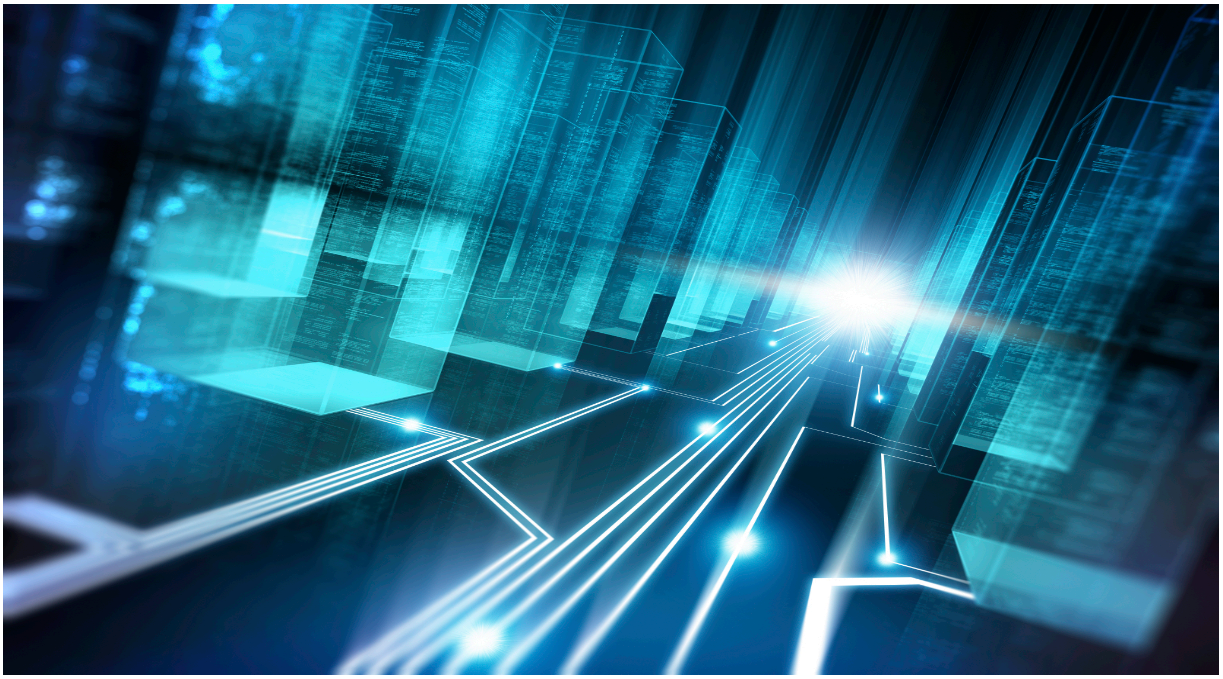


The Challenges of Cloud Information Governance: A Global Data Security Study

Sponsored by SafeNet

Independently conducted by Ponemon Institute LLC

Publication Date: October 2014

The Challenges of Cloud Information Governance: A Global Data Security Study

Ponemon Institute: October 2014

Part 1. Introduction

We are pleased to present the findings of *The Challenges of Cloud Information Governance: A Global Data Security Study* sponsored by SafeNet. The purpose of this research is to focus on how organizations are putting confidential information at risk in the cloud because of the lack of appropriate governance policies and security practices.

We surveyed 1,864 IT and IT security practitioners in the United States, United Kingdom, EMEA and APAC who are familiar and involved in their company's use of both public and private cloud resources. Seventy-two percent of respondents say their organizations are heavy (26 percent) or moderate (46 percent) users of cloud resources.

Respondents estimate that cloud use will increase over the next two years. Today respondents estimate that 33 percent of their organizations' total IT and data processing requirements are met by using cloud resources. This is expected to increase to an average of 41 percent of IT and data processing requirements. However, the findings reveal that organizations have difficulty in managing the risk without applying the right governance practices.

Throughout the world, the majority of respondents (70 percent) agree that it is more complex to manage privacy and data protection regulations in a cloud environment than on-premise networks within my organization.

Following are seven reasons why cloud governance is a challenge:

1. There is uncertainty about who is accountable for safeguarding confidential or sensitive information stored in the cloud making it difficult to determine if security and data privacy policies are in place and enforced.

