The Security of Cloud Infrastructure

Survey of U.S. IT and Compliance Practitioners

Sponsored by Vormetric

Independently conducted by Ponemon Institute LLC

Publication Date: November 2011

The Security of Cloud Infrastructure

Survey of U.S. IT and Compliance Practitioners
Ponemon Institute, November 2011

Part 1: Introduction

Ponemon Institute is pleased to present the results of The Security of Cloud Infrastructure. This research was conducted to determine how organizations manage the inherent data security risks associated with IT infrastructure services provided by public or hybrid cloud providers. Our study surveyed IT operations, IT security and compliance practitioners. The findings reveal the gulf between those working in IT and those in compliance about service provider controls, top security measures and roles and responsibilities.

Sponsored by Vormetric, the study's goal is to learn how organizations resolve (or fail to resolve) the tradeoff between cloud efficiencies and IT security. The tension in cloud deployment seems to revolve around the assumption that cloud services are less secure than on-premise computing but the benefits seem to be perceived as outweighing the risks to sensitive and confidential data. This tension is especially acute for cloud infrastructure services. This is the fourth study conducted by Ponemon Institute on security and governance issues in cloud infrastructure services.[1]

The study surveyed 613 IT and IT security practitioners and 405 individuals who work in compliance, privacy, data protection and other related fields in the United States. The total sample size is 1,018. Respondents were asked to self-report if they are familiar with cloud computing and if their organizations use cloud computing services. Only those individuals who are familiar with cloud computing were included in this sample.

IT & IT security respondents (hereafter referred to as IT practitioners) have an average of approximately 10 years of experience in their field and the respondents in compliance have an average of 11 years of experience. More than half (57 percent) of the IT practitioners and 73 percent of the compliance respondents are at the supervisor or higher level. Seventy percent of IT and 66 percent of compliance practitioners work in organizations with a headcount of more than 2,000 employees.

We believe this study is important because it provides insights on how IT and compliance practitioners are at odds on some issues involving data security in the cloud. The following are the main differences:

- Only one-third of IT security respondents think IaaS environments are as secure as on premise data centers. However, half of compliance respondents think IaaS is as secure.
- A higher percentage (42 percent) of compliance respondents believe their organizations have adequate technologies to secure their IaaS environments. Only 35 percent of IT respondents think this is the case.
- IT respondents believe encryption should be used to make data unreadable by cloud services providers. However, compliance practitioners believe encryption should be used to enforce separation of duties that prevent IT administrators from accessing data they do not need in order to perform their work.

---

[1]See the following Ponemon Institute research reports:
Flying Blind in the Cloud: The State of Information Governance Ponemon Institute April 2010
Security of Cloud Computing Users Ponemon Institute, May 2010
Security of Cloud Computing Providers Ponemon Institute April 2011

- Twenty-one percent of compliance officers say they are responsible for defining security requirements in the cloud and 22 percent of IT respondents believe business unit leaders are responsible for defining security requirements in the cloud. However, both groups agree that business unit leaders are responsible for enforcing cloud security requirements and no one role is responsible for implementing security in the cloud.

Other salient findings from this study are:

- **The budget for cloud computing is increasing**. On average, approximately 20 percent of the IT budget in organizations participating in this study is allocated to cloud services. However, this is expected to increase to approximately 31 percent over the next 12 to 24 months.

- **Security concerns do not seem to prevent moving to the cloud**. More than half (56 percent) of IT practitioners say that security concerns will not keep their organizations from adopting cloud services.

- **Data in the IaaS cloud environment is perceived to be as a greater security risk**. SaaS is considered by both groups to be more secure.

- **Unstructured data is considered most important to store in the cloud infrastructure environment**. Such data includes files, documents and emails.

- **Internal audit is not included in cloud security issues**. More than half of respondents say their organization's internal audit review does not provide feedback about the security in cloud infrastructure.

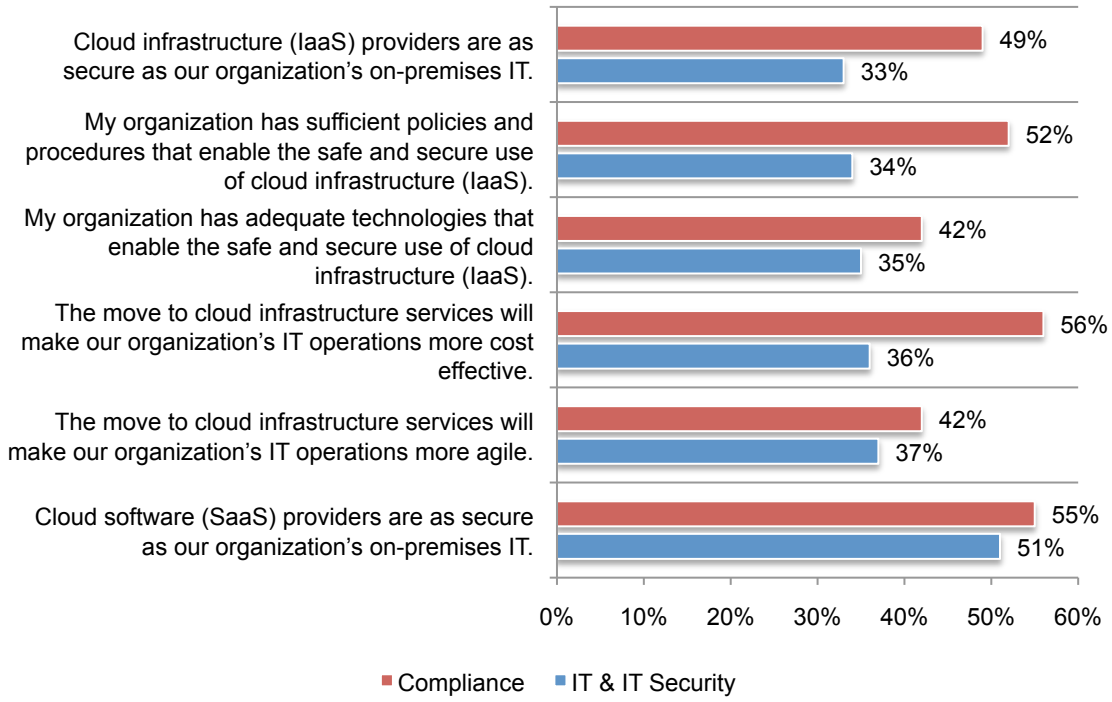
- **Encryption is not widely used by cloud providers**. Only 31 percent say their organization's major cloud provider(s) use encryption to protect data from insider threats.

- **Majority of organizations in our study use similar enabling technologies**. Firewalls, anti-virus/anti-malware and identity and access management are the technologies and controls organizations have in place to protect sensitive or confidential information placed into cloud environments.

Part 2. Key Findings

IT respondents are more concerned about security in the cloud than compliance respondents. Bar Chart 1 summarizes the strongly agree and agree response to six attributions concerning cloud security.[2] It shows that more than half of IT and compliance practitioners are likely to agree that cloud software (SaaS) providers are as secure as their organization's on-premises IT (51 and 55 percent, respectively). However, only 33 percent of IT respondents agree that cloud infrastructure (IaaS) providers are as secure as their organization's on-premises IT. In contrast, nearly half of the compliance respondents (49 percent) agree that IaaS providers are as secure as their organization's on-premises IT.

