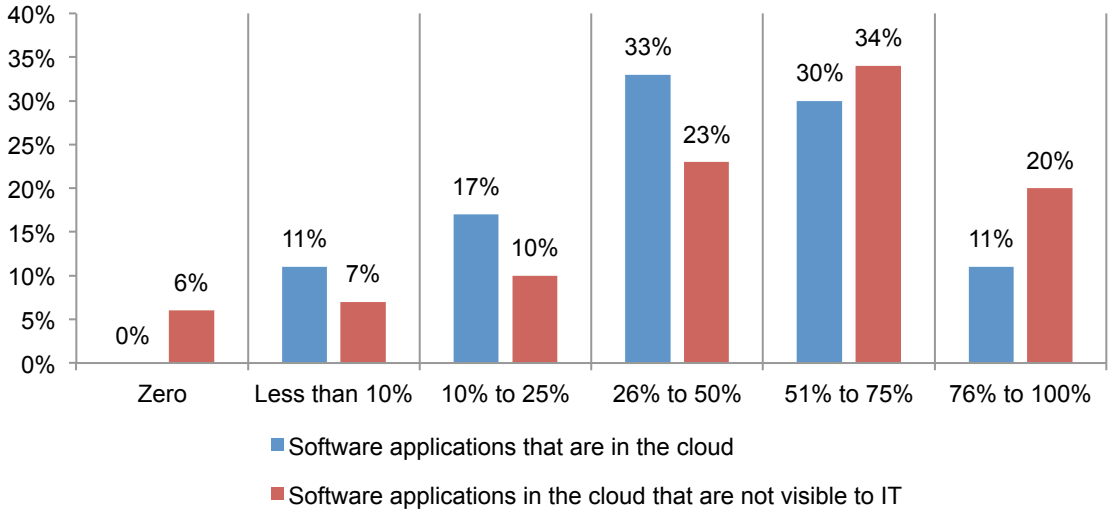
Figure 2. Security practices of cloud service providers



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 25,180 computing devices such as desktops, laptops, tablets and smartphones are connected to their organization's networks and/or enterprise systems.

We asked respondents to estimate the percentage of their organizations' 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 recognized 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



According to our present sample of respondents, 45 percent of all software applications used by organizations are in the cloud but exactly half of these applications (or 22.5 percent of the total) are **not visible** to IT. These data points are summarized in Figure 4.

Figure 4. Respondents' awareness about cloud applications in use today

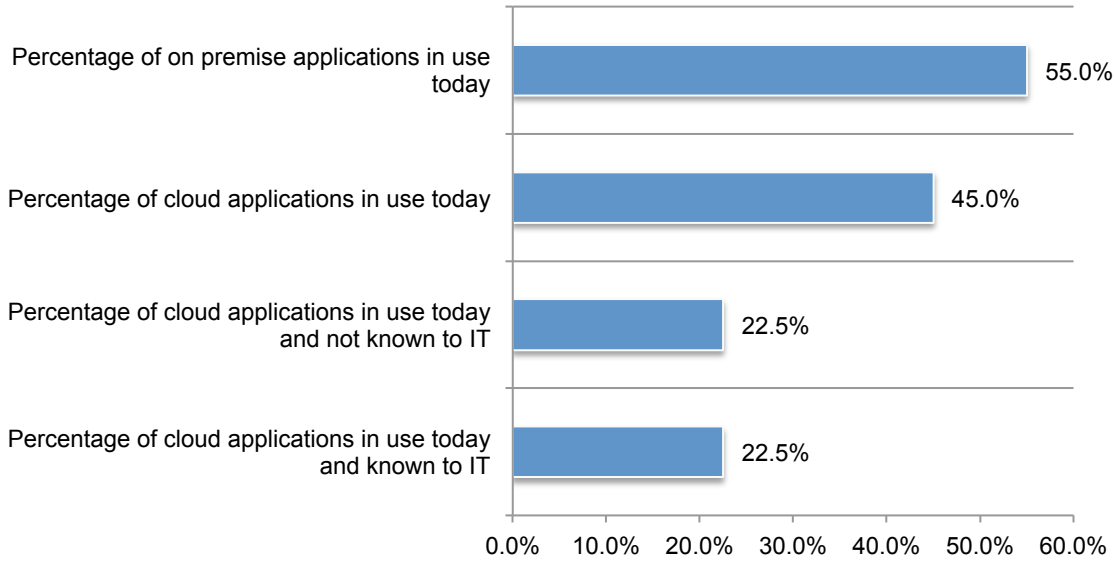
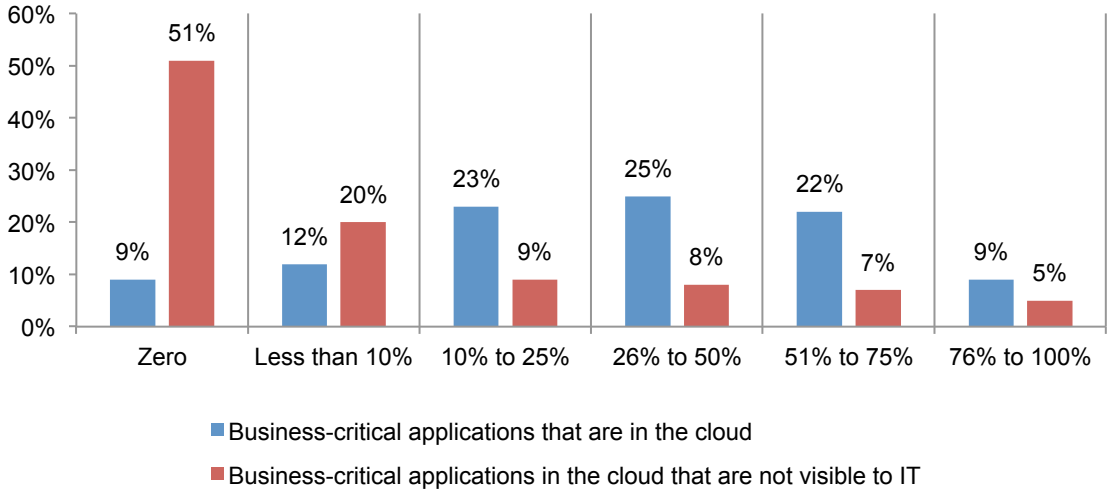


