Cloud Security: Getting It Right

Sponsored by Armor

Independently conducted by Ponemon Institute LLC

Publication Date: October 2015

Cloud Security: Getting It Right

Ponemon Institute, October 2015

Part 1. Introduction

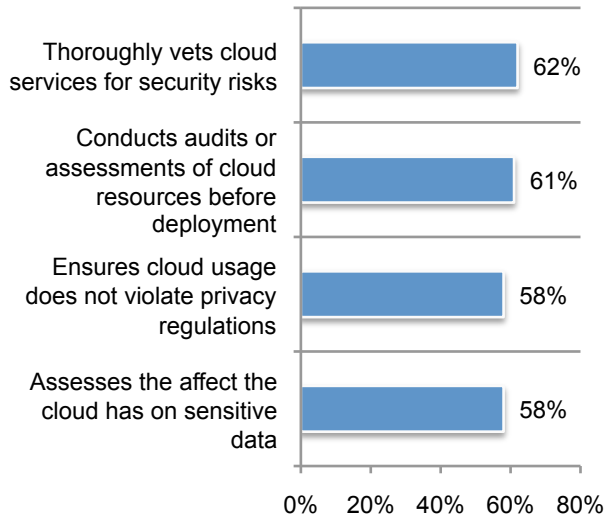
Cloud Security: Getting It Right, sponsored by Armor, reveals eight security mistakes companies make when using cloud resources. If not corrected, companies will continue to find it difficult to reduce the risk of having their sensitive or confidential data breached or compromised in the cloud.

As confirmed in this study, outsourcing sensitive data to the cloud is becoming an important strategy for companies seeking to control costs and increase efficiency. Therefore, it is critical for companies to understand how they can stop the mistakes and best address the threats to sensitive and confidential information in the cloud.

The findings in Figure 1 reveal why the majority of companies represented in this study are not getting cloud security right. Specifically, they are not investing the time and resources to make sure sensitive and confidential data in the cloud is secure. The majority of companies in this study:

Figure 1. Why companies are not doing cloud security right

Unsure, disagree and strongly disagree combined



- Do not assess the affect the cloud may have on the ability to protect and secure confidential or sensitive information (58 percent of respondents)
- Do not thoroughly vet cloud services for security risks (62 percent of respondents)
- Are not vigilant in conducting audits or assessments of cloud resources before deployment (61 percent of respondents)
- Ensure cloud usage does not violate privacy and/or data protection regulations (58 percent of respondents)

Because organizations are not taking these important steps, almost half (48 percent of respondents) of organizations represented in this study limit the use and/or storage of sensitive and confidential data in the cloud. Instead of not taking advantage of the benefits provided by the cloud, a much better approach to cloud security would be for organizations to improve their approach to vetting and securing cloud providers and ensuring they are in compliance with all applicable privacy and data protection regulations.

The eight cloud security mistakes

We surveyed 990 individuals in the United States and United Kingdom who hold such positions as chief information officer, director of IT operations and chief information security officer. To ensure a quality response, only individuals who are knowledgeable about their companies' use of cloud services participated in the research.

Represented in this research are organizations that process business-critical applications in the cloud environment and store sensitive or confidential information business data in the cloud environment. Based on the findings, we have identified the following eight cloud security mistakes:

1. IT security is rarely involved in ensuring the security of SaaS and IaaS.
2. Most companies are not evaluating SaaS applications and IaaS resources for security prior to deployment.
3. IT is in the dark about cloud services and infrastructure in their organizations. Instead, procurement and cloud users are responsible for cloud security.
4. IT security is not involved in evaluating cloud service providers.
5. Companies do not ensure offshore cloud providers are in compliance with regulations and do they care?
6. Companies' cloud deployment strategy often leaves out the use of security technologies in the cloud environment.
7. Inspection of data in the cloud rarely happens.
8. Despite concerns about cloud security, organizations are not willing to pay for extra security.

Part 2. Key findings

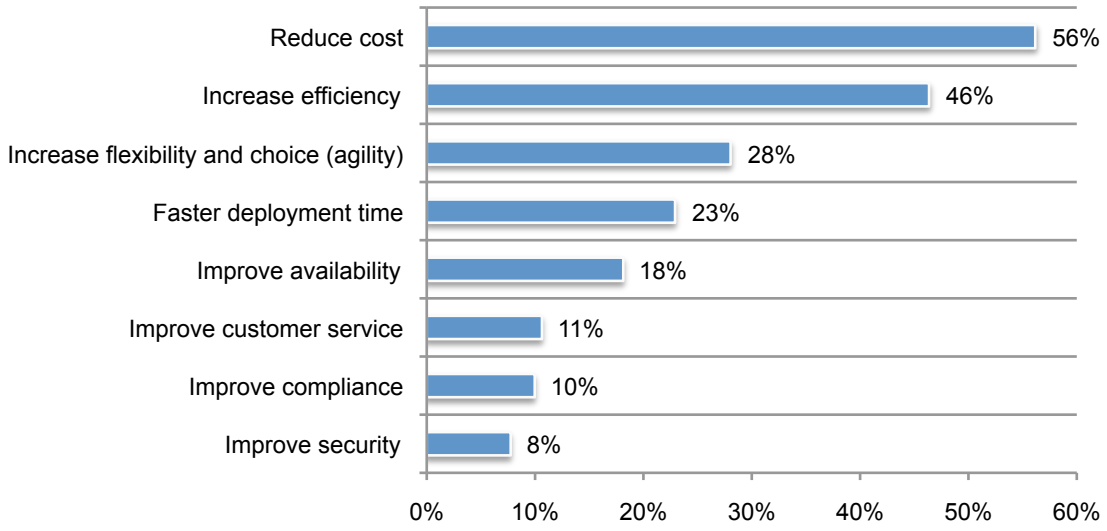
In this section, we present an analysis of the key findings. The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics.

- The growing appeal of Software as a Service (SaaS) and Infrastructure as a Service (IaaS)
- Eight cloud security mistakes put confidential data at risk
- Differences between organizations in the United States and United Kingdom
- Conclusion: How to get cloud security right

The growing appeal of SaaS and IaaS

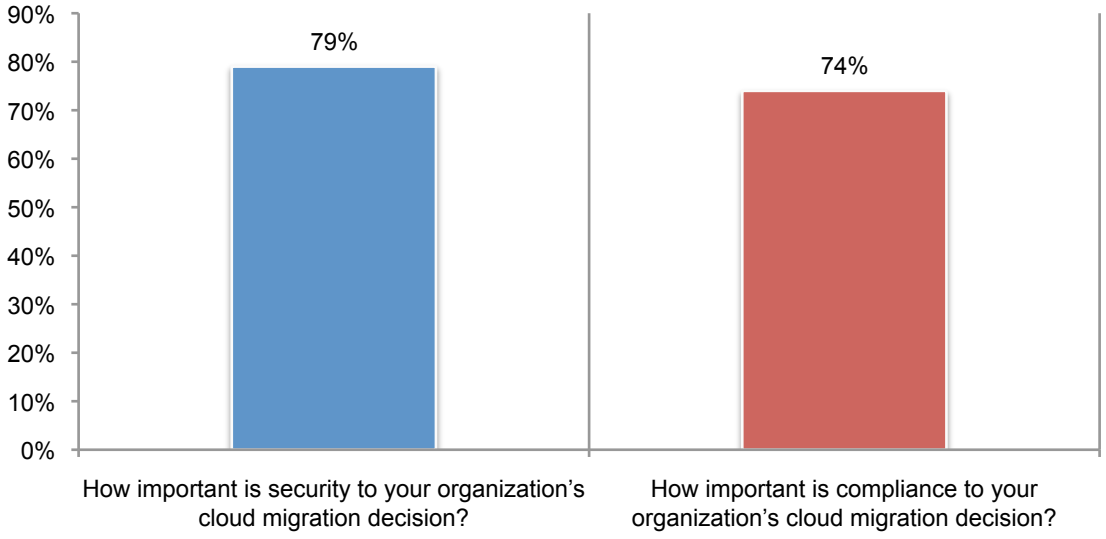
Reduced cost and increased efficiency drives the use of cloud services. As shown in Figure 2, 56 percent of respondents say the ability to save money is by far the primary reason to use cloud resources. Forty-six percent say it increases efficiency. Only 8 percent say it is to improve security and 10 percent say it is to improve compliance. The importance of cost and efficiency may explain why the procurement function and the end user, as discussed later in this report, are most involved in making decisions about the use of cloud resources.

Figure 2. Primary reasons cloud resources are used
Two responses permitted



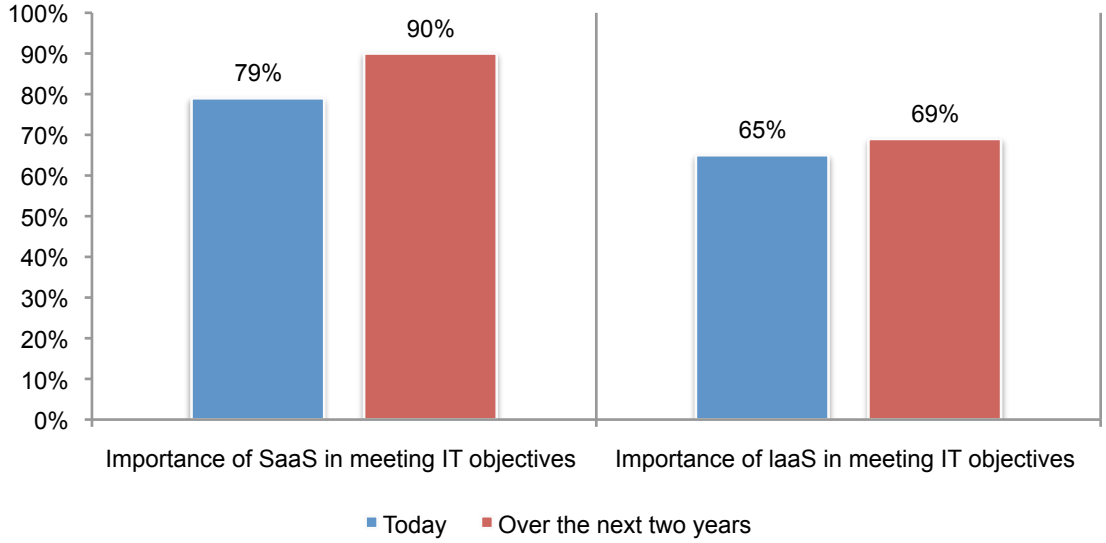
Security and compliance are important to the cloud migration decision. The findings in this study indicate companies are not taking the necessary steps to ensure the security and compliance of cloud providers. However, as shown in Figure 3, 79 percent or respondents say security is important always or most of the time and 74 percent of respondents say compliance is considered important always or most of the time.