Bar Chart 1. Attributions about cloud security
Strongly agree & agree responses

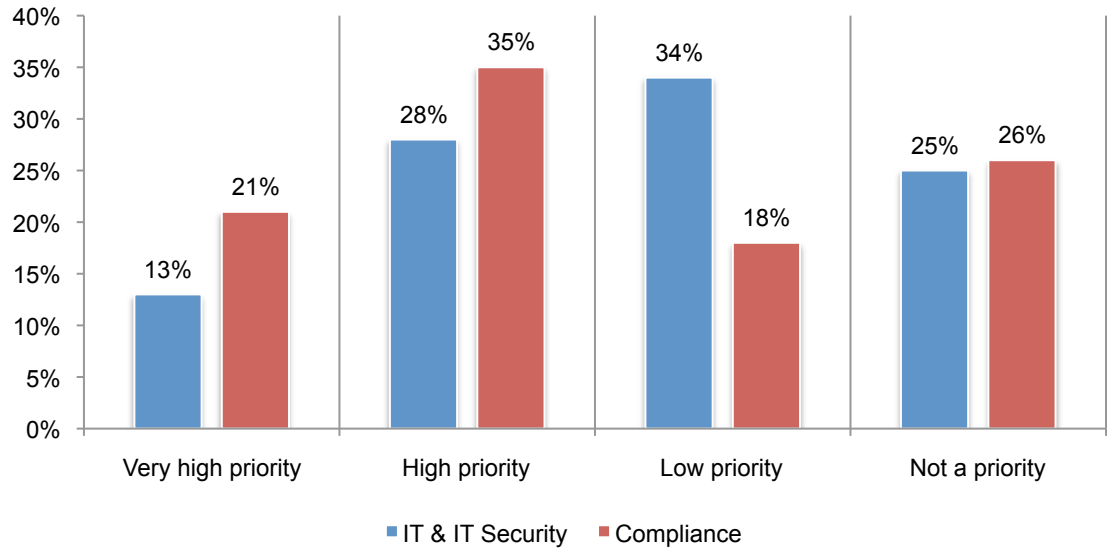


There is also a significant difference in agreement between IT and compliance respondents with respect to whether their organization has sufficient policies and procedures that enable the safe and secure use of cloud infrastructure (IaaS). Accordingly, only 34 percent of IT believe this is the case as opposed to 52 percent of the compliance respondents.

[2]In this paper, we use attributions to capture the perceptions of respondents concerning the security of cloud computing environments. These attributions or statements are evaluated using a five-point adjective scale ranging from strongly agree to strongly disagree. A favorable or affirmative response is defined as a strongly agree or agree response. A negative or non-affirmative response is defined as a strongly disagree, disagree or unsure response.

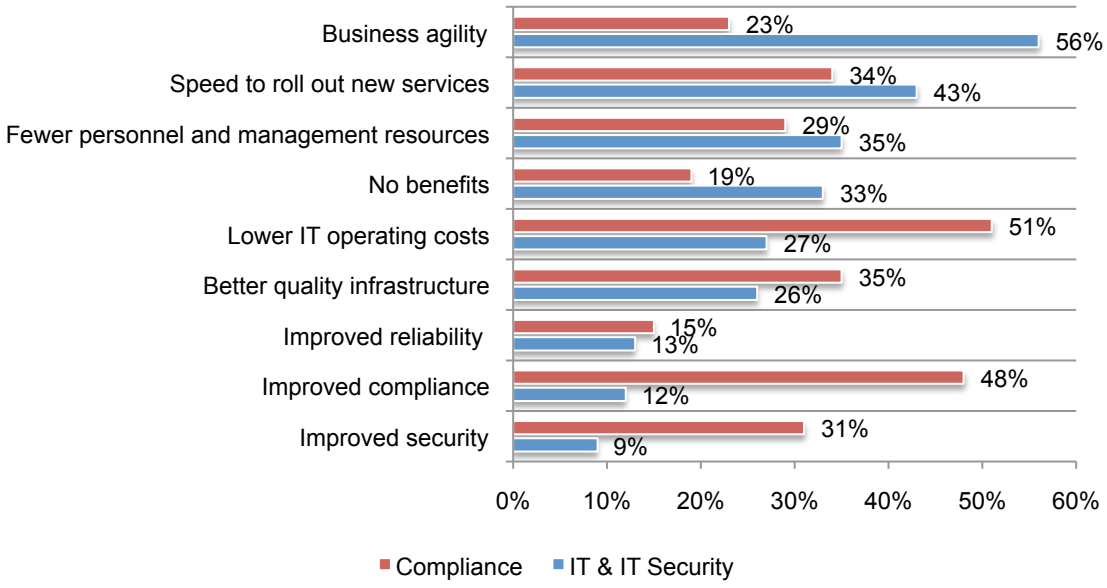
While there are concerns about security, the evaluation of the security of IaaS providers is rated as a low priority or not a priority. Bar Chart 2 shows 59 (34 + 25) percent of IT respondents say that when evaluating IaaS providers, security is a low or not a priority. In contrast, more than half of compliance respondents say security is a very high (21 percent) or high priority (35 percent) when evaluating IaaS providers.

Bar Chart 2. How much of a priority is security when evaluating IaaS providers?



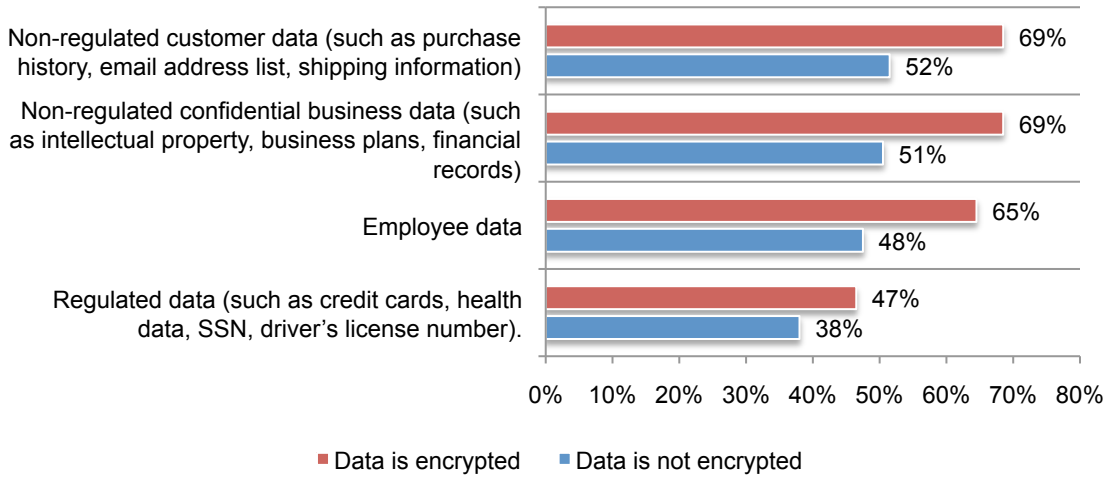
Bar Chart 3 reveals that these two groups see different benefits from using IaaS as opposed to on-premise IT resources. IT respondents believe business agility, speed to roll out new services and fewer personnel and management resources are the main benefits. Compliance respondents believe it is lower operating costs followed by improved compliance and better quality infrastructure are the main benefits. The widest gap or disagreement between these two samples concern improved compliance (Diff = 36 percent) and business agility (Diff = 33 percent).