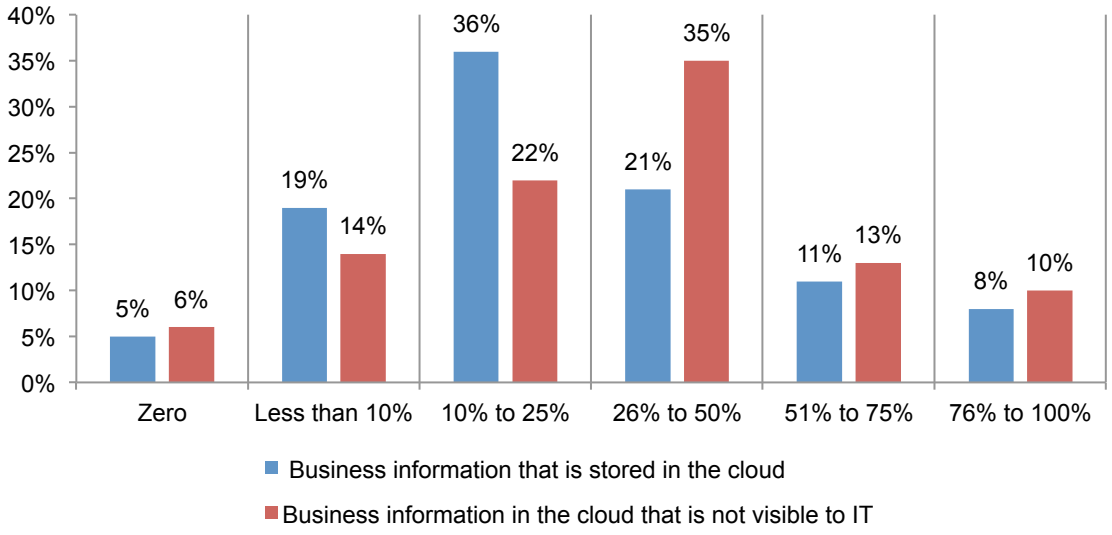
Figure 5 shows the range of business-critical applications in the cloud. On average, 36 percent of these applications used in organizations are estimated to be in the cloud, which is evidence that the cloud is maturing. However, respondents estimate that 15 percent are not visible to IT.

Figure 5. Business-critical applications in the cloud
Estimated percentage of business-critical applications



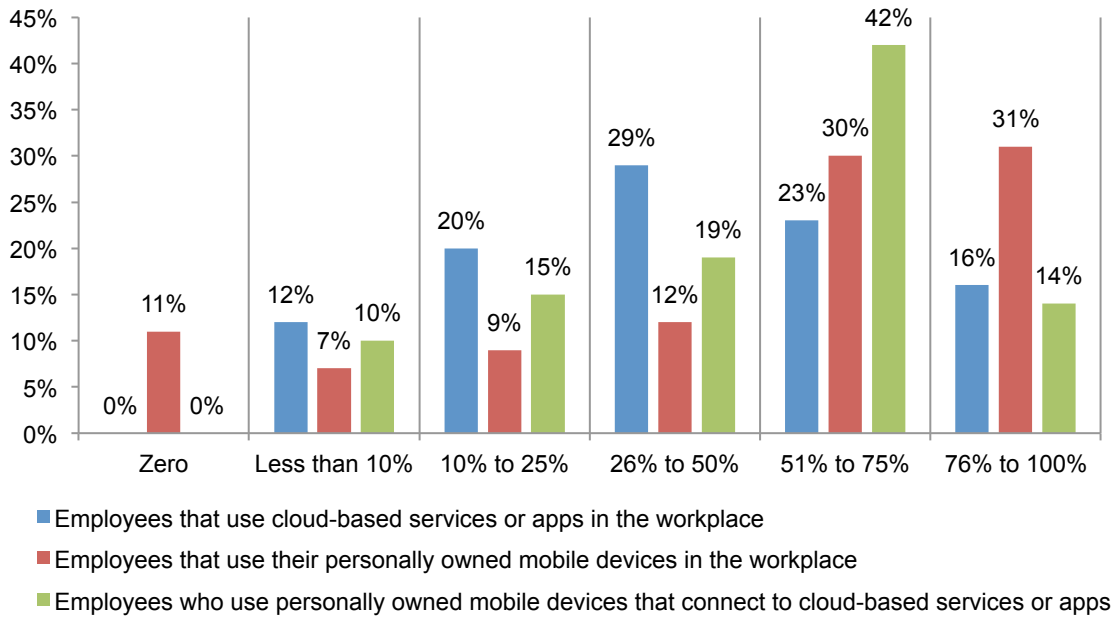
According to Figure 6, 30 percent of business information is stored in the cloud but of this, respondents estimate 35 percent is not visible to IT. This suggests that many organizations are at risk because they do not know what sensitive or confidential information such as IP is in the cloud.