Figure 3. The importance of security and compliance the cloud migration decision
Always and most of the time response combined



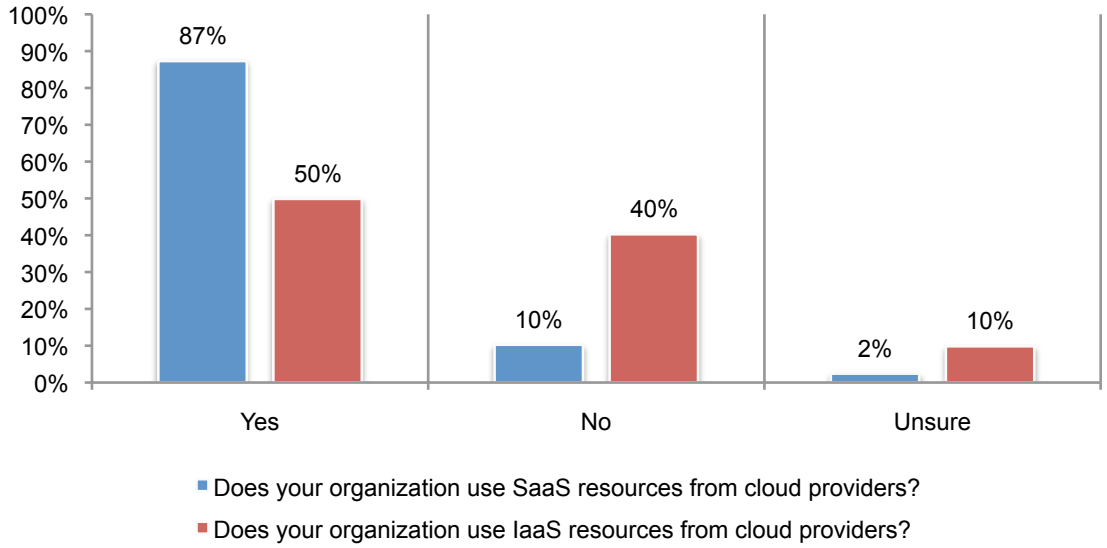
SaaS and IaaS grow in importance despite a lack of confidence in their security. As shown in Figure 4, the importance of SaaS will significantly outpace IaaS. Today, 79 percent of respondents say SaaS is important today to meeting IT objectives and 90 percent say it will be important over the next two years. Sixty-five percent of respondents say IaaS is important today and will grow slightly in importance over the next two years (69 percent of respondents).

Figure 4. The importance of SaaS and IaaS today and over the next two years
Very important and important response combined



According to Figure 5, 87 percent of respondents say their organizations use SaaS resources from cloud providers and 50 percent of respondents say their organizations use IaaS from cloud providers. On average, these organizations are using 13 different SaaS providers and 6 IaaS providers. An average of 32 percent of business-critical applications use SaaS versus conventional software applications and 25 percent of business-critical resources use IaaS versus on premises infrastructure services.

Figure 5. Does your organization use SaaS and IaaS resources from cloud providers?



On-premise IT is considered more secure than the cloud. On average, 56 percent of respondents have confidence their organizations are meeting their security objectives in the on-premise IT environment but only 33 percent of respondents say they have confidence they are meeting the security objectives in the cloud.

Figure 6 reveals the significant differences in levels of confidence between security in the on-premise IT environment and in the cloud. The biggest differences are the ability to limit access to the IT infrastructure (54 percent difference), enforce security policies (52 percent difference) and prevent or curtail system-level connections from insecure endpoints (48 percent difference).

Figure 6. Confidence in on-premise IT and cloud security
Very confident and confident response combined

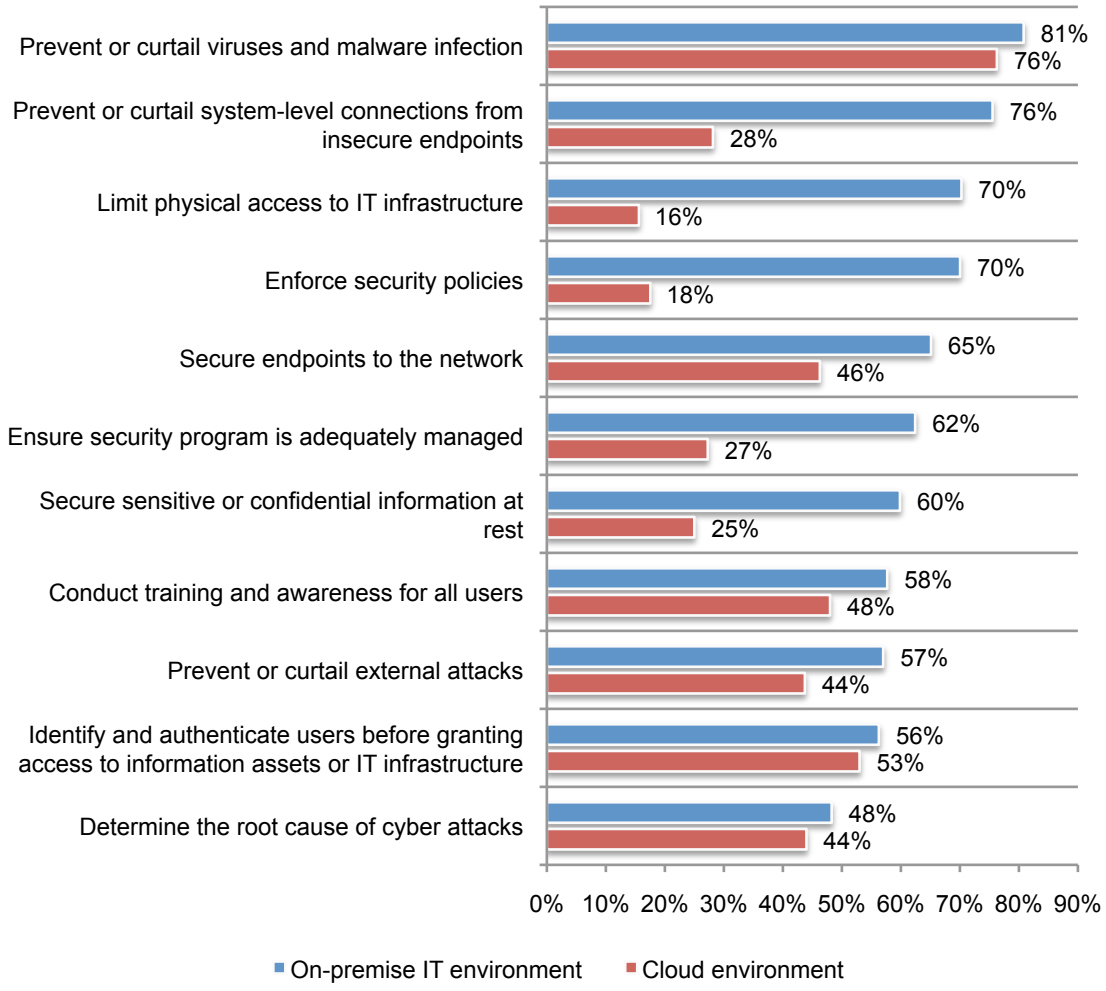
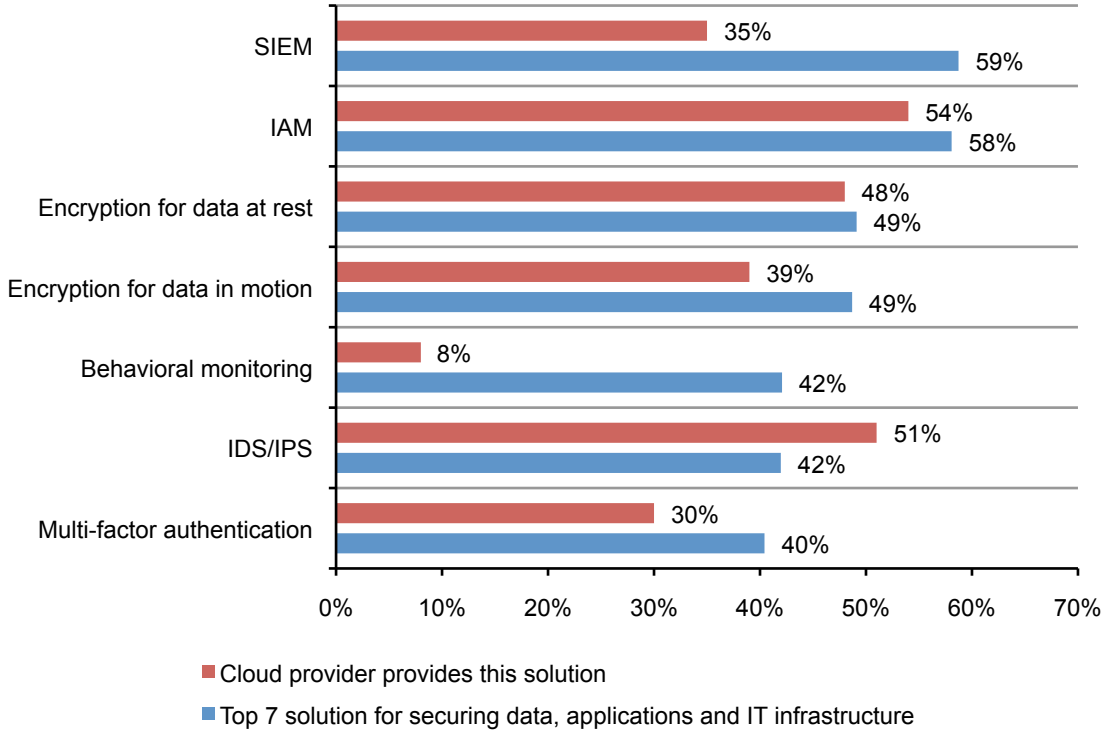


Figure 7 lists the of top seven security solutions for securing data, applications and IT infrastructure according to all respondents. This figure also lists the availability of each solution as a service provided by the respondents' cloud providers. As can be seen, SIEM, identity and access management (IAM), encryption for data at rest, encryption for data in motion, behavioral, IDS/IPS and multi-factor authentication are the seven most important security solutions.