Bar Chart 3. What benefits does your organization experience by using IaaS?
More than one choice permitted



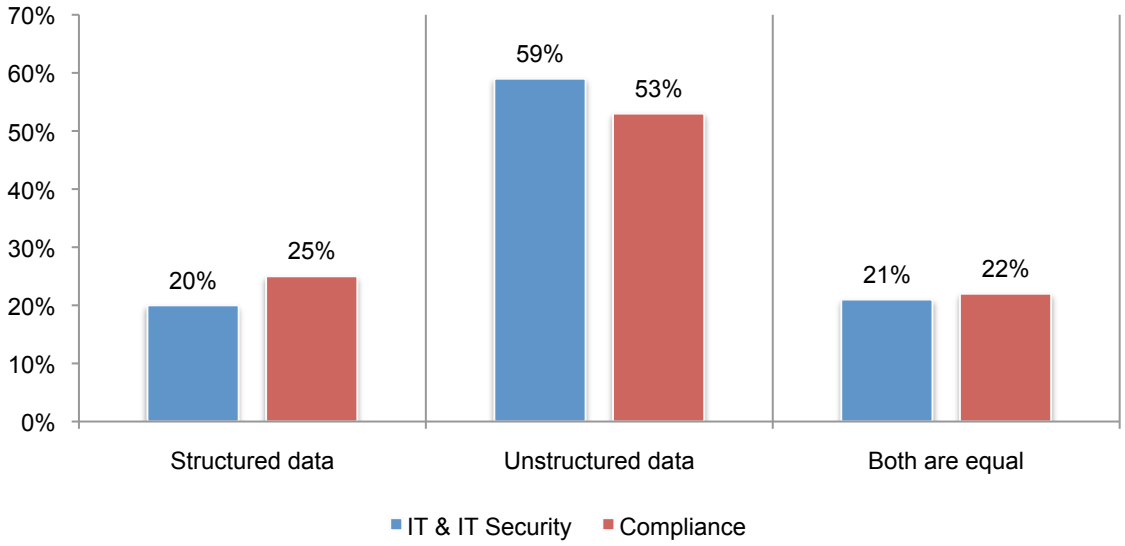
Encryption makes a difference when determining what data types to put in the cloud infrastructure. Bar Chart 4 presents respondents' perceptions about four different data types that may be processed or retained in cloud environments. As can be seen, respondents (IT and compliance practitioners combined) say their organizations are more likely to place non-regulated customer data, non-regulated confidential business data regulated data and employee data in the cloud infrastructure environment if this data was encrypted.

Bar Chart 4. What data types would you place in the cloud infrastructure environment?
IT and compliance samples combined[3]



According to Bar Chart 5, a majority of IT (59 percent) and compliance (53 percent) respondents agree that unstructured data – such as emails, documents, spreadsheets and more – is the type of sensitive data organizations considered most important for storage in cloud infrastructure environments.

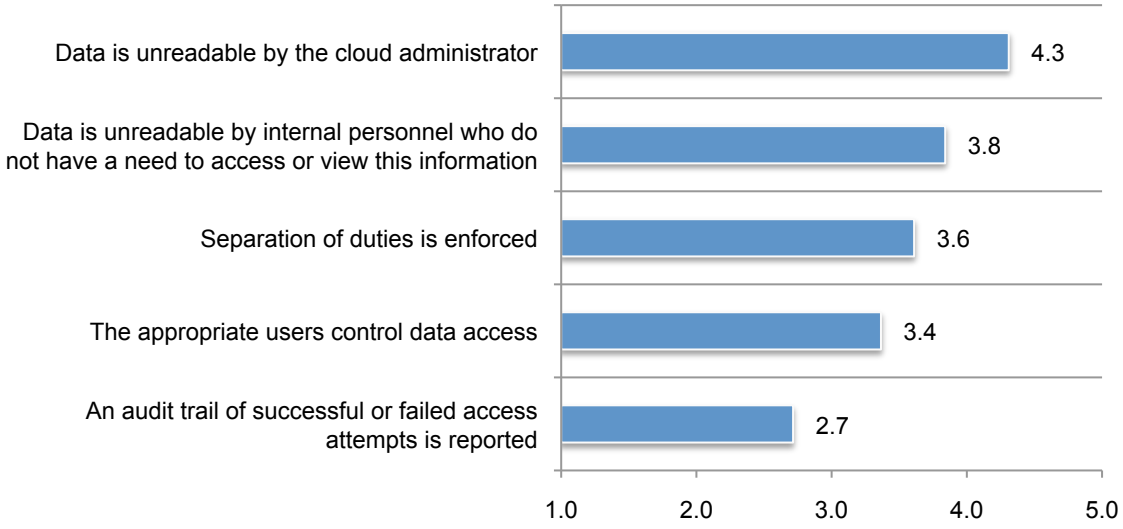
Bar Chart 5. What types of sensitive data does your organization consider most important to store in the cloud infrastructure environment?



[3]To simplify the presentation, we combine the two samples. The Appendix (attached herein) provides the detailed results presented for the IT and compliance samples separately.

The security feature considered most important when placing sensitive data in the cloud infrastructure by both IT and compliance respondents is to make this data unreadable to cloud administrators. Bar Chart 6 shows the average rank order of five security steps or features, wherein each feature is ranked from most important to least important. Clearly, the two top ranked security features concerns making sensitive data unreadable to cloud administrators or other internal personnel who do not have a need to access or view this information.[4]

Bar Chart 6. What are the most important security steps or features when processing or storing sensitive data in the cloud infrastructure environment?
Average rank from 5 = most important to 1 = least important
IT and compliance samples combined[5]