Figure 6. Business information in the cloud
Estimated percentage of business information



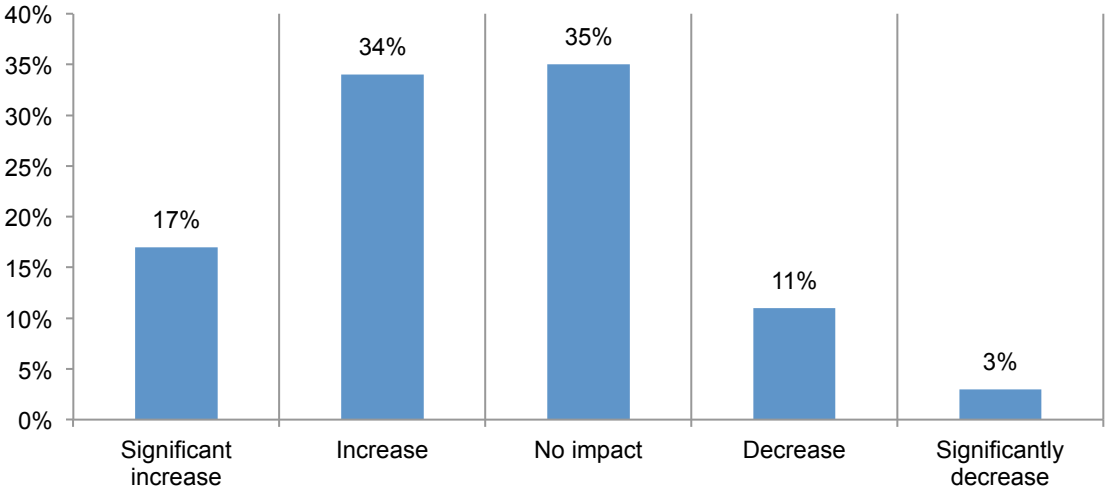
What employees do in the cloud. On average, 44 percent of employees in organizations use cloud-based services or apps in the workplace and approximately 53 percent use their personally owned mobile devices (BYOD) in the workplace. About 50 percent of these employees use their own devices to connect to cloud-based services or apps.

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



Do certain changes in an organization's use of cloud services affect the likelihood of a data breach? As discussed, 17 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 [2] 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 organization. As shown, 90 percent of respondents say their organization 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 a primary cloud service provider moves its data center operations from the U.S. to an off-shore location.

Table 1. Summary of nine cloud multiplier scenarios	Does this scenario increase the probability of a data breach for your organization?
S1. The number of network-connected mobile devices with access to cloud services increases by 50 percent within your organization over a 12-month period.	77%
S2. The use of cloud services increases by 50 percent within your organization over a 12-month period.	86%
S3. The use of cloud infrastructure services increases by 50 percent within your organization over a 12-month period.	69%
S4. The backup and storage of sensitive and/or confidential information in the cloud increases by 50 percent within your organization over a 12-month period.	90%
S5. The number of employee-owned mobile devices with access to cloud services increases by 50 percent within your organization over a 12-month period.	83%
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 organization over a 12-month period.	85%
S7. One of your organization's primary cloud services provider moves their data center operations from the United States to an off-shore location.	65%
S8. One of your organization's primary cloud services provider expanded operations too quickly and is now experiencing financial difficulties.	73%
S9. One of your organization's primary cloud providers fails a compliance audit. The audit failure concerns the provider's inability to securely manage identity and authentication processes.	68%