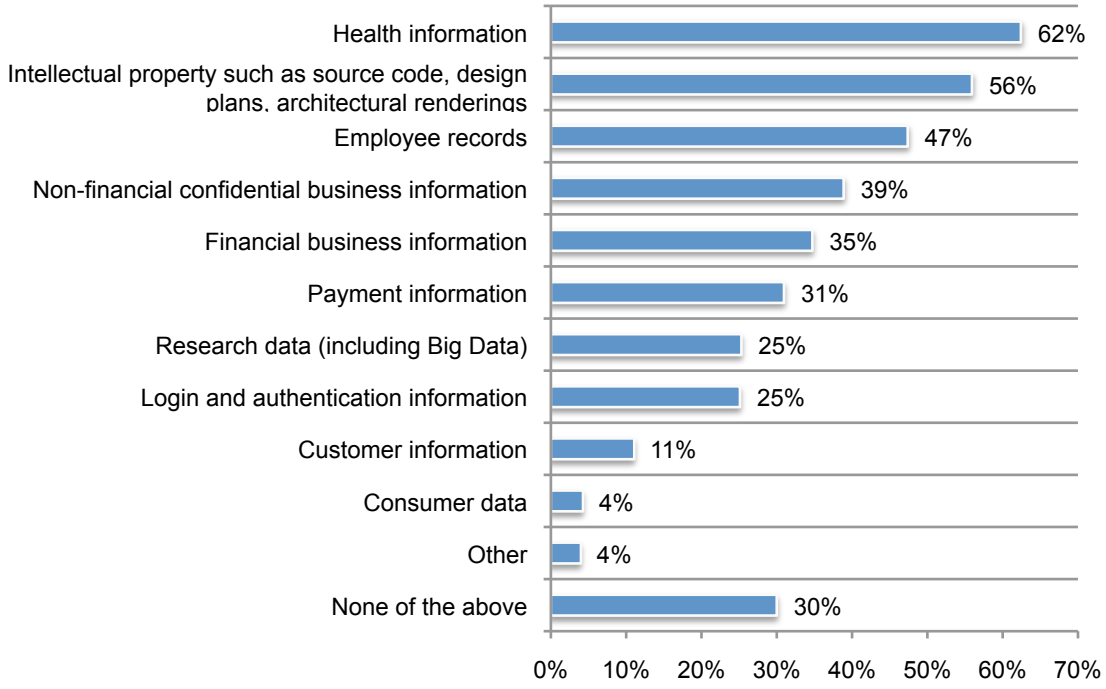
With respect to differences between importance and availability, the widest gaps are behavioral monitoring (Diff = 36%), SIEM (Diff = 24%) and encryption for data in motion (Diff = 10%). The only negative gap pertains to IDS/IPB (Diff = -9%).

Figure 7. Top seven solutions for securing data, applications and IT infrastructure: Does your cloud provider provide this as a service?
More than one response permitted



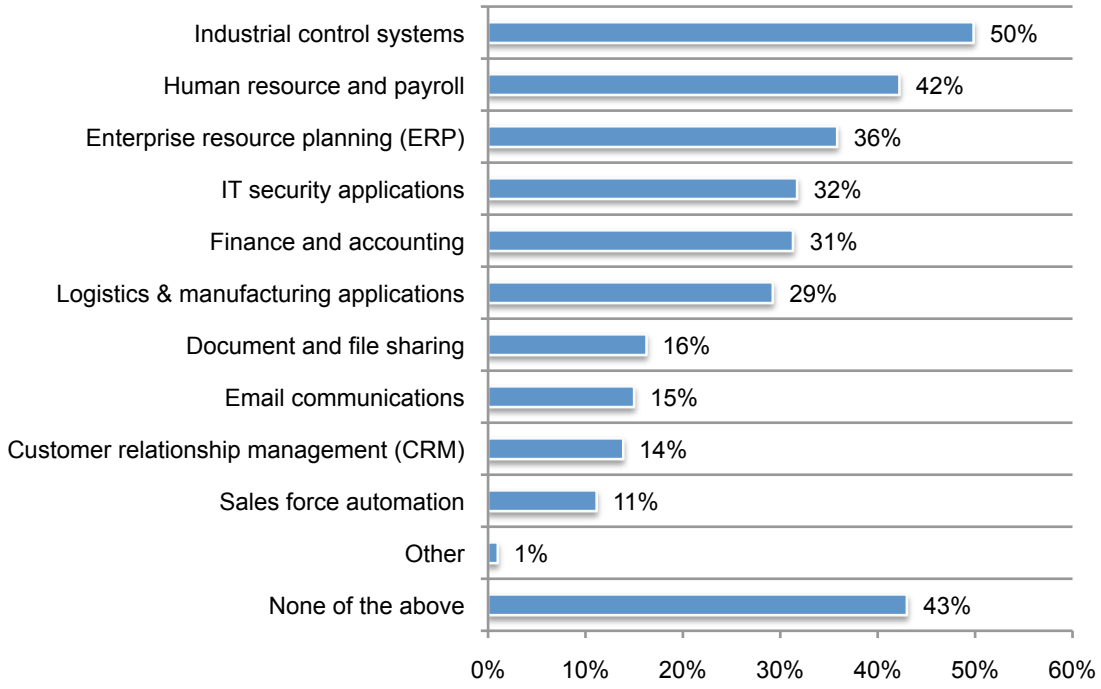
Data considered too risky for the cloud. Because of these security issues, 52 percent of respondents say their organization limits the use and storage of sensitive and confidential data in the cloud. According to Figure 8, confidential data such as health information (62 percent of respondents), intellectual property (56 percent of respondents) and employee records (47 percent of respondents) are considered too sensitive to be processed and stored in the cloud.

Figure 8. Top 5 types of confidential or sensitive information too risky to be processed and/or stored in the cloud
More than one response permitted



What are the business applications considered too risky to be processed and housed in the cloud? As shown in Figure 9, these are industrial control systems (50 percent of respondents), human resource and payroll (42 percent of respondents) and enterprise resource planning (36 percent of respondents). Not considered as risky are sales force automation (11 percent of respondents), customer relationship management (14 percent of respondents) and email communications (15 percent of respondents).

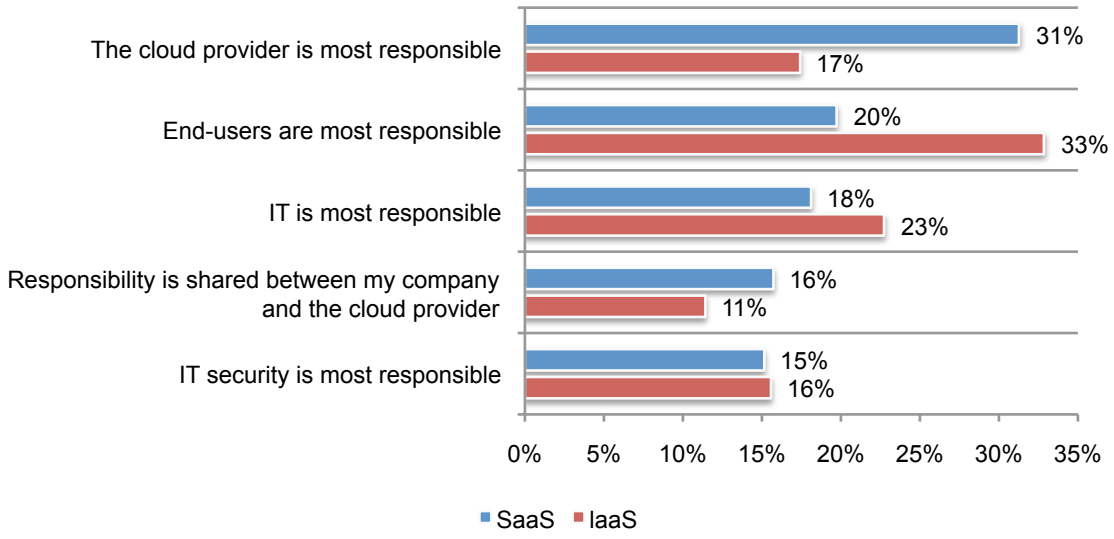
Figure 9. Top 5 types of business applications considered too risky to be processed and/or housed in the cloud
More than one response permitted



Cloud security mistakes put confidential data at risk

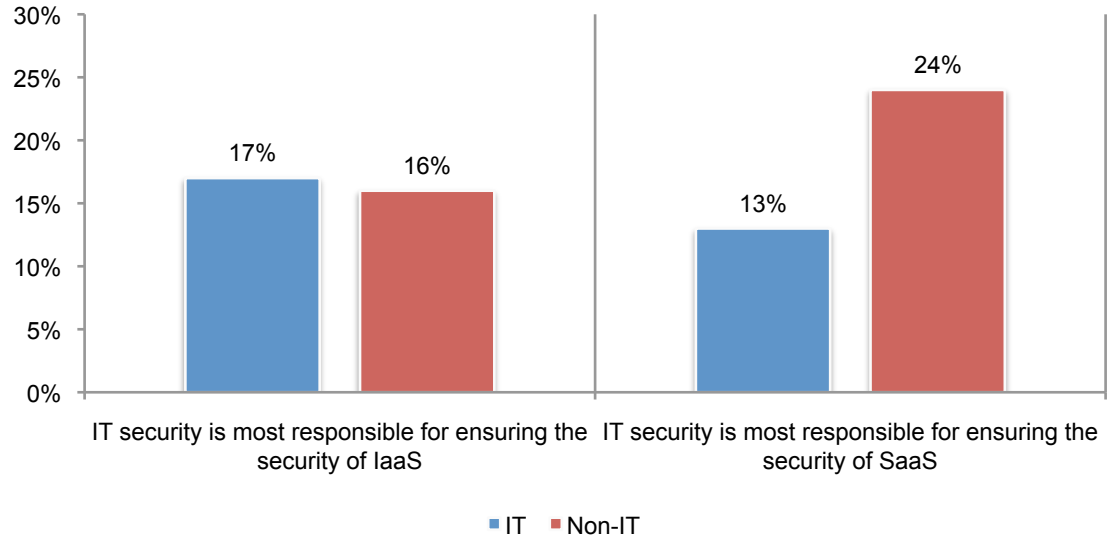
Mistake 1: IT security is rarely involved in ensuring the security of SaaS and IaaS. According to Figure 10, organizations are relying mainly upon the cloud provider to keep SaaS applications secure, (31 percent of respondents) and this is followed by the end-user being most accountable. Most responsible for ensuring security of IaaS resources is the end user (33 percent of respondents) followed by IT (23 percent of respondents).

Figure 10. Who is most responsible for ensuring the security of SaaS applications and IaaS resources in your organization?



According to Figure 10a, IT security and non-IT respondents are not in agreement about who is responsible for SaaS and IaaS security. A deeper analysis reveals 24 percent of non-IT respondents believe IT security is most responsible for ensuring the security of SaaS. While only 13 percent of IT security respondents believe they are responsible. A higher percentage of IT security respondents believe IT security is responsible for securing IaaS.