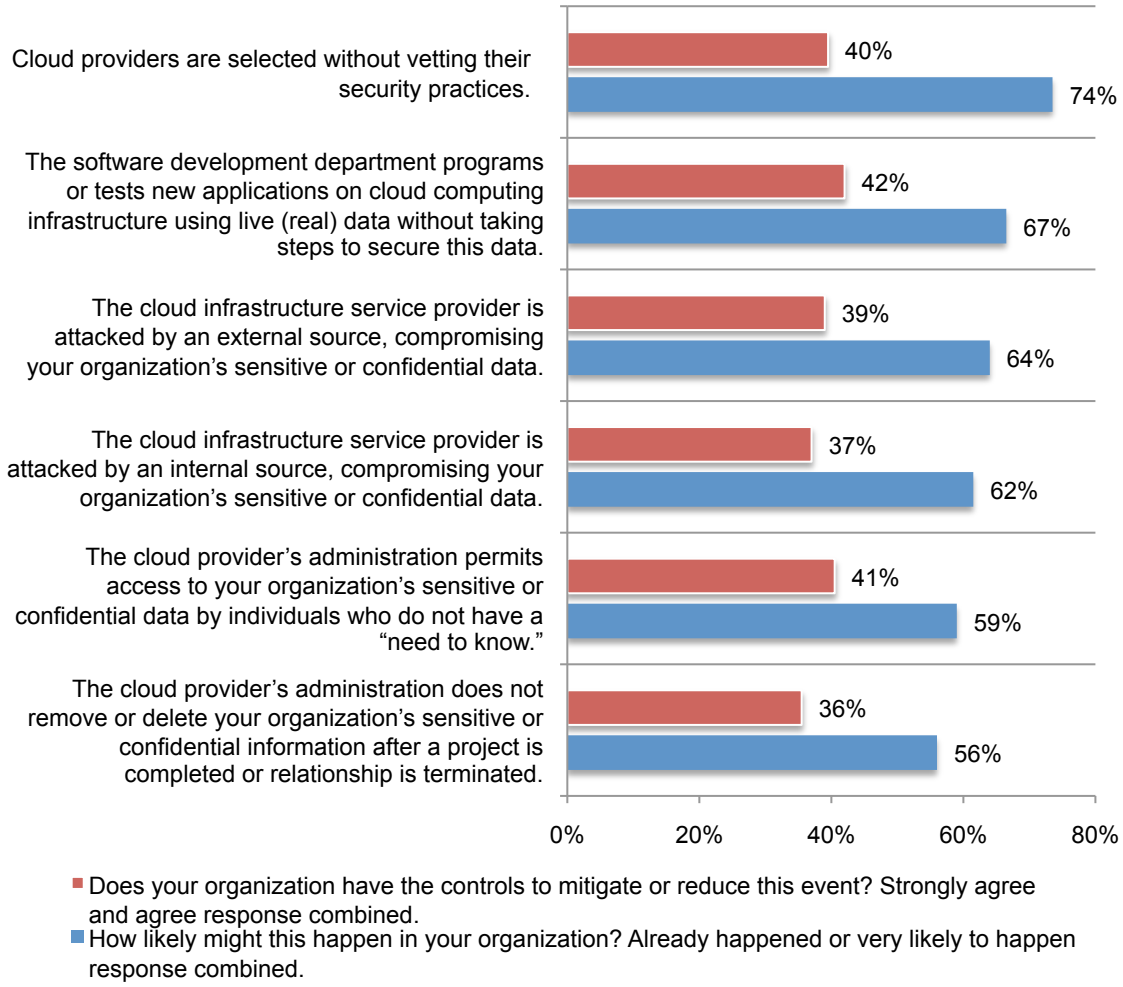


[4]Common methods ways to make data unreadable include masking, field suppression, tokenization and encryption.
[5]Ibid, Footnote 3

Organizations are at risk because of the lack of vetting and monitoring of IaaS providers. As summarized in Bar Chart 7**,** respondents (IT and compliance samples combined) believe their organizations are not proactive in ensuring the security of cloud providers. The majority of IT and compliance practitioners say that cloud providers have been selected or are very likely to be selected without vetting their security practices. Moreover, it appears that most organizations do not have the controls to mitigate or reduce the risk of these negative events.

According to respondents, cloud infrastructure security blunders already occurring or likely to occur include: software testing using live data without sufficient protections or controls (67 percent), the inability to curtail attacks from either external (64 percent) or internal (62 percent) sources, and the cloud administrator's inability to control access to sensitive or confidential data (59 percent). According to 56 percent of respondents, another very likely cloud infrastructure vulnerability is not removing or deleting sensitive or confidential information after a project is completed or the relationship is terminated.

Bar Chart 7. Scenarios about the insecure use of cloud infrastructure services by organizations.
IT and compliance samples combined[6]



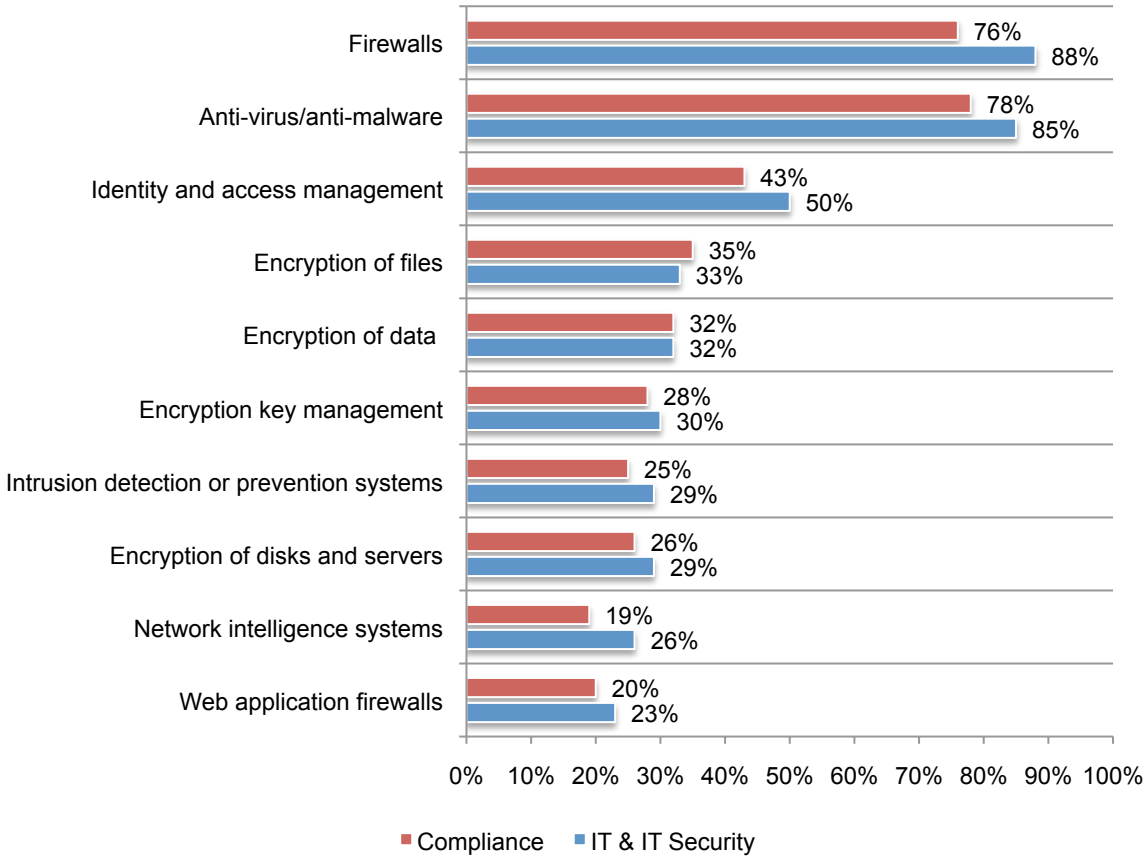
[6]Ibid, Footnote 3

The above bar chart also reports the availability of controls to curtail or mitigate each stated cloud infrastructure vulnerability. As can be seen, a majority of respondents perceive a lack of controls that protect their organizations.

For instance, only 36 percent believe they have sufficient controls to ensure the removal or deletion of their organization's information after a project is completed. Only 37 percent believe they have sufficient controls to protect the organization from malicious insiders and 39 percent say they have sufficient controls to defend against external attackers. Finally, only 41 percent believe they have sufficient controls to ensure cloud administrators restrict access on a "need to know" basis.

The majority of organizations use a similar set of enabling security technologies to protect sensitive or confidential data in the cloud infrastructure environment. Firewalls, anti-virus/anti-malware and identity and access management are the technologies and controls organizations have in place to protect sensitive or confidential data placed into cloud environments, as shown in Bar Chart 8, network intelligence systems and web application firewalls are the least used technologies to protect sensitive or confidential data placed in the cloud infrastructure environment.