2. IT security is out of the loop when companies are making decisions about the use of cloud resources and the security solutions that should be deployed. IT security is not involved in the evaluation of a cloud provider's security capabilities. Most often the security evaluations are based on word-of-mouth recommendations and contractual negotiation and legal review.

3. IT functions are not confident they know all the cloud computing applications, platform or infrastructure services the organization has because departments throughout the organization are making decisions about their use (a.k.a Shadow IT).

4. The use of encryption, tokenization or other cryptographic solution for the cloud is considered important but only 36 percent of respondents say they use these technologies to secure sensitive or confidential information at rest.

5. The inability to control how employees and third parties access and handle sensitive data in the cloud makes compliance with regulations a challenge.

6. More employees are using cloud apps without specific training on the security procedures to follow.

7. Third parties such as contractors and business partners and employees are allowed to access sensitive data in the cloud without the appropriate security solutions in place such as multi-factor authentication.

Part 2. Key findings

In this section we provide an analysis of the key findings of this research. The complete audited findings are presented in the appendix of this report. The report is organized according to the following topics:

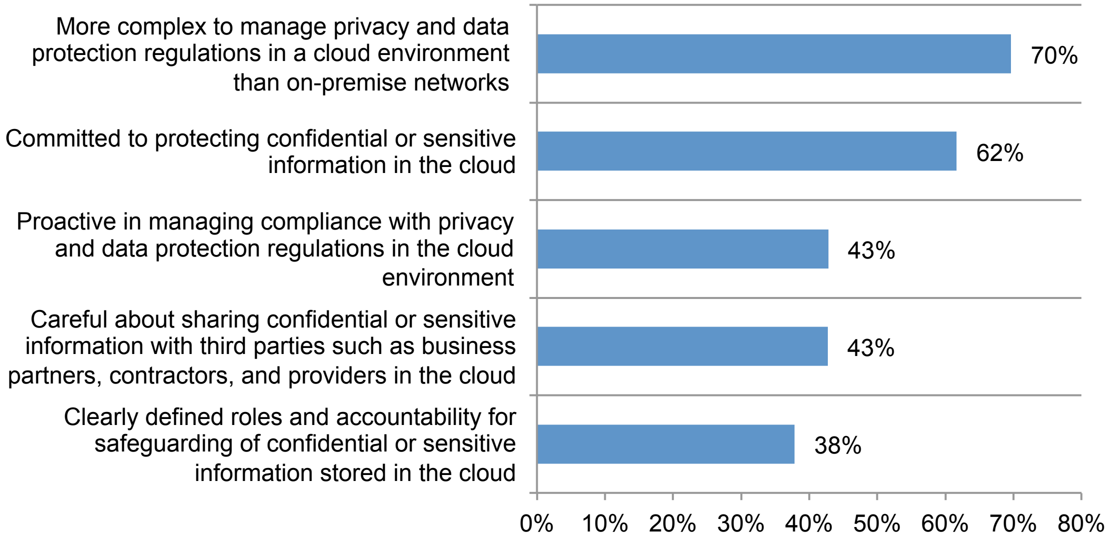
- As the cloud's popularity grows, so does the risk to sensitive data
- Cloud security is stormy because of Shadow IT
- Data security governance practices ignore the security practitioners
- Protection of data in the cloud is important but not practiced
- Cloud complicates identity and access management

As the cloud's popularity grows, so does the risk to sensitive data

Cloud usage grows without the support of necessary governance practices. On average the use of cloud computing resources for total IT and data processing requirements will increase from 33 percent to 41 percent in the next two years. Seventy-one percent of respondents say cloud computing applications or platform solutions are very important or important and over the next two years 78 percent of respondents say cloud solutions will be very important or important.

Does the growth and importance of the cloud mean there is an increase in policies and procedures to safeguard data? Figure 1 reveals that the current state of cloud governance does not include a proactive approach to reducing security risks in the cloud. As shown, 62 percent of respondents are committed to protecting confidential or sensitive information in the cloud. Seventy percent of respondents agree that it is more complex to manage privacy and data protection regulations in a cloud environment than on-premise networks within my organization. However, the complexity is not being addressed with policies and a focus on compliance with privacy and security regulations.