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

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

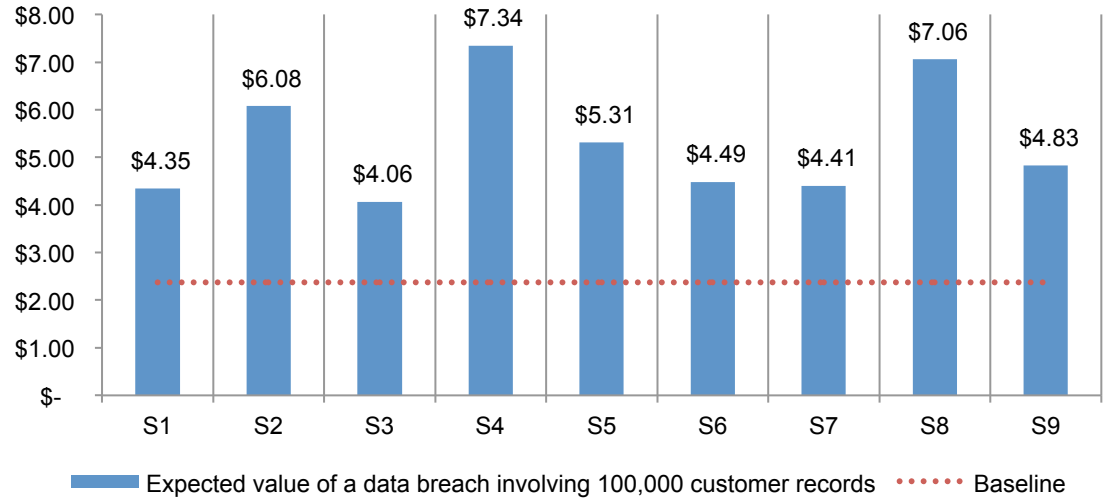
In this section, we calculate what it might cost an organization to deal with a data breach in the cloud involving customer records. These calculations are based on Ponemon Institute's recent cost of data breach research and the estimated likelihood or probability of a data breach based on cloud use.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

- First, drawing upon Ponemon Institute's most recent cost of data breach study, we determine a cost of $201.18 dollars per compromised record.[3]
- Second, based on a data breach size of 100,000 or more compromised records in the survey and using the unit cost of $201.18 times 100,000 records, we calculate a total cost of $20,118,000
- Third, from the survey results we extrapolate the average likelihood of a data breach involving 100,000 or more questions at approximately 11.8 percent over a two-year period.
- Fourth, multiplying the estimated likelihood or probability of a data breach at 11.8 percent times the total cost of $20,118,000 we calculate a baseline expected value of $2.37 million as the average of what an organization 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 organizations 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 $2.37 million. This means that all nine scenarios accelerate data breach costs.

What can cost an organization the most? A 50 percent increase in the backup and storage of sensitive customer data in the cloud could cost an average of $7.34 million if this data was lost or stolen. Another expensive data breach could result when a cloud provider expands operations too quickly and experiences financial difficulties $7.06 million.

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)



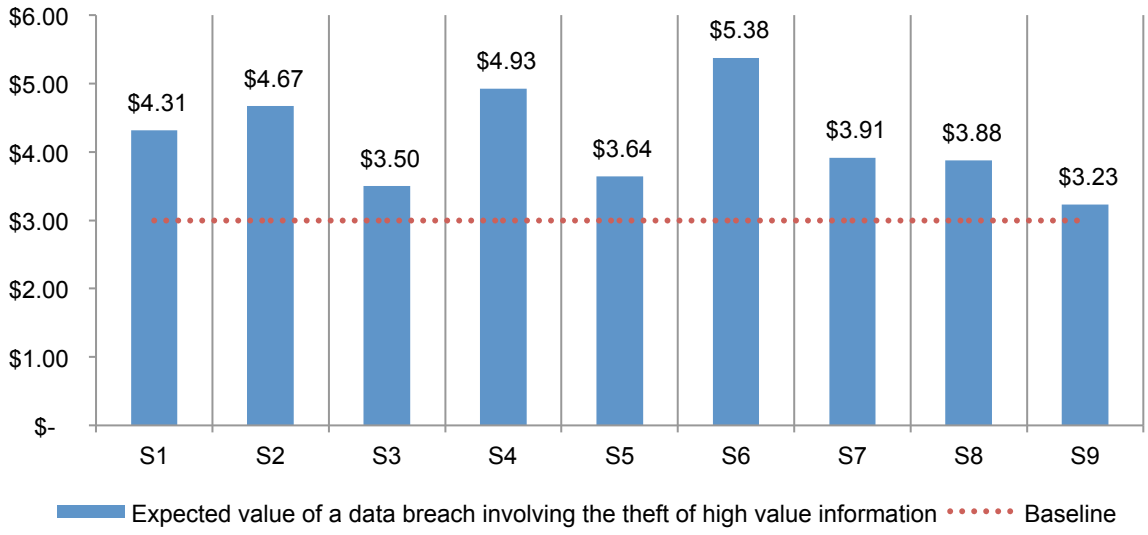
[3]See the 2014 Cost of Data Breach Study: United States, Ponemon Institute (sponsored by IBM), May 2014.