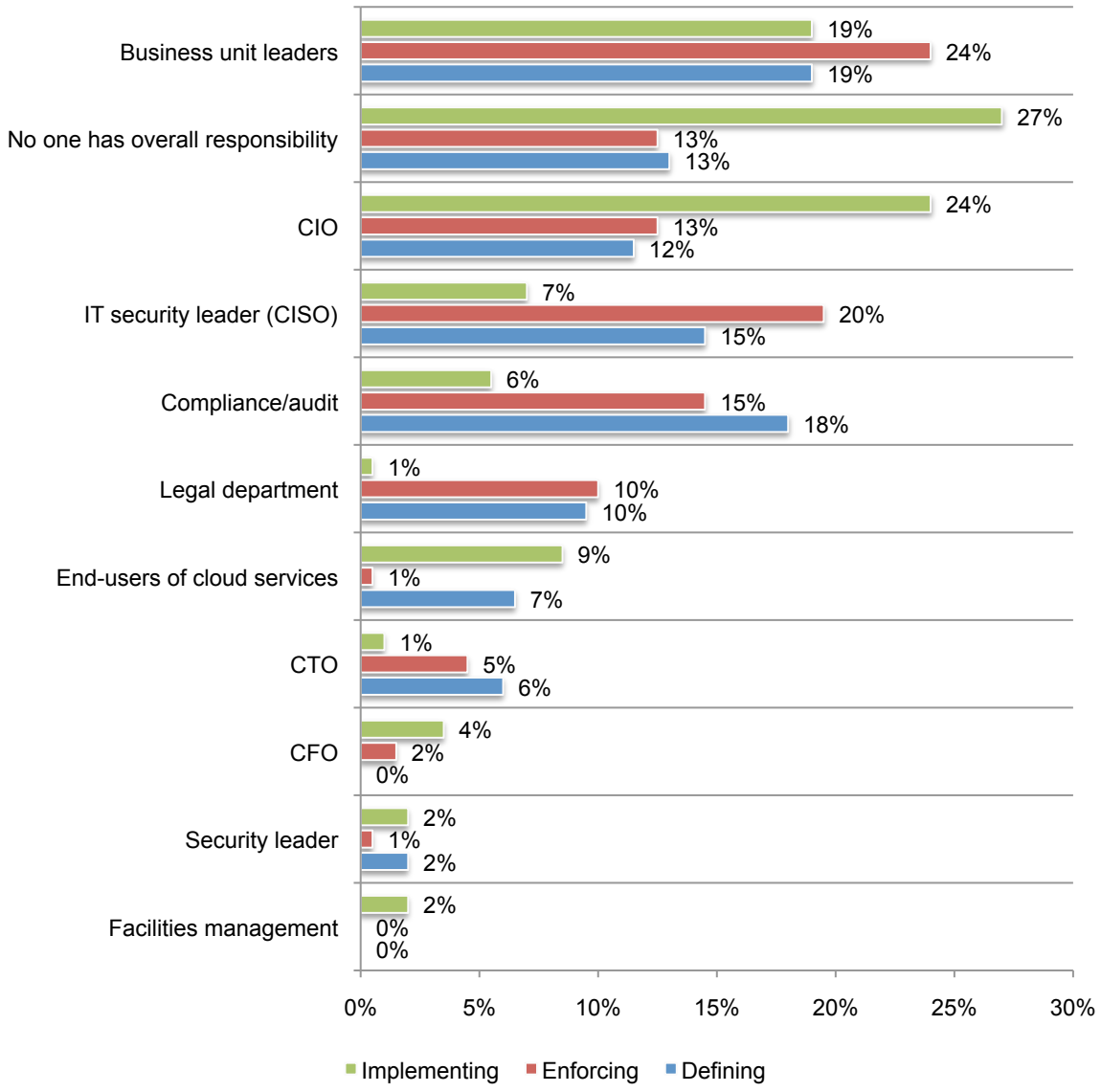
Bar Chart 8. What enabling technologies and controls does your organization have in place to protect sensitive or confidential information placed into cloud environments?
More than one choice permitted



There is no clear function, department or individual responsible for defining, enforcing and implementing security requirements for data in the cloud infrastructure environment. According to Bar Chart 9, only 7 percent of respondents (IT and compliance samples combined) say the IT security leader or CISO is most responsible for implementing the organization's cloud security requirements. Similarly, only 6 percent of respondents see the compliance/audit function as most responsible for implementing requirements. In contrast, 27 percent of respondents say no one person or function has overall responsibility for implementing cloud security requirements.

This bar chart also shows respondents generally agreeing that business unit leaders (24 percent), the CISO (20 percent) or the compliance/audit leader (15 percent) are most responsible for enforcing their organization's cloud security requirements.

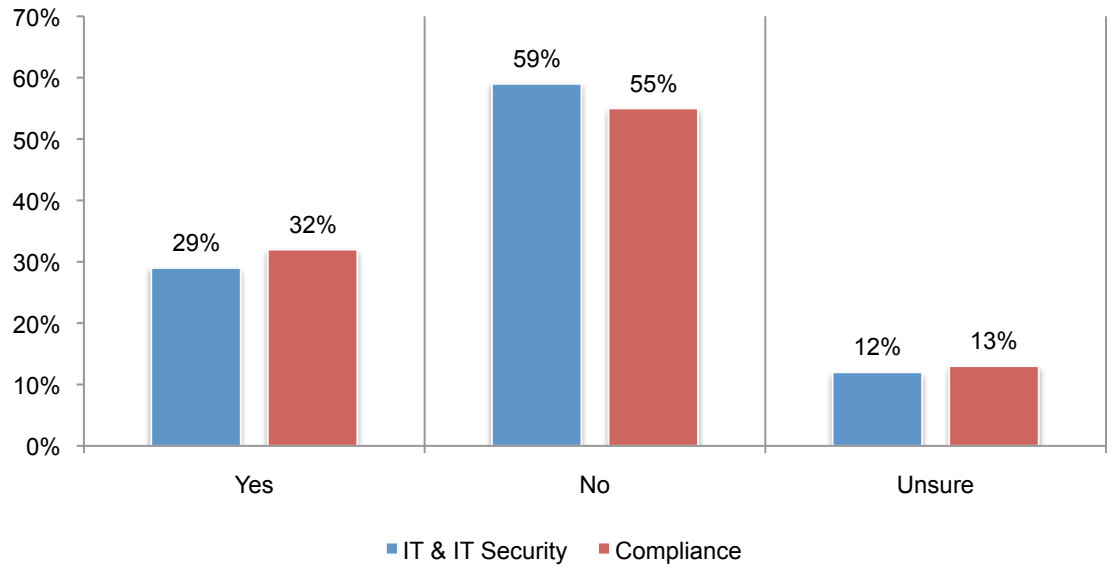
Bar Chart 9. In your organization, who is most responsible for defining, enforcing, and implementing security requirements for data in the cloud infrastructure environment?
IT and compliance samples combined[7]



[7]Ibid, Footnote 3

Internal auditors are not often called upon to review and provide feedback on security in the cloud. Bar Chart 10 reveals that a majority of respondents say their organizations do not use internal audit to review or provide feedback on the security of cloud infrastructure environments where sensitive or confidential information may be deployed.