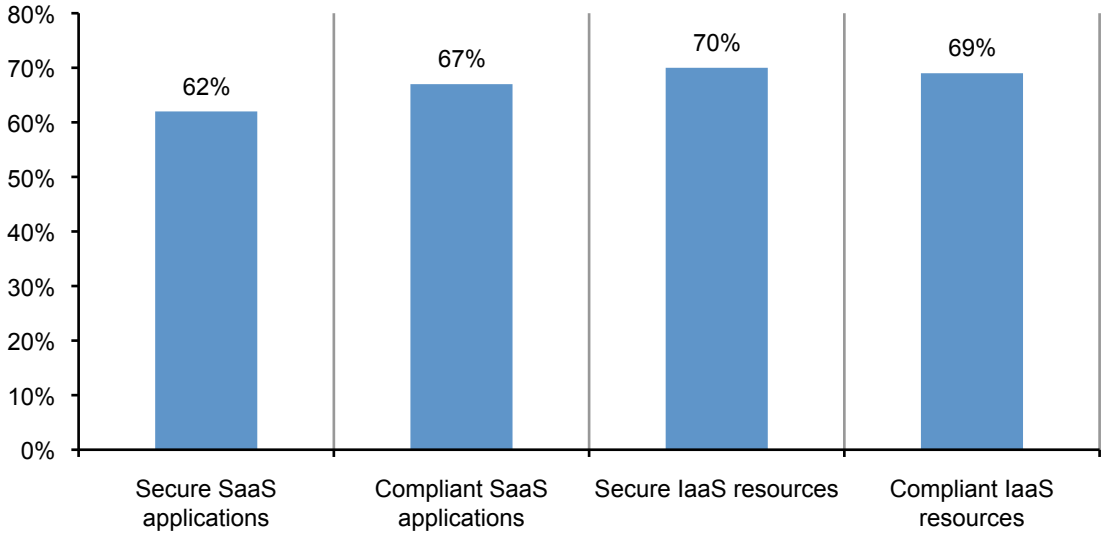
Figure 10a. Who is most responsible for ensuring the security of SaaS applications & IaaS resources in your organization?



Mistake 2: Most companies are not evaluating SaaS applications and IaaS resources for security prior to deployment. Only 44 percent of respondents say SaaS applications are evaluated and 41 percent of respondents say IaaS resources are evaluated for security prior to deployment. As a result, it is understandable confidence about security and compliance is low.

Figure 11 shows 62 percent of respondents, who are mainly in IT and IT security, have a low level of confidence in the security of SaaS and 67 percent of respondents have a low level of confidence in the compliance of SaaS applications. Similarly, 70 percent of respondents have low confidence that IaaS resources are secure and 69 percent have low confidence in IaaS compliance efforts.

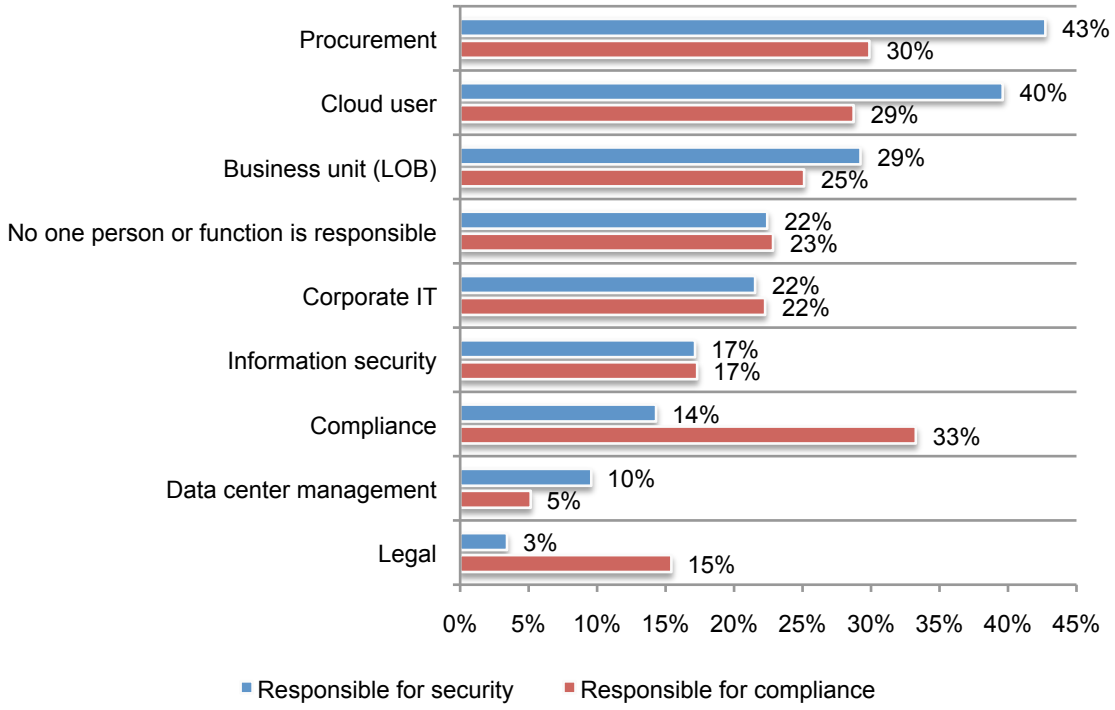
Figure 11. How confident are you that SaaS applications and IaaS resources used within your organization are secure and in compliance?
Not confident and no confidence responses combined



Mistake 3: IT is in the dark about cloud services and infrastructure in their organizations. Instead, procurement and cloud users are responsible for cloud security. According to Figure 12, 43 percent of respondents say the procurement function and 40 percent of respondents say it is the cloud user most responsible for ensuring cloud providers are adequately vetted and secured. Only 17 percent of respondents say information security and 22 percent of respondents say corporate IT is responsible.

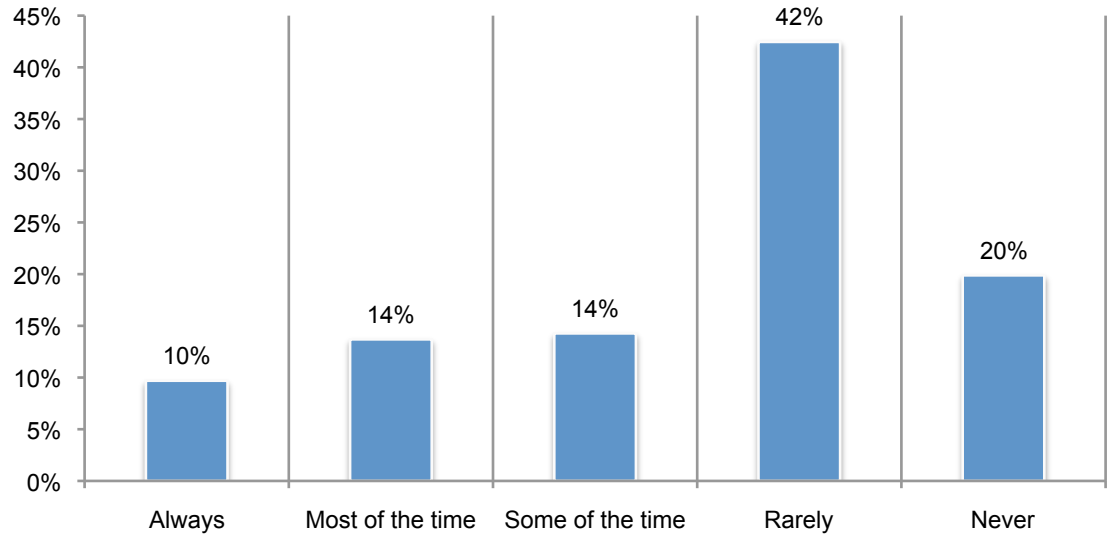
Thirty percent of respondents say procurement is most responsible for ensuring cloud providers are in compliance with all applicable privacy and data protection regulations followed by 29 percent of respondents who say it is the cloud user who is responsible. Few corporate IT and information security individuals are responsible for regulatory compliance. It is no surprise, therefore, that 67 percent of respondents say they have no or very little confidence the IT organization knows all cloud services and infrastructure in use.

Figure 12. Who is responsible for vetting and ensuring cloud providers are secure and in compliance with all applicable privacy and data protection regulations?
Two responses permitted



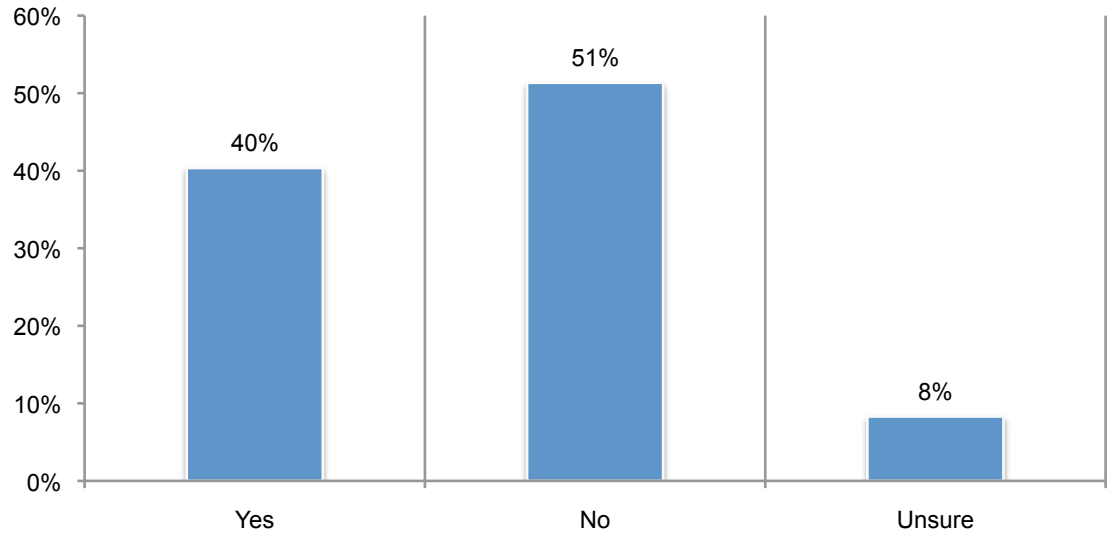
Mistake 4. IT security is not involved in evaluating cloud service providers. According to Figure 13, only 24 percent of respondents say their organization's security operations team is involved in evaluating cloud service providers always (10 percent of respondents) or most of the time (14 percent of respondents).

Figure 13. Are members of your organization's security operations involved in evaluating cloud service providers?



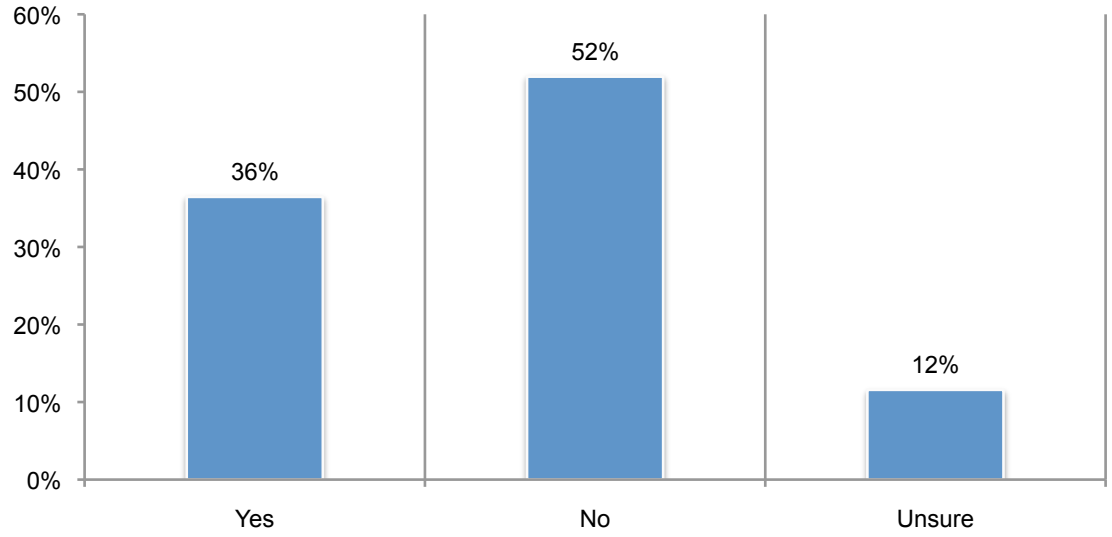
Mistake 5: Companies do not ensure offshore cloud providers are in compliance with regulations, and do they care? While 52 percent of respondents say their organizations' cloud providers operate in locations outside their home country, the majority of respondents say their organization is not vigilant in ensuring cloud usage does not violate privacy and/or data protection regulations. As shown in Figure 14, 40 percent of these respondents are concerned that sensitive data located offshore creates regulatory compliance issues but a much higher percentage don't seem to be concerned.