In this section, we calculate what it might cost an organization 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 four 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 $11,788,000.[4]
- Second, based upon the estimates provided by respondents we extrapolate the likelihood of a data breach involving the theft of high value information at 25.4 percent.
- Third, multiplying the estimated likelihood or probability of a data breach at 25.4 percent times the total cost of $11.788 million we calculate a baseline expected value of $2.99 million as the average economic impact for organizations in our study.

What can cost an organization the most when it has a data breach involving the loss or theft of IP? Figure 10 shows that the most costly scenarios involve 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) and an increase in the backup and storage of IP or business confidential information in the cloud. The average costs to deal with these two types of data breaches are $5.38 million and $4.93 million, respectively.

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



[4]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 organization. The net increase in data breach costs involving the loss or theft of 100,000 or more customer records is $2.95 million. Similarly, the net increase in data breach costs involving the theft of high value information is expected to increase by $1.17 million.

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

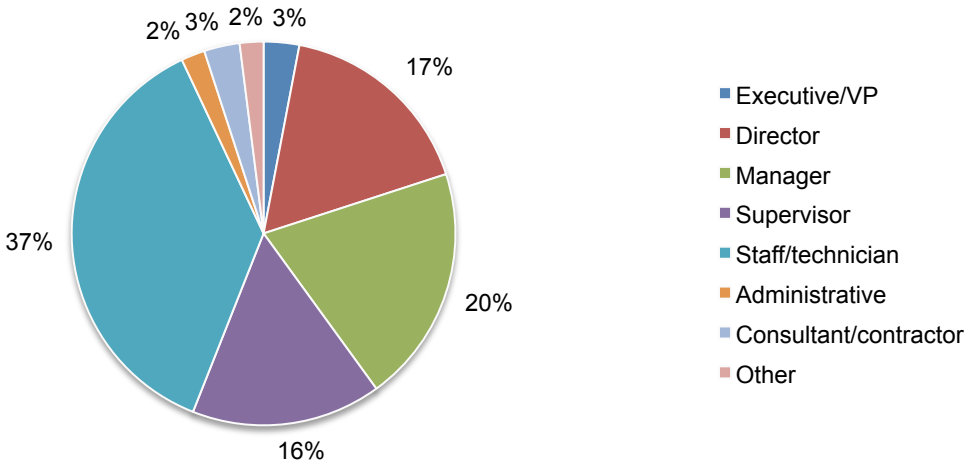
Part 4. Methods

A sampling frame of 16,330 experienced IT and IT security practitioners located in the United States were selected as participants to this survey. To ensure knowledgeable responses, all participants in this research are familiar with their company's cloud-based services. Table 2 shows 688 total returns. Screening and reliability checks required the removal of 75 surveys. Our final sample consisted of 613 surveys or a 3.8 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	16,330	100.0%
Total returns	688	4.2%
Rejected or screened surveys	75	0.5%
Final sample	613	3.8%

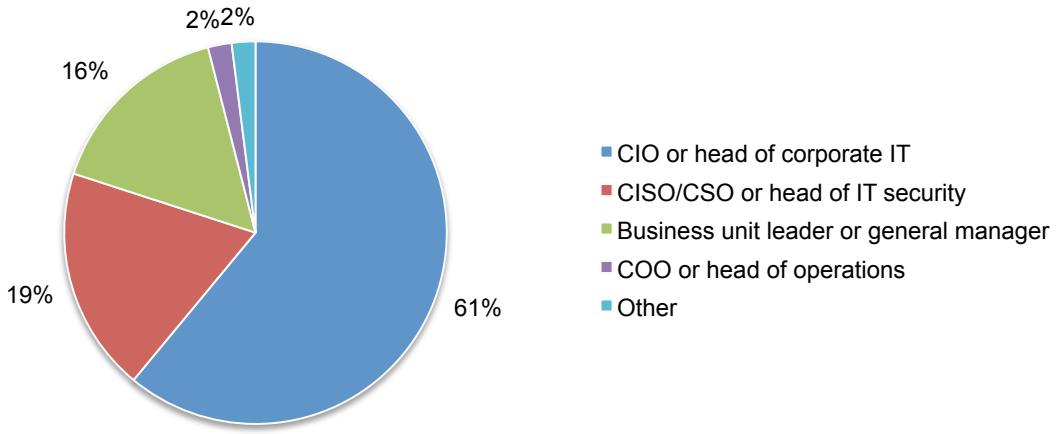
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 56 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