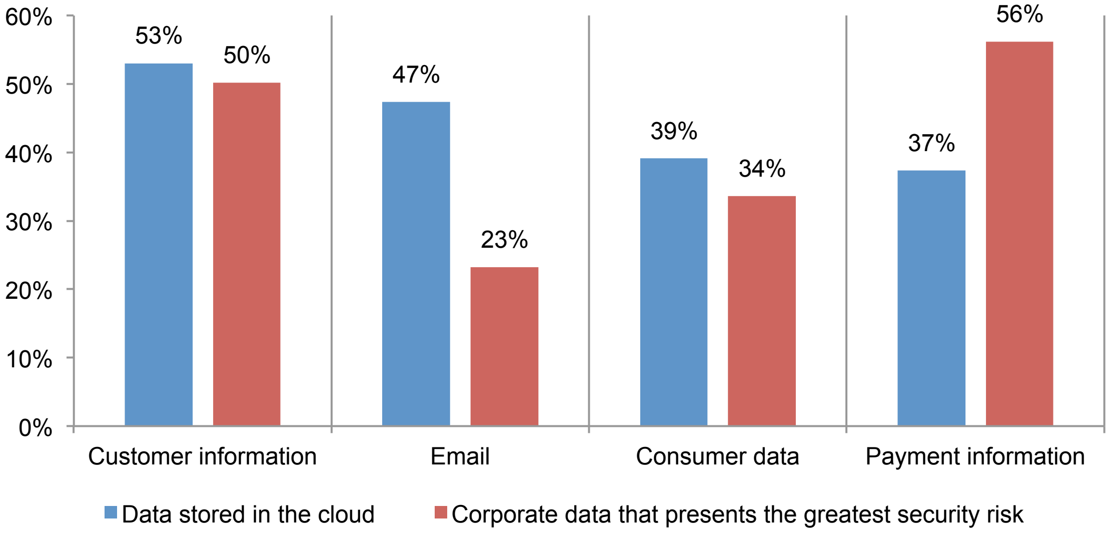
Figure 1. Perceptions about governance practices in the cloud
Strongly agree and agree response combined



Only 38 percent of respondents say their organizations have clearly defined roles and accountability for safeguarding of confidential or sensitive information in the cloud and 57 percent say their organizations are not proactive in managing compliance with privacy and data protection regulations in the cloud environment (100 percent-43 percent of respondents). Similarly, 57 percent do not agree their organization is careful about sharing sensitive information with third parties such as business partners, contractors and providers in the cloud environment.

The type of corporate data stored in the cloud is also the data most at risk. As shown in Figure 2, emails, consumer, customer and payment information are most often stored in the cloud. With the exception of emails, these types of data are also believed to pose the greatest security risk. Payment information is considered most at risk followed by customer information

Figure 2. Data in the cloud and at risk
More than one response permitted

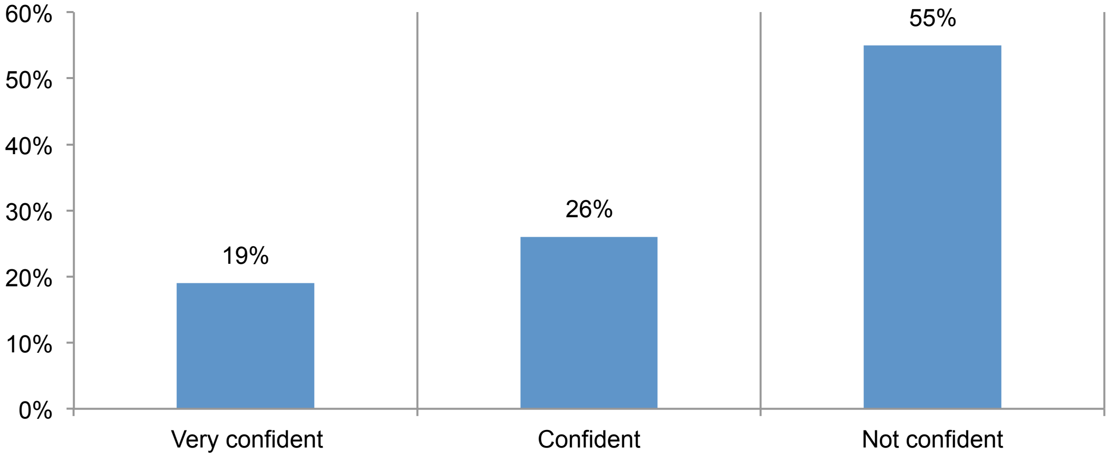


Cloud security is stormy because of Shadow IT

IT is losing control of corporate data stored in the cloud. An average of 50 percent of cloud services is deployed by departments other than corporate IT and an average of 44 percent of corporate data stored in the cloud environment is not managed or controlled by the IT department.