Figure 14. Does the fact your organization's data may be located offshore create any regulatory compliance issues?



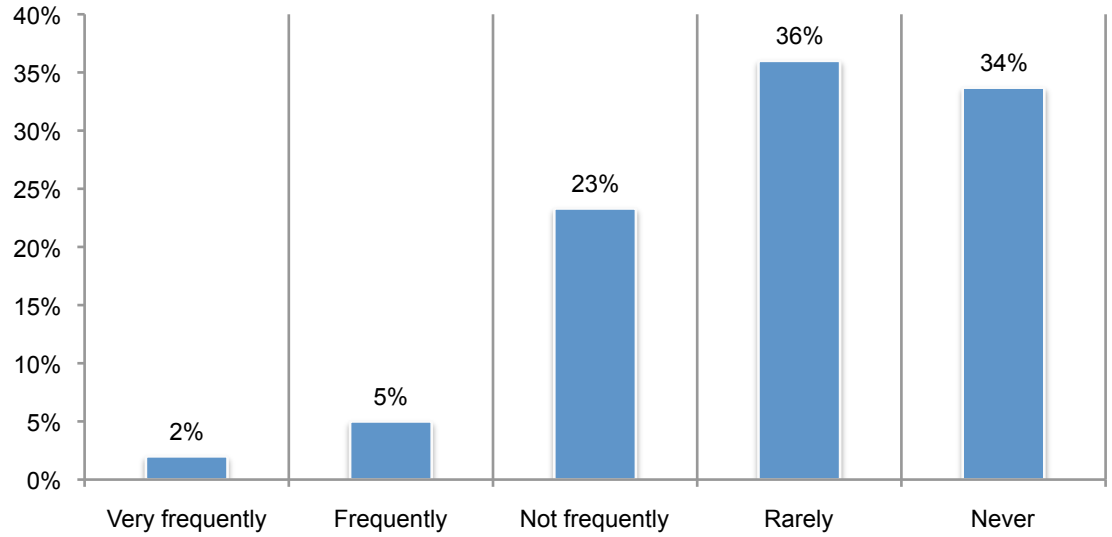
Mistake 6: Organizations' cloud deployment strategy often leaves out the use of security technologies in the cloud environment. Fifty-three percent of respondents say their organization has a cloud deployment strategy but 64 percent of respondents say the strategy does not include the use of security technologies resident in the cloud environment.

Figure 15. Does the cloud deployment strategy include the use of security technologies resident in the cloud environment?



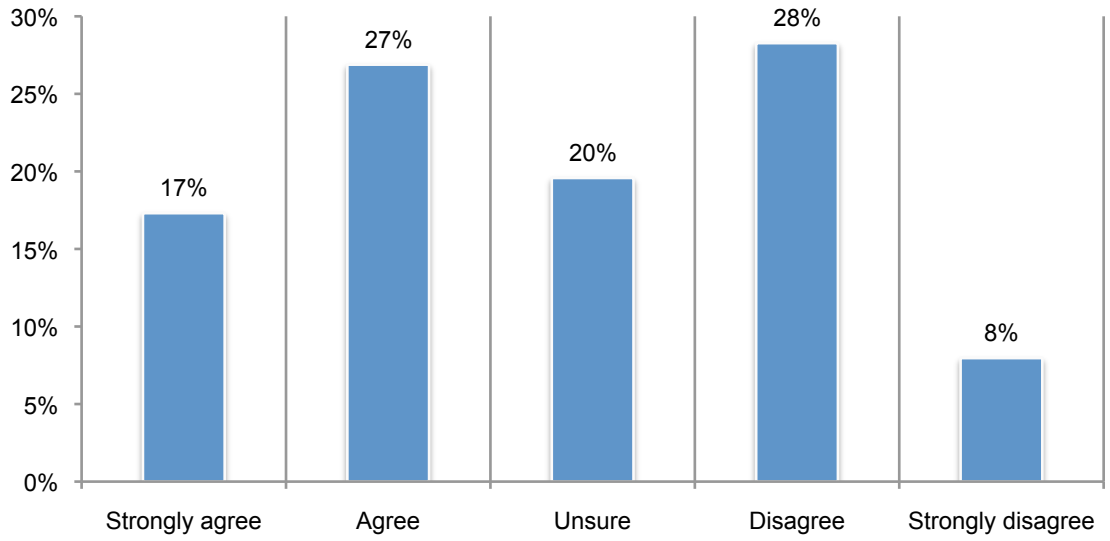
Mistake 7: Inspection of data in the cloud rarely happens. Only 22 percent of respondents say their organization has the ability to inspect data in the cloud and, as shown in Figure 16, 70 percent say it rarely or never happens. While almost half (48 percent of respondents) say their organizations have regulated data in the cloud, 51 percent of respondents say it does not increase concerns about regulatory inspections.

Figure 16. How frequently does your organization inspect this data?



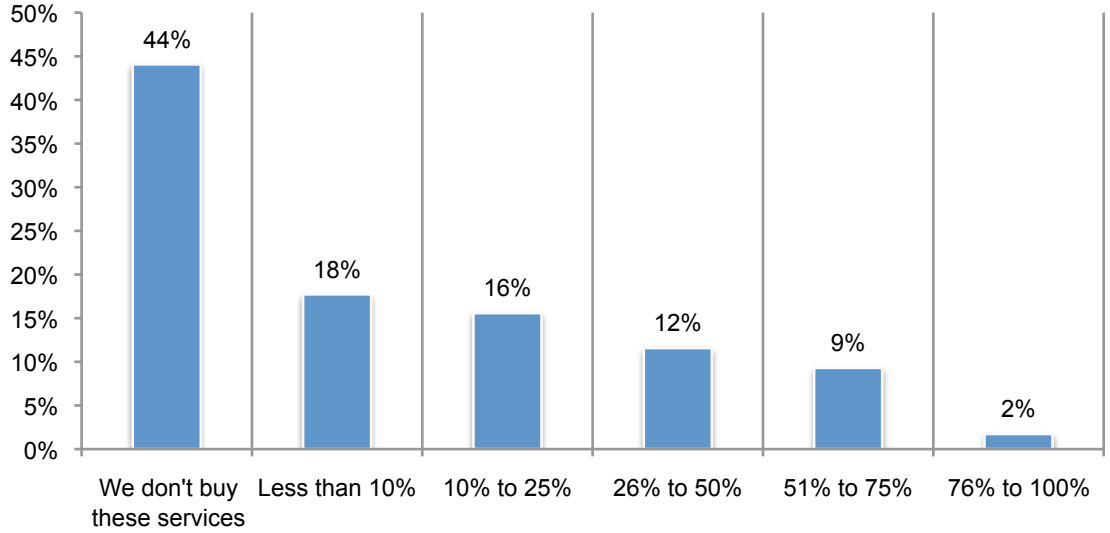
Mistake 8. Organizations are not willing to pay for extra security. According to Figure 17, despite concerns about cloud security, 56 percent of respondents say their organization would not be willing to pay a premium to ensure the security of sensitive or confidential data in the cloud. But are organizations willing to make the necessary investment in resources and governance to get cloud security right?

Figure 17. My organization is willing to pay a premium to ensure the security of sensitive or confidential data in the cloud



Thirty-seven percent of respondents say their cloud providers provide security as a premium service. However, as shown in Figure 18, 44 percent of respondents would not consider paying a premium. If security is purchased, the average premium paid is 16 percent above the base fees.

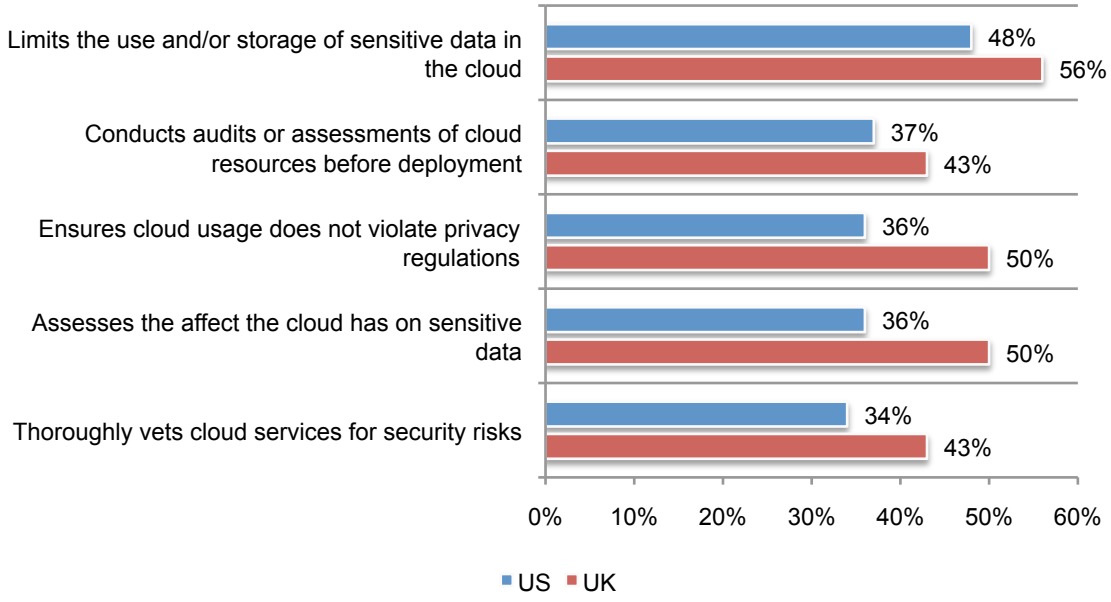
Figure 18. Does your organization pay more for premium security services in the cloud environment? Extrapolated value = 16 percent