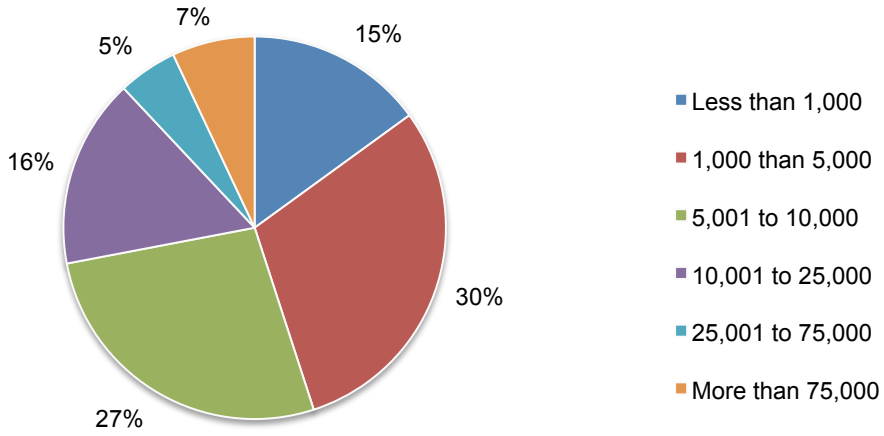
Pie Chart 2 reports that 61 percent of respondents report directly to the CIO or head of corporate IT, 19 percent report to the CISO/CSO or head of IT security and 16 percent report to the business unit leader or general manager.

Pie Chart 2. Direct reporting channel



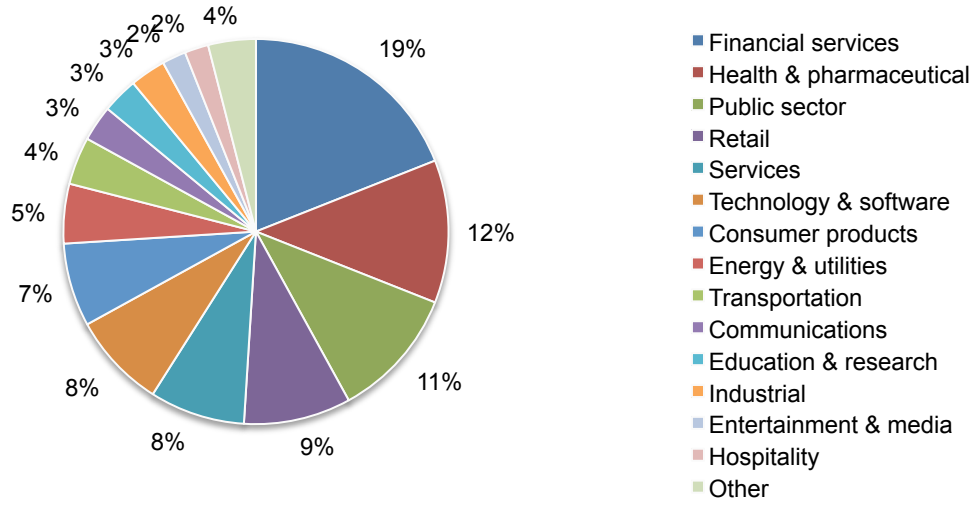
As shown in Pie Chart 3, 85 percent of respondents are from organizations with a global headcount of 1,000 or more employees.

Pie Chart 3. The full-time headcount of the global organization



Pie Chart 4 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health and pharmaceuticals (12 percent), public sector (11 percent), and retail (9 percent).

Pie Chart 4. Primary industry classification



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 March 2014.

Survey response	Freq	Pct%
Total sampling frame	16330	100.0%
Total returns	688	4.2%
Rejected or screened surveys	75	0.5%
Final sample	613	3.8%

Part 1. Screening

S1. Does your organization use cloud-based services?	Pct%
Yes	100%
No (stop)	0%
Total	100%

S2. What best defines your familiarity with the cloud-based services used by your organization today?	Pct%
Very familiar	34%
Familiar	45%
Somewhat familiar	21%
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 organization's level of effectiveness in securing data and applications used in the cloud.	Pct%
1 to 2	25%
3 to 4	26%
5 to 6	23%
7 to 8	14%
9 to 10	12%
Total	100%

Q2. What one statement best describes your opinion about the security of cloud-based services in comparison to on-premise IT security?	Pct%
On-premise IT is more secure than cloud-based services	44%
On-premise IT and cloud-based services are equally secure	35%
On-premise IT is less secure than cloud-based services	16%
Cannot determine	5%
Total	100%

Q3. Approximately, how many computing devices such as desktops (home and office), laptops, tablets and smart phones are connected to your organization's networks and/or enterprise systems?	Pct%
Less than 1,000	5%
1,001 to 5,000	22%
5,001 to 10,000	30%
10,001 to 25,000	19%
25,001 to 50,000	9%
50,001 to 75,000	6%
75,001 to 100,000	5%
100,001 to 200,000	2%
More than 200,000	2%
Total	100%

Q4a. Approximately, what percent of all software applications used by your organization are in the cloud?	Pct%
Zero	0%
Less than 10%	11%
10% to 25%	17%
26% to 50%	33%
51% to 75%	30%
76% to 100%	11%
Total	102%

Q4b. Approximately, what percent of software applications in the cloud are not known, officially recognized or approved by your organization's IT function (i.e., shadow IT)?	Pct%
Zero	6%
Less than 10%	7%
10% to 25%	10%
26% to 50%	23%
51% to 75%	34%
76% to 100%	20%
Total	100%

Q5a. Approximately, what percent of business critical applications used by your organization are in the cloud?	Pct%
Zero	9%
Less than 10%	12%
10% to 25%	23%
26% to 50%	25%
51% to 75%	22%
76% to 100%	9%
Total	100%