As a consequence, Shadow IT is a growing problem in organizations. According to Figure 3, 55 percent of respondents are not confident that the IT organization knows all cloud computing applications, platform or infrastructure services in use today.

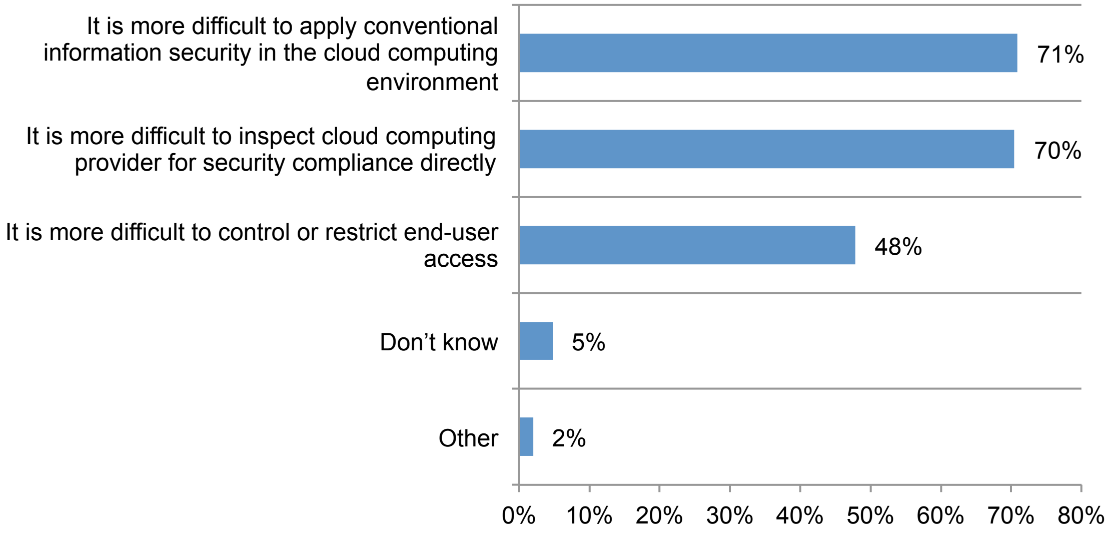
Figure 3. How confident are you that IT knows all cloud computing services in use today?



Conventional approaches to security in the cloud are difficult to apply. Sixty percent of respondents say it is more difficult to protect confidential or sensitive information.

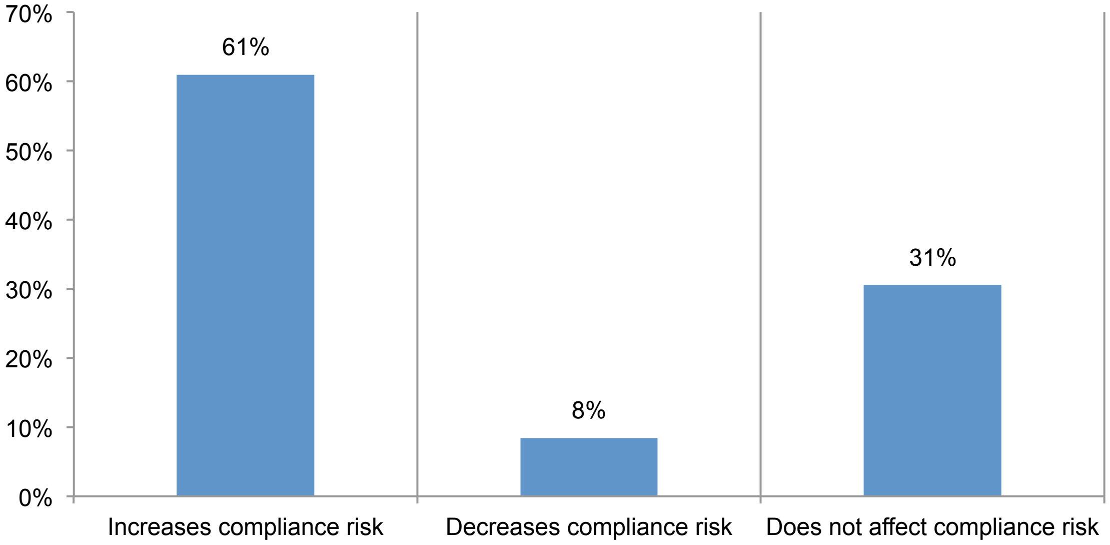
Figure 4 reveals why 60 percent say cloud security is a problem. The primary reasons are that it is more difficult to apply conventional information security in the cloud computing environment (71 percent) and the inability to directly inspect cloud-computing providers for security compliance (70 percent). This is followed by the difficulty in controlling or restricting end-user access (48 percent).