Differences between organizations in the United States and United Kingdom

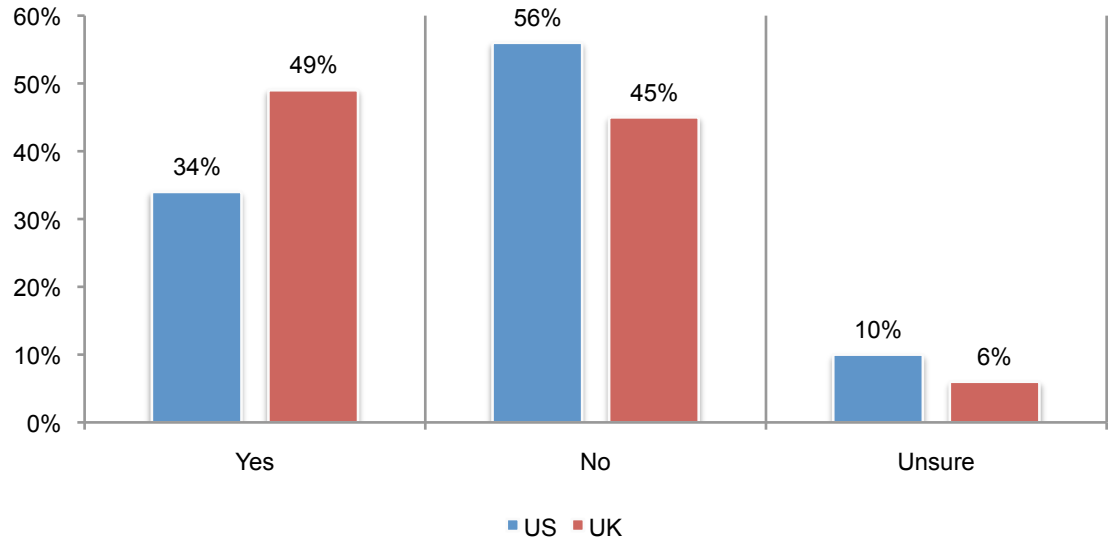
Organizations in the UK are more proactive in managing cloud security risks. As shown in Figure 19, UK respondents believe their organizations are most likely to do the following: assess the affect the cloud may have on the ability to protect and secure confidential or sensitive information, only use cloud services that are thoroughly vetted for security risks, conduct audits or assessments of cloud resources before deployment, limit the use and/or storage of sensitive and confidential data in the cloud, vigilant in ensuring cloud usage does not violate privacy and/or data protection regulations.

Figure 19. A comparison of UK and U.S. respondents' agreements about the security of cloud services in their organizations
Strongly agree and agree responses combined



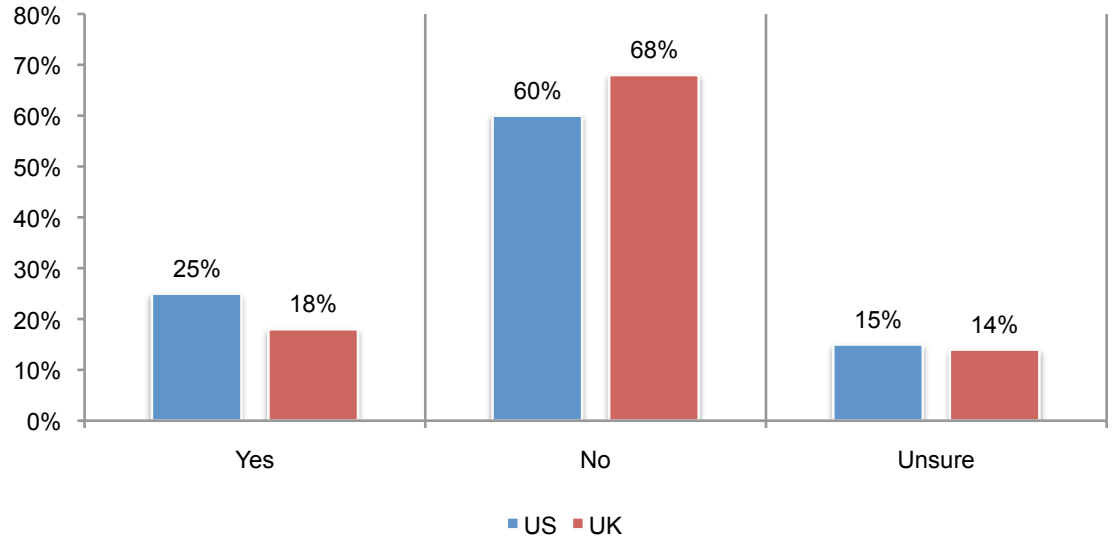
UK organizations worry more about regulatory compliance issues when data is located offshore. The majority of organizations in both countries use cloud providers in locations outside their home country. However, as shown in Figure 20, almost half of UK organizations are more worried about regulatory compliance issues than U.S. organizations.

Figure 20. Does the fact that your organization's data may be located offshore create any regulatory compliance issues?



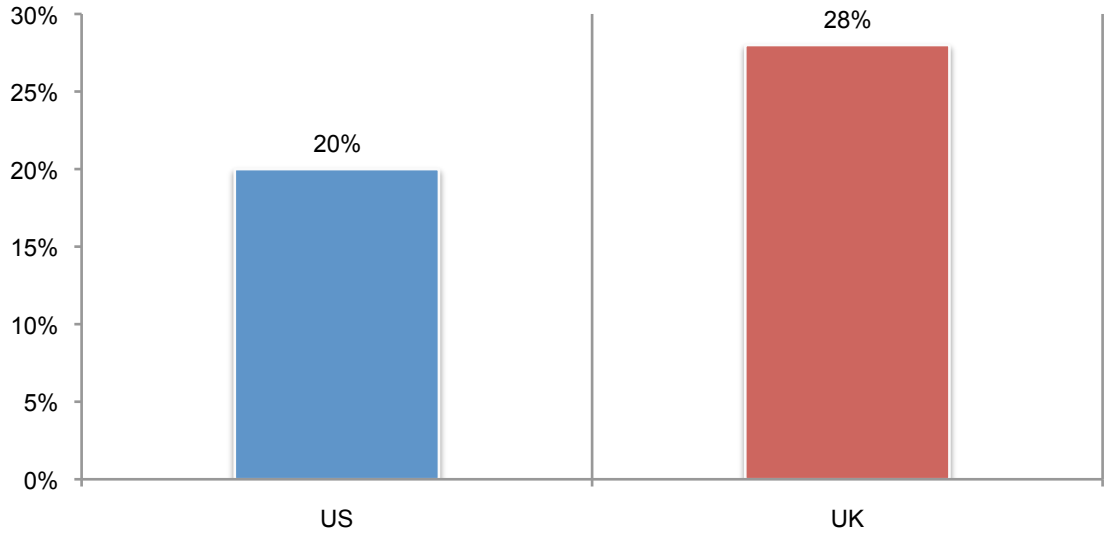
U.S. organizations are more likely to have the ability to inspect data in the cloud. As shown in Figure 21, more U.S. organizations have the ability to inspect data in the cloud (25 percent vs. 18 percent of respondents). In another finding, 68 percent of U.S. respondents and 72 percent of UK respondents say their organizations rarely or never inspect this data.

Figure 21. Does your organization have the ability to inspect data in the cloud?



UK organizations are more likely to have a security operations team involved in evaluating cloud service providers. According to Figure 22, only 20 percent of U.S. respondents versus 28 percent of UK respondents say such a team is involved always or most of the time.

Figure 22. Are members of your organization's security operations team involved in evaluating cloud service providers? Always or most of the time responses combined



Conclusion: How to get cloud security right

When it comes to cloud security and compliance, organizations are not "walking the talk". Organizations are increasing their use of SaaS and IaaS but with trepidation about cloud providers' ability to offer security and compliance with all applicable privacy regulations.

While organizations believe security and compliance are important, they clearly are not taking steps that are best handled by IT and IT security to ensure confidential and sensitive data in the cloud is secure. Instead they are mostly dependent upon the cloud provider or end user to achieve these objectives.

Steps to take should include: vetting cloud services for security risks, conducting audits or assessments of cloud resources before deployment, ensuring cloud usage does not violate privacy regulations and assessing the affect the cloud has on sensitive data. They also should have the ability to regularly inspect data in the cloud and have a cloud deployment strategy that includes the use of security technologies. Getting it right means having the same level of confidence in their cloud provider as they do with their own on-premise IT environment.

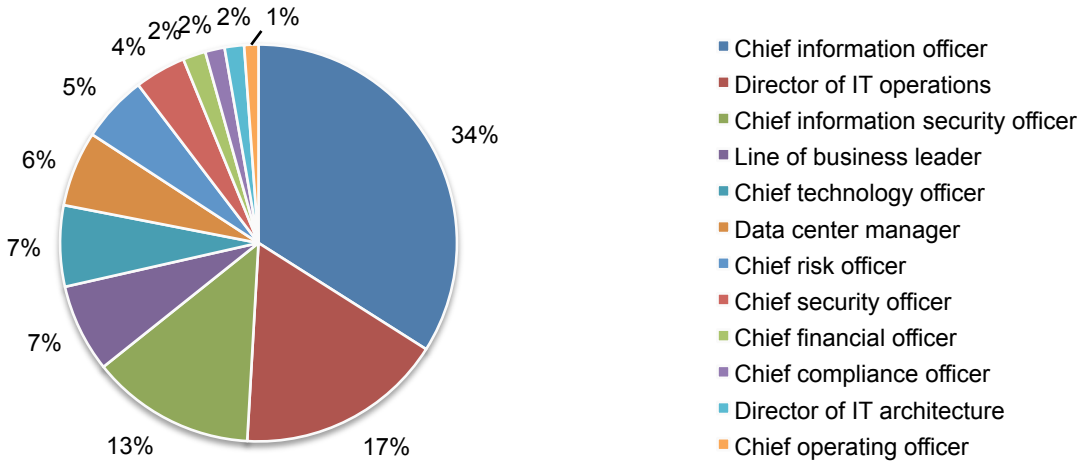
Part 3. Methods

A sampling frame composed of 29,795 individuals in the U.S. and UK who hold such positions as chief information officer, director of IT operations and chief information security officer were selected as participants in this study. To ensure a quality response, only individuals who are knowledgeable about their companies' use of cloud services participated in the research. Table 1, identifies 1,123 respondents completed the survey. Screening removed 133 surveys. The final sample was 990 surveys (or a 3.3 percent response).