Q5b. Approximately, what percent of business critical applications in the cloud are not known, officially recognized or approved by your organization's IT function (i.e., shadow IT)?	Pct%
Zero	51%
Less than 10%	20%
10% to 25%	9%
26% to 50%	8%
51% to 75%	7%
76% to 100%	5%
Total	100%

Q6a. Approximately, what percent of business information used by your organization is stored in the cloud?	Pct%
Zero	5%
Less than 10%	19%
10% to 25%	36%
26% to 50%	21%
51% to 75%	11%
76% to 100%	8%
Total	100%

Q6b. Approximately, what percent of business information in the cloud is not known, officially recognized or approved by your organization's IT function (i.e., shadow IT)?	Pct%
Zero	6%
Less than 10%	14%
10% to 25%	22%
26% to 50%	35%
51% to 75%	13%
76% to 100%	10%
Total	100%

Q7a. Approximately, what percent of sensitive or confidential business information used by your organization is stored in the cloud?	Pct%
Zero	27%
Less than 10%	40%
10% to 25%	19%
26% to 50%	7%
51% to 75%	6%
76% to 100%	1%
Total	100%

Q7b. Approximately, what percent of sensitive or confidential business information in the cloud is not known, officially recognized or approved by your organization's IT function (i.e., shadow IT)?	Pct%
Zero	10%
Less than 10%	24%
10% to 25%	34%
26% to 50%	15%
51% to 75%	16%
76% to 100%	1%
Total	100%

Q8. Approximately, what percent of employees in your organization use cloud-based services or apps in the workplace?	Pct%
Zero	0%
Less than 10%	12%
10% to 25%	20%
26% to 50%	29%
51% to 75%	23%
76% to 100%	16%
Total	100%

Q9. Approximately, what percent of employees use their personally owned mobile devices (a.k.a. BYOD) in the workplace?	Pct%
Zero	11%
Less than 10%	7%
10% to 25%	9%
26% to 50%	12%
51% to 75%	30%
76% to 100%	31%
Total	100%

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?	Pct%
Zero	0%
Less than 10%	10%
10% to 25%	15%
26% to 50%	19%
51% to 75%	42%
76% to 100%	14%
Total	100%

Part 3. The fragile cloud ecosystem

Q11. In your opinion, does the use of cloud-based services affect the likelihood of a data breach?	Pct%
Significant increase	17%
Increase	34%
No impact	35%
Decrease	11%
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?	Pct%
1% to 10%	71%
11% to 30%	21%
31% to 50%	5%
51% to 70%	2%
71% to 90%	1%
91% to 100%	0%
Total	100%

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?	Pct%
1% to 10%	50%
11% to 30%	20%
31% to 50%	11%
51% to 70%	8%
71% to 90%	5%
91% to 100%	6%
Total	100%

Scenario 1. The number of network-connected mobile devices with access to cloud services increases by 50 percent within your organization over a 12-month period.	
Q14a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	77%
No	21%
Cannot determine	2%
Total	100%

Q14b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	52%
11% to 30%	20%
31% to 50%	15%
51% to 70%	7%
71% to 90%	6%
91% to 100%	0%
Total	100%

Q14c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	29%
11% to 30%	22%
31% to 50%	15%
51% to 70%	16%
71% to 90%	13%
91% to 100%	5%
Total	100%

Scenario 2. The use of cloud services (SaaS) increases by 50 percent within your organization over a 12-month period.	
Q15a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	86%
No	12%
Cannot determine	2%
Total	100%

Q15b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	34%
11% to 30%	23%
31% to 50%	19%
51% to 70%	17%
71% to 90%	4%
91% to 100%	3%
Total	100%

Q15c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	25%
11% to 30%	21%
31% to 50%	17%
51% to 70%	16%
71% to 90%	15%
91% to 100%	6%
Total	100%

Scenario 3. The use of cloud infrastructure services (IaaS) increases by 50 percent within your organization over a 12-month period.	
Q16a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	69%
No	23%
Cannot determine	8%
Total	100%

Q16b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	44%
11% to 30%	32%
31% to 50%	18%
51% to 70%	3%
71% to 90%	2%
91% to 100%	1%
Total	100%

Q16c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	31%
11% to 30%	28%
31% to 50%	18%
51% to 70%	17%
71% to 90%	4%
91% to 100%	2%
Total	100%

Scenario 4. The backup and storage of sensitive and/or confidential information in the cloud increases by 50 percent within your organization over a 12-month period.	
Q17a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	90%
No	6%
Cannot determine	4%
Total	100%

Q17b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	23%
11% to 30%	25%
31% to 50%	21%
51% to 70%	18%
71% to 90%	8%
91% to 100%	5%
Total	100%

Q17c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	22%
11% to 30%	22%
31% to 50%	19%
51% to 70%	12%
71% to 90%	15%
91% to 100%	10%
Total	100%