Figure 4. Why cloud security is difficult to achieve
More than one response permitted



Compliance in the cloud is difficult. Sixty-one percent of respondents say the use of cloud resources increases compliance risk. This can be due to the difficulty in controlling end users’ access to sensitive data in the cloud. According to Figure 5, only 31 percent say the cloud has no affect on the company’s ability to comply with privacy and data protection regulations or legal requirements around the globe.

Figure 5. The cloud compliance risk

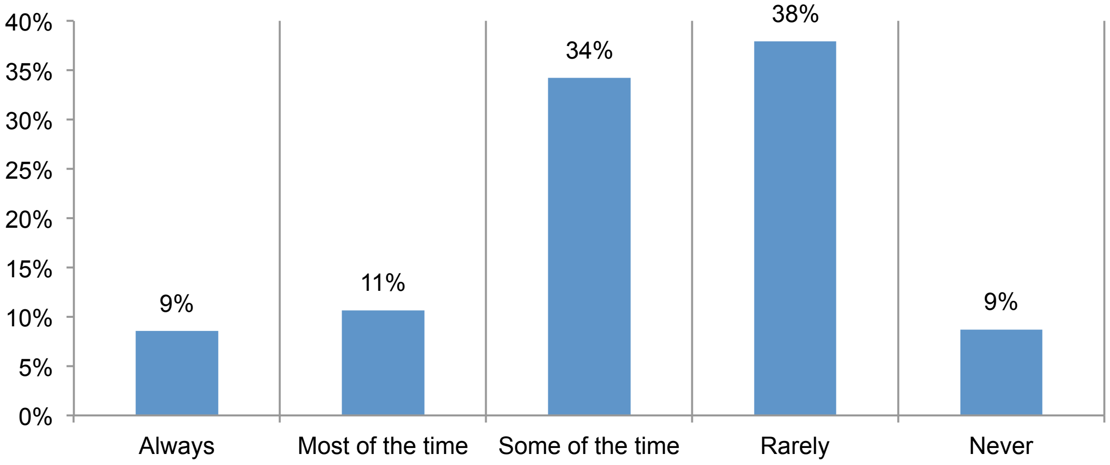


Data security governance practices ignore the security practitioners

Security practitioners are not the decision makers when it comes to the use of cloud resources. According to Figure 6, only 20 percent of respondents say members of the security team are involved in the decision-making process about using certain cloud applications or platforms.

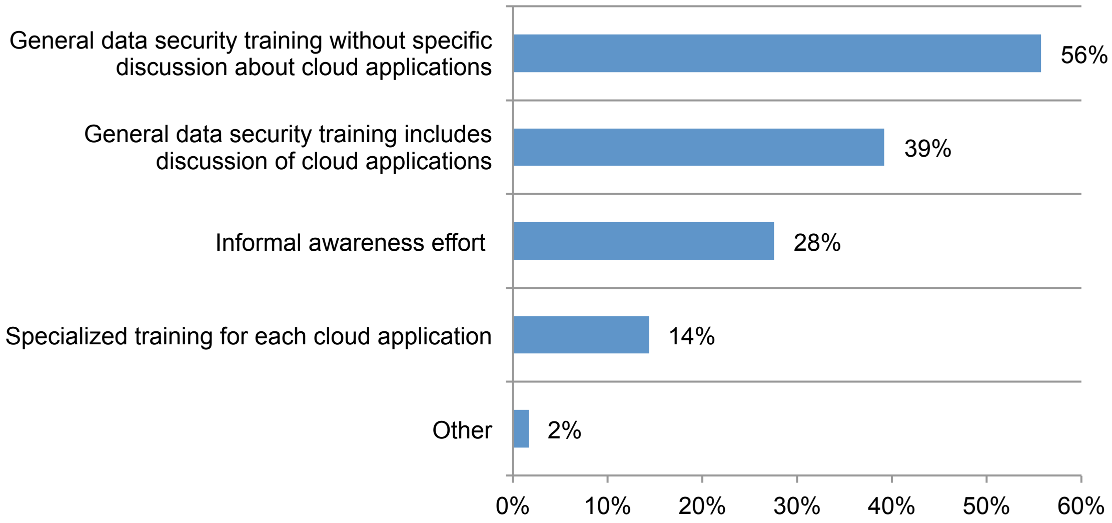
Further, security policies for the cloud are lacking**.** Only about one-third of respondents say their organizations have a policy that requires the use of security safeguards such as encryption as a condition to using certain cloud computing applications.