Table 1. Sample response	Consolidated
Total sampling frame	29,795
Total returns	1,123
Rejected or screened surveys	133
Final sample	990
Response rate	3.3%

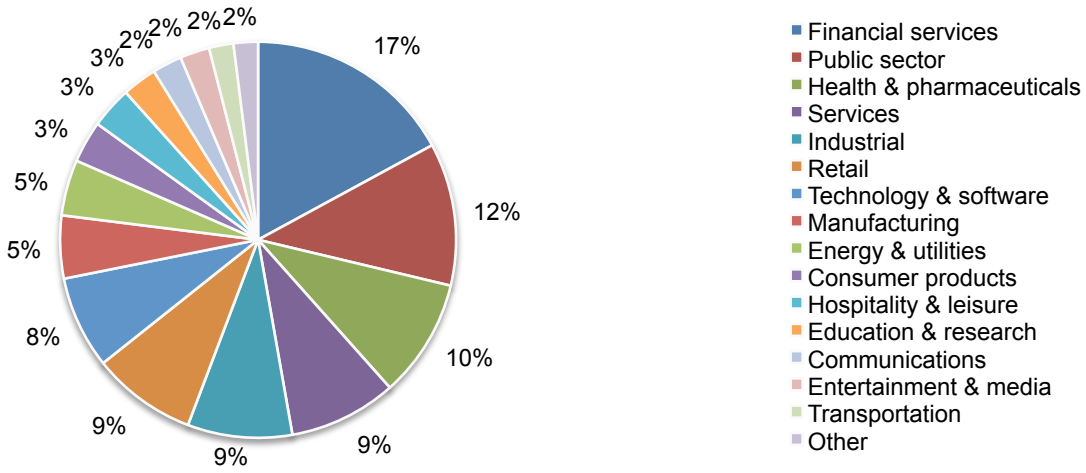
Pie Chart 1 reports the organizational role that best describes the respondent's current position. Thirty-four percent of respondents indicated CIO as their current role. This is followed by 17 percent who responded director of IT operations.

Pie Chart 1. Current organizational role



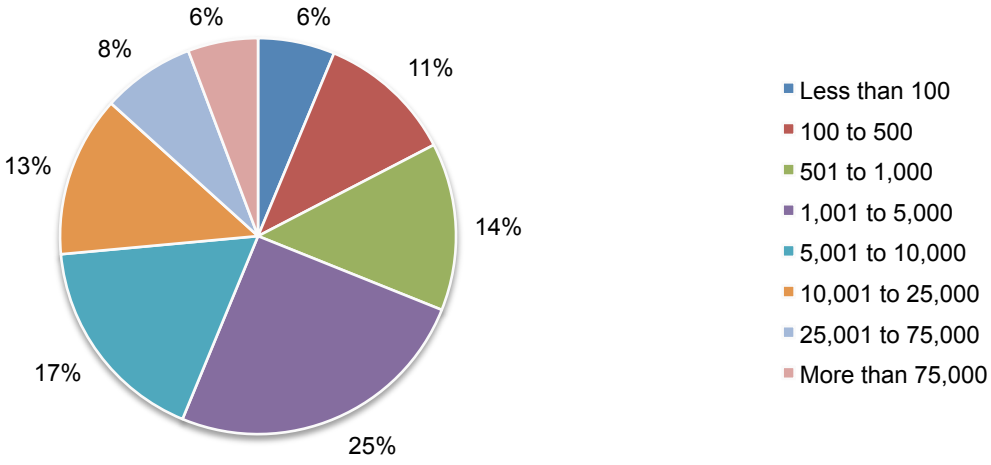
Pie Chart 2 reports the primary industry focus of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by public sector (12 percent), and health and pharmaceuticals (10 percent).

Pie Chart 2. Primary industry focus



According to Pie Chart 3, more than half of the respondents (69 percent) are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 3. Worldwide headcount of the organization



Part 4. Caveats

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 knowledgeable about their companies' use of cloud services and are located in various organizations in the United States and United Kingdom. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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 2015.

Survey response	Combined
Total sampling frame	29795
Total returns	1123
Rejected or screened surveys	133
Final sample	990
Response rate	3.3%
Sample weights	100%

Part 1. Screening

S1. What best describes your organization's use of cloud services and infrastructure?	Combined
Heavy use	38%
Moderate use	44%
Light use	18%
No use (stop)	0%
Total	100%

S2. Does your organization process business-critical applications in the cloud environment?	Combined
Yes	100%
No (stop)	0%
Total	100%

S3. Does your organization process and/or store sensitive or confidential business data in the cloud environment?	Combined
Yes	100%
No (stop)	0%
Total	100%

S4. What best describes your organization's primary approach to cloud deployment? Please check one.	Combined
Use mostly public clouds	58%
Use mostly private clouds	19%
Use a combination of public and privacy clouds (hybrid)	23%
Unsure (stop)	0%
Total	100%

Part 2. Attributions

Please use the scale provided below each statement to express your opinions about the security of cloud resources used by your organization.	
Q1a. My organization assesses the affect the cloud may have on the ability to protect and secure confidential or sensitive information.	Combined
Strongly agree	18%
Agree	24%
Unsure	17%
Disagree	31%
Strongly disagree	10%
Total	100%

Q1b. My organization only uses cloud services that are thoroughly vetted for security risks.	Combined
Strongly agree	15%
Agree	22%
Unsure	24%
Disagree	30%
Strongly disagree	8%
Total	100%

Q1c. My organization is vigilant in conducting audits or assessments of cloud resources before deployment.	Combined
Strongly agree	17%
Agree	22%
Unsure	22%
Disagree	32%
Strongly disagree	7%
Total	100%

Q1d. My organization limits the use and/or storage of sensitive and confidential data in the cloud.	Combined
Strongly agree	23%
Agree	29%
Unsure	21%
Disagree	21%
Strongly disagree	6%
Total	100%

Q1e. My organization is vigilant in ensuring cloud usage does not violate privacy and/or data protection regulations.	Combined
Strongly agree	19%
Agree	23%
Unsure	21%
Disagree	27%
Strongly disagree	10%
Total	100%

Q1f. My organization's top security objective includes meeting or exceeding regulatory requirements.	Combined
Strongly agree	12%
Agree	20%
Unsure	20%
Disagree	35%
Strongly disagree	14%
Total	100%

Q1g. My organization is willing to pay a premium to ensure the security of sensitive or confidential data in the cloud.	Combined
Strongly agree	17%
Agree	27%
Unsure	20%
Disagree	28%
Strongly disagree	8%
Total	100%

Part 3. Cloud Experience

Software as a service (SaaS) is software deployment whereby a provider licenses an application to customers for use as a service on demand. SaaS software vendors may host the application on their own web servers or upload the application to the consumer device, disabling it after use or after the on-demand contract expires.

Q2a. Does your organization use SaaS resources from cloud providers?	Combined
Yes	87%
No	10%
Unsure	2%
Total	100%

Q2b. If yes, how many different SaaS providers does your organization use in the normal course of business?	Combined
1	2%
2 to 5	22%
6 to 10	32%
11 to 25	26%
More than 25	18%
Total	100%
Extrapolated value	13.30

Q2c. If yes, what percent of your organization's business-critical applications uses SaaS versus conventional software applications?	Combined
Less than 10%	17%
10% to 25%	34%
26% to 50%	30%
51% to 75%	12%
76% to 100%	6%
Total	100%
Extrapolated value	32%

Q2d. In your opinion, who is most responsible for ensuring the security of SaaS applications used within your organization?	Combined
End-users are most responsible	20%
IT is most responsible	18%
IT security is most responsible	15%
The cloud provider is most responsible	31%
Responsibility is shared between my company and the cloud provider	16%
Total	100%

Q2e. How important is the use of SaaS in meeting your organization's IT objectives?	
Q2e-1. Today	Combined
Very important	32%
Important	47%
Not important	20%
Irrelevant	1%
Total	100%

Q2e-2. Over the next 2 years	Combined
Very important	44%
Important	46%
Not important	9%
Irrelevant	1%
Total	100%

Q2f. How confident are you that SaaS applications used within your organization are secure? Please use the following 10-point scale from 1 = no confidence to 10 = very high confidence.	Combined
1 or 2	23%
3 or 4	22%
5 or 6	18%
7 or 8	19%
9 or 10	19%
Total	100%
Extrapolated value	5.28

Q2g. How confident are you that SaaS applications used by your organization are compliant with all applicable privacy and/or data protection regulations? Please use the following 10-point scale from 1 = no confidence to 10 = very high confidence.	Combined
1 or 2	25%
3 or 4	22%
5 or 6	19%
7 or 8	18%
9 or 10	15%
Total	100%
Extrapolated value	5.01

Q2h. Are SaaS applications evaluated for security prior to deployment within your organization?	Combined
Yes	44%
No	44%
Unsure	12%
Total	100%

Infrastructure as a Service (IaaS) is the delivery of a computer infrastructure as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service. The service is typically billed on a utility computing basis and the amount of resources consumed (and therefore the cost) will typically reflect the level of activity.	
Q3a. Does your organization use IaaS resources from cloud providers?	Combined
Yes	50%
No	40%
Unsure	10%
Total	100%

Q3b. If yes, how many different IaaS providers does your organization use in the normal course of business?	Combined
1	9%
2 to 5	47%
6 to 10	36%
11 to 25	7%
More than 25	1%
Total	100%

Extrapolated value	6.11

Q3c. If yes, what percent of your organization's business-critical resources utilizes IaaS versus on-premises infrastructure services?	Combined
Less than 10%	33%
10% to 25%	29%
26% to 50%	25%
51% to 75%	12%
76% to 100%	0%
Total	100%
Extrapolated value	25%

Q3d. In your opinion, who is most responsible for ensuring the security of IaaS resources used within your organization?	Combined
End-users are most responsible	33%
IT is most responsible	23%
IT security is most responsible	16%
The cloud provider is most responsible	17%
Responsibility is shared between my company and the cloud provider	11%
Total	100%

Q3e. How important is the use of IaaS in meeting your organization's IT and data processing objectives?	
Q3e-1. Today	Combined
Very important	30%
Important	35%
Not important	30%
Irrelevant	4%
Total	100%

Q3e-2. Over the next 2 years	Combined
Very important	34%
Important	35%
Not important	28%
Irrelevant	3%
Total	100%

Q3f. How confident are you that IaaS resources used within your organization are secure? Please use the following 10-point scale from 1 = no confidence to 10 = very high confidence.	Combined
1 or 2	29%
3 or 4	22%
5 or 6	19%
7 or 8	21%
9 or 10	9%
Total	100%
Extrapolated value	4.66

Q3g. How confident are you that IaaS resources used by your organization are compliant with all applicable privacy and/or data protection regulations? Please use the following 10-point scale from 1 = no confidence to 10 = very high confidence.	Combined
1 or 2	29%
3 or 4	22%
5 or 6	18%
7 or 8	18%
9 or 10	12%
Total	100%

Extrapolated value	4.74

Q3h. Are IaaS resources evaluated for security prior to deployment within in you organization?	Combined
Yes	41%
No	43%
Unsure	16%
Total	100%

Q4. What are the primary reasons why cloud resources are used within your organization? Please select only two choices.	Combined
Reduce cost	56%
Increase efficiency	46%
Improve security	8%
Improve compliance	10%
Improve availability	18%
Faster deployment time	23%
Increase flexibility and choice (agility)	28%
Improve customer service	11%
Total	200%