Bar Chart 10. Does your organization's internal audit review and provide feedback on security in the cloud infrastructure environment?



Part 3. Methods

Table 1 summarizes the sampling response for a web-based survey we conducted over a three-week period concluding in October 2011. A total of 18,750 individuals in the IT and IT security fields as well as 11,569 individuals in various organizational compliance functions[8] were invited to participate in this research. All individuals contacted held bona fide credentials and were located in business or governmental organizations. This resulted in a total return of 718 individuals in the IT and IT security sample and 524 individuals in the compliance sample. After rejecting surveys because of reliability or screening criteria, we achieved final sample sizes of 613 for IT and IT security (3.3 percent response rate) and 405 for compliance (3.5 percent response rate).

Table 1. Sample response	IT & IT Security	Compliance
Sampling frame	18,750	11,569
Total returns	718	524
Rejected surveys	46	26
Sample before screening	672	498
Final sample	613	405
Response rate	3.3%	3.5%

Table 2 summarizes the organizational position of respondents in both the IT and IT security sample and compliance sample. As can be seen, respondents in both samples hold responsible positions. Fifty-seven percent of IT and IT security practitioners self-report they are at or above the supervisory level. Seventy-three percent of compliance practitioners say they are at or above the supervisory level.

Table 2. Respondents' position level	IT & IT Security	Compliance
Senior Executive	1%	0%
Vice President	1%	2%
Director	16%	21%
Manager	21%	32%
Supervisor	18%	18%
Technician	34%	5%
Staff or Administrative	6%	15%
Contractor	2%	4%
Other (please specify)	1%	3%
Total	100%	100%

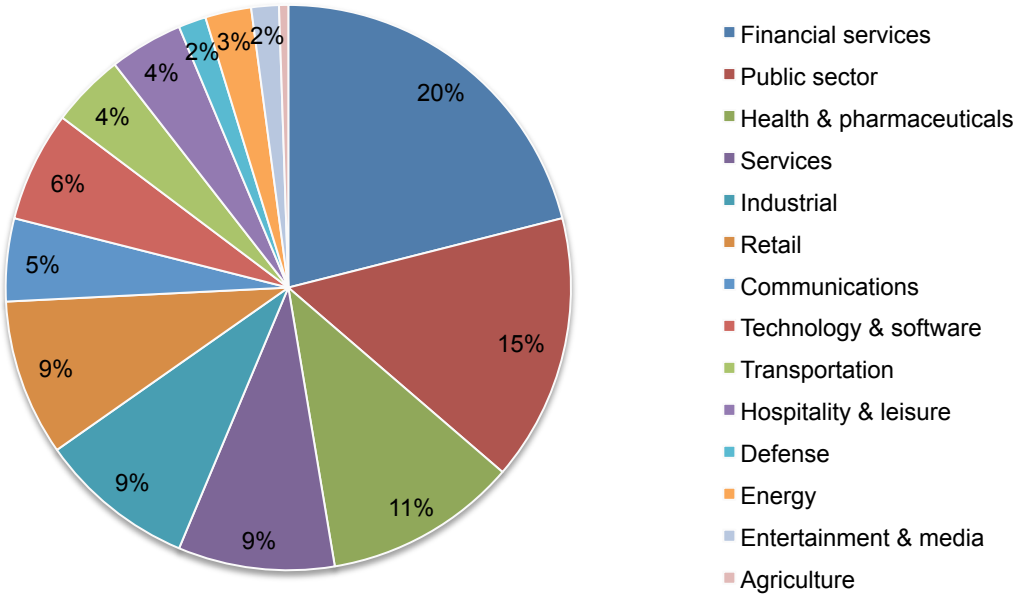
As noted in Table 3, the average years of relevant work experience for IT and IT security practitioners is 9.71 years. The average years of relevant work experience for compliance practitioners is 11.02 years.

Table 3. Respondents' experience in mean years	IT & IT Security	Compliance
Total years of experience	9.71	11.02
Total years in present position	4.15	4.77

[8]The organizational compliance functions in this sample include individuals in IT compliance, quality assurance, privacy and data protection office, corporate compliance, regulatory compliance, legal department and more.

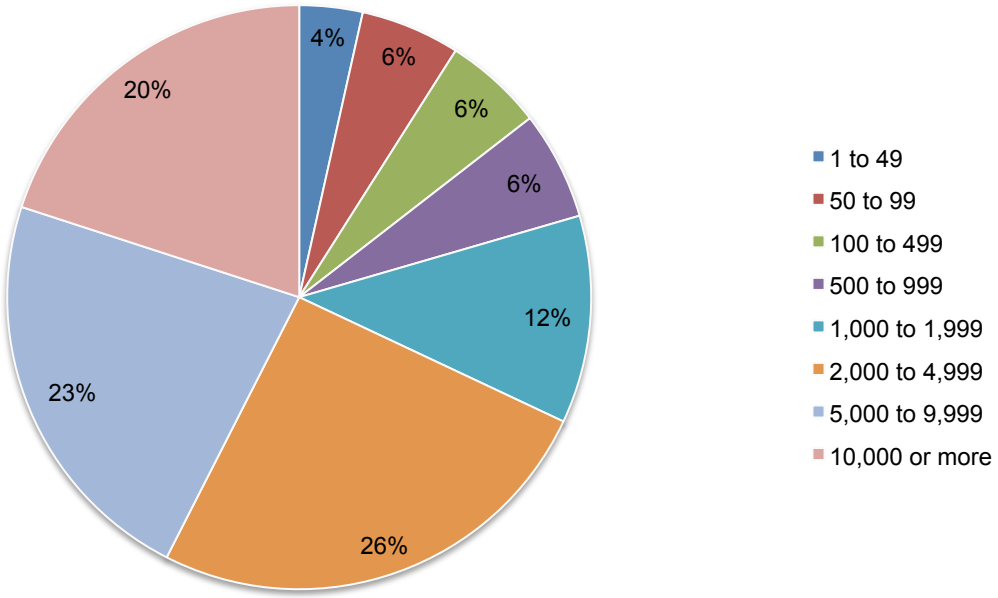
The industry classification of respondents' organizations for both the IT and compliance samples (combined) is reported in Pie Chart 1. As can be seen, financial services represents the largest segment at 20 percent. The second largest segment is public sector at 15 percent. In addition, at 11 percent, the third largest segment concerns health and pharmaceutical companies.

Pie Chart 1. Industry distribution of respondents' organizations
IT and compliance samples combined



As shown in Pie Chart 2, approximately one-third (34 percent) of participating organizations have less than 1,000 employees. In contrast, 43 percent of the combined IT and compliance samples are represented by large organizations with 5,000 or more employees.

Pie Chart 2. Global headcount (size) of respondents' organizations
IT and compliance samples combined



Part 4. Implications and limitations

The study reveals that in many cases, especially with IaaS, there is recognition that there are security risks to sensitive and confidential data stored in a cloud environment. However, the benefits and the desire to migrate to the cloud in organizations seem to outweigh the concerns.

We believe some of the main implications from this research are:

- Security in the cloud is a concern, especially in IaaS environments.
- Encryption is considered one of the most important enabling technologies for securing IaaS clouds.
- Organizations feel they lack adequate technologies to secure their IaaS environments.
- Ownership for security in the cloud is dispersed throughout the organization, making it difficult to implement an enterprise-wide data security strategy.