Figure 6. Is the security team involved in cloud decisions?



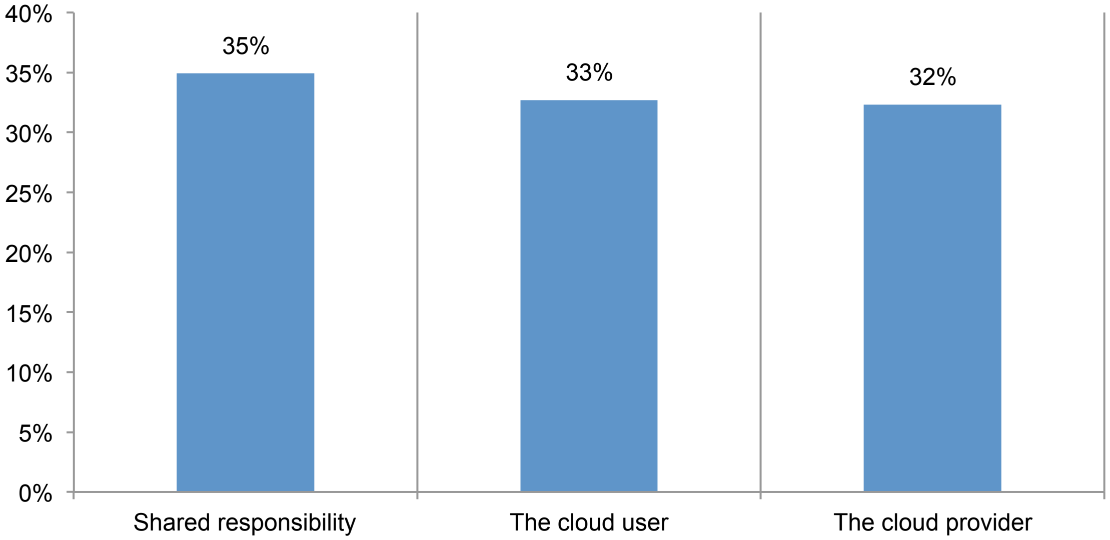
Specialized employee training for safeguarding data in cloud apps is lacking. When asked how their organizations educate employees about safeguarding sensitive or confidential information in cloud applications, only 14 percent of respondents say they have training targeted to the security risks created by the use of cloud applications, as shown in Figure 7. The majority of respondents (56 percent) say training focuses on general security topics without specific discussion about cloud applications.

Figure 7. How organizations educate employees about cloud application risks
More than one response permitted



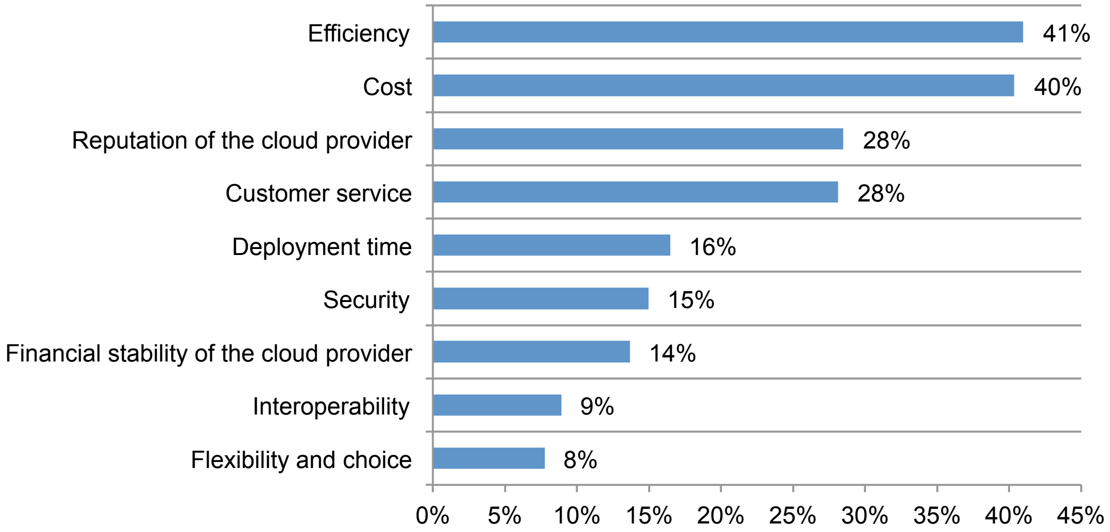
Who is most responsible for cloud security? According to Figure 8, respondents have mixed views on who should be most responsible for protecting sensitive or confidential data in the cloud. Thirty-five percent believe it is a shared responsibility. However, 33 percent say it is the cloud user. This uncertainty makes it difficult to have clearly defined roles and accountability for safeguarding information in the cloud.