Q5. How confident are you that your IT organization knows all cloud services and infrastructure in use today? Please use the following 10-point scale from 1 = no confidence to 10 = very high confidence.	Combined
1 or 2	30%
3 or 4	37%
5 or 6	13%
7 or 8	11%
9 or 10	8%
Total	100%
Extrapolated value	4.10

Q6. Which individuals or functions within your organization are responsible for ensuring cloud providers are adequately vetted and secured? Please only select the top two choices.	Combined
Cloud user	40%
Business unit (LOB)	29%
Corporate IT	22%
Compliance	14%
Legal	3%
Procurement	43%
Information security	17%
Data center management	10%
No one person or function is responsible	22%
Other (please specify)	0%
Total	200%

Q7. Which individuals or functions within your organization are responsible for ensuring cloud providers are in compliance with all applicable privacy and data protection regulations? Please only select the top two choices.	Combined
Cloud user	29%
Business unit (LOB)	25%
Corporate IT	22%
Compliance	33%
Legal	15%
Procurement	30%
Information security	17%
Data center management	5%
No one person or function is responsible	23%
Other (please specify)	0%
Total	200%

Q8. What types of confidential or sensitive information does your organization consider too risky to be processed and/or stored in the cloud?	Combined
Consumer data	4%
Customer information	11%
Payment information	31%
Login and authentication information	25%
Employee records	47%
Health information	62%
Non-financial confidential business information	39%
Financial business information	35%
Intellectual property such as source code, design plans, architectural renderings	56%
Research data (including Big Data)	25%
Other (please specify)	4%
None of the above	30%
Total	370%

Q9. What types of business applications does your organization consider too risky to be processed and housed in the cloud?	Combined
Customer relationship management (CRM)	14%
Document and file sharing	16%
Email communications	15%
Enterprise resource planning (ERP)	36%
Finance and accounting	31%
Human resource and payroll	42%
Sales force automation	11%
IT security applications	32%
Logistics & manufacturing applications	29%
Industrial control systems	50%
None of the above	43%
Other (please specify)	1%
Total	321%

Q10a. Do any of your organization's cloud providers operate in locations outside your home country (US or UK)?	Combined
Yes	52%
No	28%
Unsure	20%
Total	100%

Q10b. If yes, does the fact that your organization's data may be located offshore create any regulatory compliance issues?	Combined
Yes	40%
No	51%
Unsure	8%
Total	100%

Q11a. Do any of your organization's cloud providers provide security as a premium service?	Combined
Yes	37%
No	50%
Unsure	13%
Total	100%

Q11b. If yes, how much does your organization pay above base fees to obtain premium security services in the cloud environment? Please express your answer in percentage terms.	Combined
We don't buy these services	44%
Less than 10%	18%
10% to 25%	16%
26% to 50%	12%
51% to 75%	9%
76% to 100%	2%
Total	100%
Extrapolated value	16%

Q12a. Does your organization have a cloud deployment strategy?	Combined
Yes	53%
No	35%
Unsure	12%
Total	100%

Q12b. If yes, does this deployment strategy include the use of security technologies resident in the cloud environment?	Combined
Yes	36%
No	52%
Unsure	12%
Total	100%

Q13a. Does your organization have regulated data in the cloud?	Combined
Yes	48%
No	42%
Unsure	10%
Total	100%

Q13b. If yes, does it increase concerns about regulatory inspections?	Combined
Yes	49%
No	43%
Unsure	8%
Total	100%

Q14a. Does your organization have the ability to inspect data in the cloud?	Combined
Yes	22%
No	63%
Unsure	15%

Total	100%

Q14b. if yes, how frequently does your organization inspect this data?	Combined
Very frequently	2%
Frequently	5%
Not frequently	23%
Rarely	36%
Never	34%
Total	100%

Q15. What privacy and data protection regulations does your cloud provider ensure compliance? Please select all that apply.	Combined
HIPAA	
GLBA	
FERPA	
PCI DSS	
NIST	
FERC CIP	
US state data breach regulations	
Country-level data protection authorities	
Total	

Q16a. Following are security objectives in the on-premise IT environment. Each percentage represents the confident and very confident response (combined from a 4-point scale).	Combined
Access to highly qualified IT security personnel	56%
Achieve compliance with leading self-regulatory frameworks including PCI DSS, ISO, NIST, etc.	43%
Comply with all legal requirements	29%
Conduct independent audits	56%
Conduct training and awareness for all users	58%
Control all live data used in development	29%
Determine the root cause of cyber attacks	48%
Encrypt sensitive or confidential information assets whenever feasible	52%
Enforce security policies	70%
Ensure disaster recovery and business continuity processes are effective	54%
Ensure security governance is effective	60%
Ensure security program is adequately managed	62%
Identify and authenticate users before granting access to information assets or IT infrastructure	56%
Know where information assets are physically located	41%
Limit physical access to IT infrastructure	70%
Monitor traffic intelligence	58%
Perform patches to software promptly	55%
Prevent or curtail data loss or theft	60%
Prevent or curtail external attacks	57%
Prevent or curtail internal attacks	72%
Prevent or curtail system downtime and business interruption	57%
Prevent or curtail system-level connections from insecure endpoints	76%
Prevent or curtail viruses and malware infection	81%
Secure endpoints to the network	65%
Secure sensitive or confidential information at rest	60%
Secure sensitive or confidential information in motion	58%
Secure vendor relationships before sharing information assets	38%
Average confidence level	56%

Q16b. Following are security objectives in the cloud environment. Each percentage represents the confident and very confident response (combined from a 4-point scale).	Combined
Access to highly qualified IT security personnel	34%
Achieve compliance with leading self-regulatory frameworks including PCI DSS, ISO, NIST, etc.	32%
Comply with all legal requirements	23%
Conduct independent audits	36%
Conduct training and awareness for all users	48%
Control all live data used in development	18%
Determine the root cause of cyber attacks	44%
Encrypt sensitive or confidential information assets whenever feasible	37%
Enforce security policies	18%
Ensure disaster recovery and business continuity processes are effective	27%
Ensure security governance is effective	26%
Ensure security program is adequately managed	27%
Identify and authenticate users before granting access to information assets or IT infrastructure	53%
Know where information assets are physically located	15%
Limit physical access to IT infrastructure	16%
Monitor traffic intelligence	36%
Perform patches to software promptly	22%
Prevent or curtail data loss or theft	42%
Prevent or curtail external attacks	44%
Prevent or curtail internal attacks	25%
Prevent or curtail system downtime and business interruption	35%
Prevent or curtail system-level connections from insecure endpoints	28%
Prevent or curtail viruses and malware infection	76%
Secure endpoints to the network	46%
Secure sensitive or confidential information at rest	25%
Secure sensitive or confidential information in motion	36%
Secure vendor relationships before sharing information assets	17%
Average confidence level	33%

Q17a. Please review the following list of 23 IT security solutions that may be deployed by your organization today. Please check the top 7 solutions that your organization needs to secure data, applications and IT infrastructure.	Combined
Access governance systems	23%
Advance firewalls (NGFW/UTM)	38%
Anti-virus & anti-malware	38%
Code debugging	11%
Data loss prevention (DLP)	28%
Database scanning	32%
Security intelligence & event management (SIEM)	59%
Encryption for data at rest	49%
Encryption for data in motion	49%
Encryption for wireless communication	7%
Endpoint security management	25%
Web application firewalls (WAF)	21%
Identity & access management	58%
ID credentialing system	7%
Intrusion detection or prevention (IDS/IPS)	42%
Log management	19%
Security patch management	15%
Perimeter or location surveillance	8%
Sandbox or isolation tools	27%
Dual factor authentication	40%
Single sign-on (SSO)	35%
Employee (behavioral) monitoring	42%
Virtual private network (VPN)	25%
Total	700%

Q17b. Please check the IT security solutions available from your cloud vendor(s).	Combined
Access governance systems	6%
Advance firewalls (NGFW/UTM)	17%
Anti-virus & anti-malware	84%
Code debugging	5%
Data loss prevention (DLP)	22%
Database scanning	68%
Security intelligence & event management (SIEM)	39%
Encryption for data at rest	49%
Encryption for data in motion	41%
Encryption for wireless communication	2%
Endpoint security management	9%
Web application firewalls (WAF)	19%
Identity & access management	58%
ID credentialing system	0%
Intrusion detection or prevention (IDS/IPS)	54%
Log management	40%
Security patch management	46%
Perimeter or location surveillance	1%
Sandbox or isolation tools	23%
Dual factor authentication	31%
Single sign-on (SSO)	14%
Employee (behavioral) monitoring	7%
Virtual private network (VPN)	24%
Total	659%

Q18. Please review the following list of 13 control activities that may be deployed by your organization to secure data, applications and IT infrastructure. Please check the activities available from your cloud vendor(s).	Combined
Certifications (such as SOC 2/3, PCI DSS, ISO, NIST, HIPPA and others)	45%
Controls assessment	8%
Cyber incident response team	28%
External audit	16%
Helpdesk	71%
IT audit	8%
Monitoring regulatory requirements	12%
Policies and procedures	27%
Quality assurances	5%
Redress and enforcement	9%
Training & certification of data handlers	34%
Vetting and monitoring of third parties	24%
Workplace surveillance	6%
Total	294%

Q19. Are members of your organization's security operations team involved in evaluating cloud service providers?	Combined
Always	10%
Most of the time	14%
Some of the time	14%
Rarely	42%
Never	20%
Total	100%

Q20. How important is security to your organization's cloud migration decision?	Combined
Always	34%
Most of the time	45%
Some of the time	13%
Rarely	8%
Never	1%
Total	100%

Q21. How important is compliance to your organization's cloud migration decision?	Combined
Always	37%
Most of the time	37%
Some of the time	20%
Rarely	6%
Never	0%
Total	100%

Part 5. Organization & Respondent Demographics

D1. What organizational role best defines your current position?	Combined
Chief executive officer	0%
Chief operating officer	1%
Chief financial officer	2%
Chief information officer	34%
Chief technology officer	7%
Chief information security officer	13%
Chief security officer	4%
Chief compliance officer	2%
General counsel	0%
Director of internal audit	0%
Chief risk officer	5%
Director of IT infrastructure	0%
Director of IT architecture	2%
Director of IT operations	17%
Data center manager	6%
Line of business leader	7%
Other	0%
Total	100%

D2. What industry best describes your company's industry concentration or focus?	Combined
Agriculture & food services	1%
Communications	2%
Consumer products	3%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	17%
Health & pharmaceuticals	10%
Hospitality & leisure	3%
Industrial	9%
Manufacturing	5%
Public sector	12%
Retail	9%
Services	9%
Technology & software	8%
Transportation	2%
Other	0%
Total	100%

D3. What is the worldwide headcount of your company?	Combined
Less than 100	6%
100 to 500	11%
501 to 1,000	14%
1,001 to 5,000	25%
5,001 to 10,000	17%
10,001 to 25,000	13%
25,001 to 75,000	8%
More than 75,000	6%
Total	100%

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.