In summary, we believe this is the first study to survey both IT and compliance practitioners about the security of cloud infrastructure. Despite differences between the IT and compliance samples, we conclude that both groups are concerned about the security of sensitive or confidential data placed in the cloud infrastructure environment.

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 in IT and IT security located in the United States, 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 or perceptions about data protection activities from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the sample is representative of individuals in the IT, IT security and compliance fields. We also acknowledge that the results may be biased by external events.

  We also acknowledge bias caused by compensating respondents to complete this research within a holdout period. 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 certain respondents 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 over a three-week period ending in October 2011.

Sample response	IT	Compliance	Combined
Sampling frame	18,750	11,569	30,319
Total returns	718	524	1,242
Rejected surveys	46	26	72
Sample before screening	672	498	1,170
Final sample	613	405	1,018
Response rate	3.3%	3.5%	3.4%

Part 1. Screening

S1. How familiar are you with cloud computing?	IT	Compliance
Very familiar	176	68
Somewhat familiar	401	219
Not familiar	73	162
No knowledge (stop)	22	49
Total	672	498

S2. Does your organization use cloud-computing services (such as those described in the above definition)?	IT	Compliance
Yes	613	405
No (stop)	59	44
Total	650	449

S3. What best describes your organization's use of cloud computing? Please check one.	IT	Compliance
Mostly public clouds	329	232
Mostly private clouds	126	81
A combination of public and private clouds (hybrid)	158	92
Total	613	405

Part 2. General Questions

Q1. IT: What best describes your organization's use of public cloud computing resources today?	Do not use	Heavy use	Moderate
Software as a service (SaaS)	9%	25%	33%
Infrastructure as a service (IaaS)	18%	9%	30%
Platform as a service (PaaS)	61%	4%	8%

Q1. Compliance: What best describes your organization's use of public cloud computing resources today?	Do not use	Heavy use	Moderate
Software as a service (SaaS)	10%	24%	35%
Infrastructure as a service (IaaS)	21%	7%	33%
Platform as a service (PaaS)	70%	2%	9%

Q2. Please rate the following statements using the scale provided below each item. Strongly agree and agree responses.	IT	Compliance
Q2a. Cloud infrastructure (IaaS) providers are as secure as our organization's on-premises IT.	33%	49%
Q2b. Cloud software (SaaS) providers are as secure as our organization's on-premises IT.	51%	55%
Q2c. My organization has adequate technologies that enable the safe and secure use of cloud infrastructure (IaaS).	35%	42%
Q2d. My organization has sufficient policies and procedures that enable the safe and secure use of cloud infrastructure (IaaS).	34%	52%
Q2e. The move to cloud infrastructure services will make our organization's IT operations more cost effective.	36%	56%
Q2f. The move to cloud infrastructure services will make our organization's IT operations more agile.	37%	42%

Please estimate Q3 and Q4 based on the budget required to meet IT operating needs.

Q3. Today, how much of your IT budget is allocated to cloud services (SaaS, IaaS and PaaS combined)?	IT	Compliance
None	9%	8%
1 to 25%	68%	63%
26 to 50%	13%	15%
51 to 75%	8%	11%
76 to 100%	2%	3%
Total	100%	100%
Extrapolated value	20%	23%

Q4. In the next 12-24 months, how much of your IT budget will be allocated to cloud services (SaaS, IaaS and PaaS combined)?	IT	Compliance
None	5%	5%
1 to 25%	44%	42%
26 to 50%	32%	31%
51 to 75%	14%	16%
76 to 100%	5%	6%
Total	100%	100%
Extrapolated value	31%	32%

Q5. Do concerns about data security keep your organization from adopting cloud services?	IT	Compliance
Yes	31%	37%
No	56%	49%
Unsure	13%	14%
Total	100%	100%

Q6. From the list provided below, please select your top two concerns about using IaaS instead of on-premises IT.	IT	Compliance
Data security and privacy compliance risks	31%	35%
Workload and complexity	57%	37%
Costs that may creep up in the future	12%	23%
Bandwidth bottlenecks	56%	15%
Quick recovery of data in the event of a disaster	19%	36%
Violation of agreements with vendors and business partners	6%	39%
Total	181%	185%

Q7. Please rate the following statements about cloud computing resources using the scale provided below each item. Strongly agree and agree responses.	IT	Compliance
Q7a. Data located in the SaaS cloud environment presents a very high security risk for our organization.	49%	51%
Q7b. Data located in the IaaS cloud environment presents a very high security risk for our organization.	63%	59%

Q8. What benefits does your organization experience by using IaaS? Please select all that apply.	IT	Compliance
Business agility	56%	23%
Speed to roll out new services	43%	34%
Lower IT operating costs	27%	51%
Fewer personnel and management resources	35%	29%
Improved reliability	13%	15%
Better quality infrastructure	26%	35%
Improved compliance	12%	48%
Improved security	9%	31%
No benefits	33%	19%
Total	254%	285%

Q9. How much of a priority is security when evaluating IaaS providers?	IT	Compliance
Very high priority	13%	21%
High priority	28%	35%
Low priority	34%	18%
Not a priority	25%	26%
Total	100%	100%

Q10. What data types would you place in the cloud infrastructure environment if this data **was not encrypted**? Please select all that apply.	IT	Compliance
Regulated data (such as credit cards, health data, SSN, driver's license number).	51%	44%
Non-regulated customer data (such as purchase history, email address list, shipping information)	53%	50%
Non-regulated confidential business data (such as intellectual property, business plans, financial records)	42%	34%
Employee data	55%	46%
Average	50%	44%

Q11. What data types would you place in the cloud infrastructure environment if this data **was encrypted**? Please select all that apply.	IT	Compliance
Regulated data (such as credit cards, health data, SSN, driver's license number).	65%	64%
Non-regulated customer data (such as purchase history, email address list, shipping information)	72%	65%
Non-regulated confidential business data (such as intellectual property, business plans, financial records)	48%	45%
Employee data	70%	67%
Total	64%	60%

Q12. What type of sensitive data does your organization consider most important to store in the cloud infrastructure environment?	IT	Compliance
Structured data (in a database)	20%	25%
Unstructured data (files, documents, emails, etc.)	59%	53%
Both	21%	22%
Total	100%	100%

Q13. What are the most important security features when placing sensitive data in the cloud infrastructure environment? Please rank from 5 = most important to 1 = least important. **Average rank.**	IT	Compliance
Data is unreadable by the cloud administrator	4.59	4.03
Data is unreadable by internal personnel who do not have a need to access or view this information	3.56	4.12
The appropriate users control data access	3.17	3.56
An audit trail of successful or failed access attempts is reported	2.16	3.27
Separation of duties is enforced	3.02	4.20
Average	3.30	3.84

Q14. IT: In your organization, who is most responsible for (1) defining, (2) enforcing, and (3) implementing security requirements for data in the cloud infrastructure environment?	Defining	Enforcing	Implementing
CEO	0%	0%	0%
CFO	0%	3%	3%
CIO	12%	12%	23%
CTO	7%	6%	0%
IT security leader (CISO)	16%	19%	6%
Security leader (CSO)	2%	1%	4%
Compliance/audit	15%	16%	7%
Legal department	9%	12%	0%
Business unit leaders	22%	20%	18%
End-users of cloud services	9%	1%	9%
Facilities or data center management	0%	0%	4%
No one role has overall responsibility	8%	10%	26%
Other	100%	100%	100%