Figure 8. Who is responsible for cloud security?



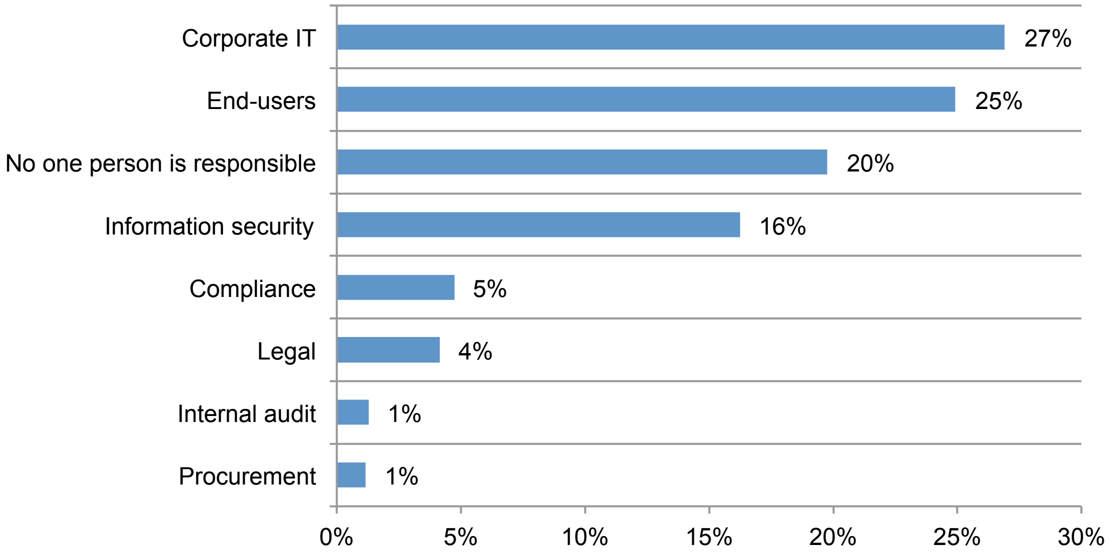
Cost and efficiency are the most important factors for selecting a cloud provider. Forty-one percent of respondents say efficiency and 40 percent say cost are the primary reasons for selecting a particular cloud provide, as shown in Figure 9. Only 15 percent say it is for their security practices.