Scenario 5. The number of employee-owned mobile devices (a.k.a. BYOD) with access to cloud services increases by 50 percent within your organization over a 12-month period.	
Q18a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	83%
No	12%
Cannot determine	5%
Total	100%

Q18b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	42%
11% to 30%	23%
31% to 50%	15%
51% to 70%	13%
71% to 90%	5%
91% to 100%	2%
Total	100%

Q18c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	33%
11% to 30%	27%
31% to 50%	16%
51% to 70%	12%
71% to 90%	8%
91% to 100%	4%
Total	100%

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 organization over a 12-month period.	
Q19a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	85%
No	11%
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?	Pct%
1% to 10%	43%
11% to 30%	30%
31% to 50%	15%
51% to 70%	8%
71% to 90%	3%
91% to 100%	1%
Total	100%

Q19c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	15%
11% to 30%	23%
31% to 50%	15%
51% to 70%	22%
71% to 90%	18%
91% to 100%	7%
Total	100%

Scenario 7. One of your organization's primary cloud services provider moves their data center operations from the United States to an off-shore location.	
Q20a. In your opinion, would this scenario increase the probability of a data breach for your organization?	Pct%
Yes	65%
No	26%
Cannot determine	9%
Total	100%

Q20b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	44%
11% to 30%	29%
31% to 50%	17%
51% to 70%	6%
71% to 90%	2%
91% to 100%	2%
Total	100%

Q20c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	22%
11% to 30%	28%
31% to 50%	26%
51% to 70%	17%
71% to 90%	5%
91% to 100%	2%
Total	100%

Scenario 8. One of your organization'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 organization?	Pct%
Yes	73%
No	20%
Cannot determine	7%
Total	100%

Q21b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	26%
11% to 30%	22%
31% to 50%	25%
51% to 70%	15%
71% to 90%	7%
91% to 100%	5%
Total	100%

Q21c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	23%
11% to 30%	25%
31% to 50%	29%
51% to 70%	18%
71% to 90%	3%
91% to 100%	2%
Total	100%

Scenario 9. One of your organization'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 organization?	Pct%
Yes	68%
No	29%
Cannot determine	3%
Total	100%

Q22b. If yes, please provide a revised estimate of a material data breach involving the loss or theft of customer records?	Pct%
1% to 10%	35%
11% to 30%	38%
31% to 50%	12%
51% to 70%	11%
71% to 90%	4%
91% to 100%	0%
Total	100%

Q22c. If yes, please provide a revised estimate of a material data breach involving the theft of high value IP or business confidential information.	Pct%
1% to 10%	32%
11% to 30%	30%
31% to 50%	20%
51% to 70%	13%
71% to 90%	5%
91% to 100%	0%
Total	100%

Part 4. Attributions used for cloud confidence index (11 items)	Strongly agree	Agree
Q25a. My organization's use of cloud resources does not diminish its ability to protect confidential or sensitive information.	13%	21%
Q25b. My organization's use of cloud resources does not diminish its ability to secure business-critical applications.	14%	22%
Q25c. The cloud services used by my organization are thoroughly vetted for security before deployment.	18%	20%
Q25d. My organization is vigilant in conducting audits or assessments of cloud-based services.	14%	23%
Q25e. My organization is proactive in assessing information that is too sensitive be stored in the cloud.	15%	16%
Q25f. My organization's IT security leader (a.k.a. CISO) is responsible for ensuring our organization's safe use of cloud computing resources.	21%	24%
Q25g. The cloud service providers used by my organization would notify us immediately if they had a data breach involving the loss or theft of our customer data.	11%	18%
Q25h. The cloud service providers used by my organization would notify us immediately if they had a data breach involving the loss or theft of our intellectual property or business confidential information.	10%	18%
Q25i. My organization's cloud service providers utilize enabling security technologies to protect and secure sensitive and/or confidential information.	12%	19%
Q25j. My organization's cloud service providers are in full compliance with privacy and data protection regulations and laws.	14%	22%
Q25k. My organization's cloud service providers are financially stable (i.e., good financial health).	15%	26%

Part 5. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Pct%
Executive/VP	3%
Director	17%
Manager	20%
Supervisor	16%
Staff/technician	37%
Administrative	2%
Consultant/contractor	3%
Other	2%
Total	100%

D2. What best describes your direct reporting channel?	Pct%
CEO/executive committee	0%
COO or head of operations	2%
CFO, controller or head of finance	1%
CIO or head of corporate IT	61%
Business unit leader or general manager	16%
Head of compliance or internal audit	1%
CISO/CSO or head of IT security	19%
Other	0%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
Less than 1,000	15%
1,000 than 5,000	30%
5,001 to 10,000	27%
10,001 to 25,000	16%
25,001 to 75,000	5%
More than 75,000	7%
Total	100%

D4. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	7%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	19%
Health & pharmaceutical	12%
Hospitality	2%
Industrial	3%
Public sector	11%
Retail	9%
Services	8%
Technology & software	8%
Transportation	4%
Other	2%
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 organizations.

As a member of the **Council of American Survey Research Organizations (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.