Q14. Compliance: In your organization, who is most responsible for (1) defining, (2) enforcing, and (3) implementing security requirements for data in the cloud infrastructure environment?	Defining	Enforcing	Implementing
CEO	0%	0%	0%
CFO	0%	0%	4%
CIO	11%	13%	25%
CTO	5%	3%	2%
IT security leader (CISO)	13%	20%	8%
Security leader (CSO)	2%	0%	0%
Compliance/audit	21%	13%	4%
Legal department	10%	8%	1%
Business unit leaders	16%	28%	20%
End-users of cloud services	4%	0%	8%
Facilities or data center management	0%	0%	0%
No one role has overall responsibility	18%	15%	28%
Other	100%	100%	100%

Q15, Very significant and significant response	IT	Compliance
Q15a. How significant is the role of IT security when choosing or evaluating cloud infrastructure providers before deploying their services?	45%	52%
Q15b. How significant is the role of compliance or auditing when choosing or evaluating cloud infrastructure providers before deploying their services?	38%	49%

	How likely would this happen to your organization? Already occurred & very likely to occur response.	
Q16. The following are 11 scenarios about the insecure use of cloud infrastructure services by organizations.	IT	Compliance
Q16a. Cloud providers are selected without vetting their security practices.	80%	67%
Q16b. The software development department programs or tests new applications on cloud computing infrastructure using live (real) data without taking steps to secure this data.	68%	65%
Q16c. The cloud infrastructure service provider has an unintentional mishap or systems glitch that results in the exposure of your organization's sensitive or confidential data.	63%	59%
Q16d. The cloud infrastructure service provider is attacked by an internal source, compromising your organization's sensitive or confidential data.	63%	60%
Q16e. The cloud infrastructure service provider is attacked by an external source, compromising your organization's sensitive or confidential data.	69%	59%
Q16f. The cloud provider's administration fails to notify your organization that sensitive or confidential data was exposed (for instance to another cloud customer) or stolen.	56%	44%
Q16g. The cloud provider's administration permits access to your organization's sensitive or confidential data by individuals who do not have a "need to know."	72%	46%
Q16h. The cloud provider's administration shares your organization's sensitive or confidential data with other third parties (such as a business or law enforcement) without obtaining your permission.	64%	45%
Q16i. The cloud provider's administration does not remove or delete your organization's sensitive or confidential information after a project is completed or relationship is terminated.	69%	43%
Q16j. While your organization uses encryption to protect data, the cloud provider does not protect the encryption keys from unauthorized access.	44%	36%
Average	65%	52%

Q17. The following are 11 scenarios about the insecure use of cloud infrastructure services by organizations.	Your organization has the controls to mitigate or reduce this event. Strongly agree & agree response.	
Q17a. Cloud providers are selected without vetting their security practices.	IT	Compliance
Q17b. The software development department programs or tests new applications on cloud computing infrastructure using live (real) data without taking steps to secure this data.	33%	46%
Q17c. The cloud infrastructure service provider has an unintentional mishap or systems glitch that results in the exposure of your organization's sensitive or confidential data.	41%	43%
Q17d. The cloud infrastructure service provider is attacked by an internal source, compromising your organization's sensitive or confidential data.	28%	33%
Q17e. The cloud infrastructure service provider is attacked by an external source, compromising your organization's sensitive or confidential data.	38%	36%
Q17f. The cloud provider's administration fails to notify your organization that sensitive or confidential data was exposed (for instance to another cloud customer) or stolen.	38%	40%
Q17g. The cloud provider's administration permits access to your organization's sensitive or confidential data by individuals who do not have a "need to know."	36%	41%
Q17h. The cloud provider's administration shares your organization's sensitive or confidential data with other third parties (such as a business or law enforcement) without obtaining your permission.	39%	42%
Q17i. The cloud provider's administration does not remove or delete your organization's sensitive or confidential information after a project is completed or relationship is terminated.	36%	40%
Q17j. While your organization uses encryption to protect data, the cloud provider does not protect the encryption keys from unauthorized access.	34%	37%
Average	36%	40%

Q18. Does your organization's major cloud provider(s) use encryption to protect data from insider threats?	IT	Compliance
Yes	31%	32%
No	59%	51%
Unsure	10%	17%
Total	100%	100%

Q19. What enabling technologies and controls does your organization have in place to protect sensitive or confidential information placed into cloud environments?	IT	Compliance
Firewalls	88%	76%
Anti-virus/anti-malware	85%	78%
Encryption of data	32%	32%
Encryption of files	33%	35%
Encryption of disks and servers	29%	26%
Identity and access management	50%	43%
Network intelligence systems	26%	19%
Intrusion detection or prevention systems	29%	25%
Web application firewalls	23%	20%
Encryption key management	30%	28%
Other (please specify)	5%	6%
Total	430%	388%

Q20. Does your organization's internal audit review and provide feedback on security in the cloud infrastructure environment?	IT	Compliance
Yes	29%	32%
No	59%	55%
Unsure	12%	13%
Total	100%	100%

Part 4. Organization characteristics and respondent demographics

D1. What organizational level best describes your current position?	IT	Compliance
Senior Executive	1%	0%
Vice President	1%	2%
Director	16%	21%
Manager	21%	32%
Supervisor	18%	18%
Technician	34%	5%
Staff or Administrative	6%	15%
Contractor	2%	4%
Other (please specify)	1%	3%
Total	100%	100%

D2. Check the country or U.S. region where your company's primary headquarters is located.	IT	Compliance
Northeast	18%	19%
Mid-Atlantic	17%	17%
Midwest	16%	17%
Southeast	12%	13%
Southwest	13%	13%
Pacific-West	17%	18%
Outside US	5%	4%
Total	100%	100%

Experience in years	IT	Compliance
D3a. Total years of experience (mean)	9.71	11.02
D3b. Total years in present position (mean)	4.15	4.77

D4. What industry best describes your organization's industry concentration or focus?	IT	Compliance
Agriculture	0%	0.01
Communications	5%	4%
Defense	2%	1%
Energy	2%	3%
Entertainment & media	1%	2%
Financial services	21%	19%
Health & pharmaceuticals	11%	10%
Hospitality & leisure	3%	5%
Industrial	8%	9%
Public sector	14%	15%
Retail	8%	9%
Services	9%	8%
Technology & software	5%	7%
Transportation	5%	3%
Other	6%	4%
Total	100%	100%

D5. What best describes your role in managing data protection and security risk in your organization? Select all that apply.	IT	Compliance
Setting priorities	31%	43%
Managing budgets	30%	36%
Selecting vendors and contractors	38%	29%
Determining privacy and data protection strategy	22%	31%
Evaluating program performance	28%	33%
None of the above	26%	14%
Total	175%	186%

D6. What is the worldwide headcount of your organization?	IT	Compliance
1 to 49	3%	4%
50 to 99	5%	6%
100 to 499	6%	5%
500 to 999	5%	7%
1,000 to 1,999	11%	12%
2,000 to 4,999	26%	25%
5,000 to 9,999	23%	22%
10,000 or more	21%	19%
Total	100%	100%

If you have any questions about this research, please contact Ponemon Institute at research@ponemon.org, or contact us via our toll free number 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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.