Figure 9. How do you select a cloud provider?
Two responses permitted



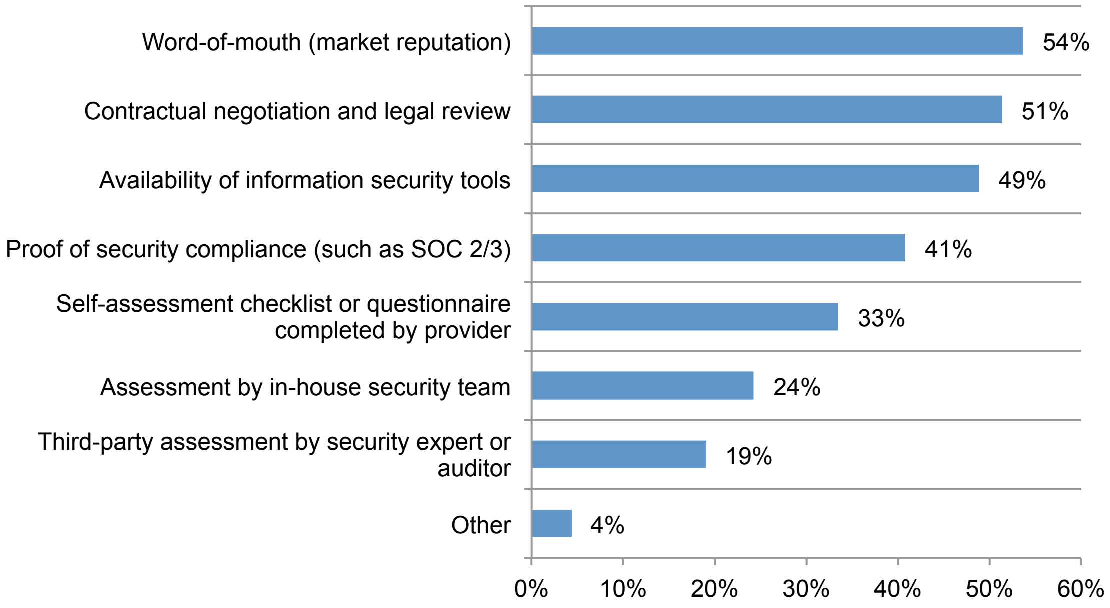
Evaluation of cloud providers is not the responsibility of IT security. Fifty-three percent of respondents say their organizations evaluate the security capabilities prior to engagement or deployment. However, only 16 percent of respondents say it is the security function that is most responsible for evaluating the cloud provider's security capabilities, as shown in Figure 10. Most likely it is corporate IT or the end-user (27 percent and 25 percent, respectively).

Figure 10. Who evaluates the cloud provider's security capabilities?



Security evaluations of cloud providers are superficial. Figure 11 reveals that 54 percent of respondents say word-of-mouth or market reputation is used to evaluate the provider, followed by contractual negotiation and legal review (51 percent of respondents). Less than half (49 percent) of respondents say they look at the availability of information security tools. Fewer organizations look at proof of security compliance (41 percent), a self-assessment security questionnaire (33 percent) and an assessment by in-house security team (24 percent).

Figure 11. How cloud providers are evaluated
More than one response permitted

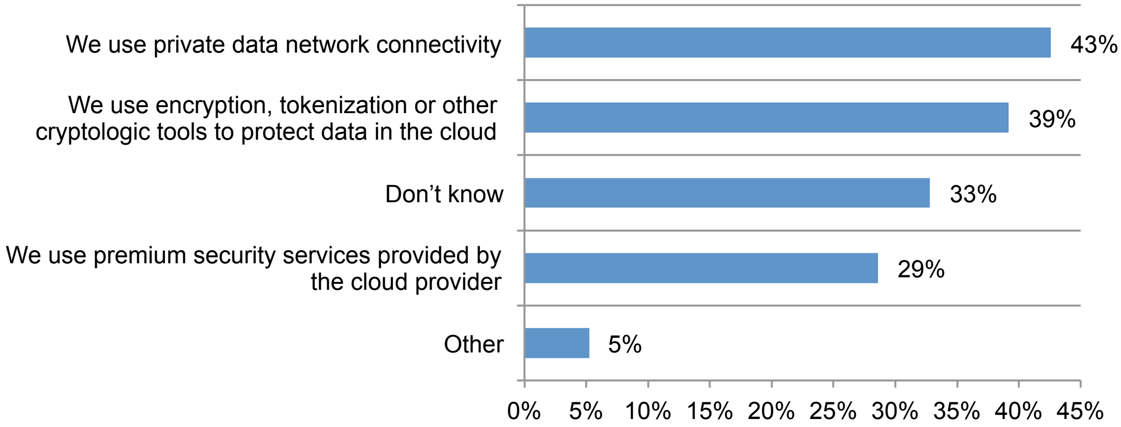


Protection of data in the cloud is important but not practiced

More organizations use private data network connectivity to secure data in the cloud. When asked what security solutions are used to protect data in the cloud, 39 percent of respondents say their organizations use encryption, tokenization or other cryptographic tools to protect data in the cloud, as shown in Figure 12. Most respondents (43 percent) say they use private data network connectivity.

One-third of respondents say they don't know what security solutions they use. Probably because respondents believe decisions about business units and corporate IT are making investments in security without input from IT security.

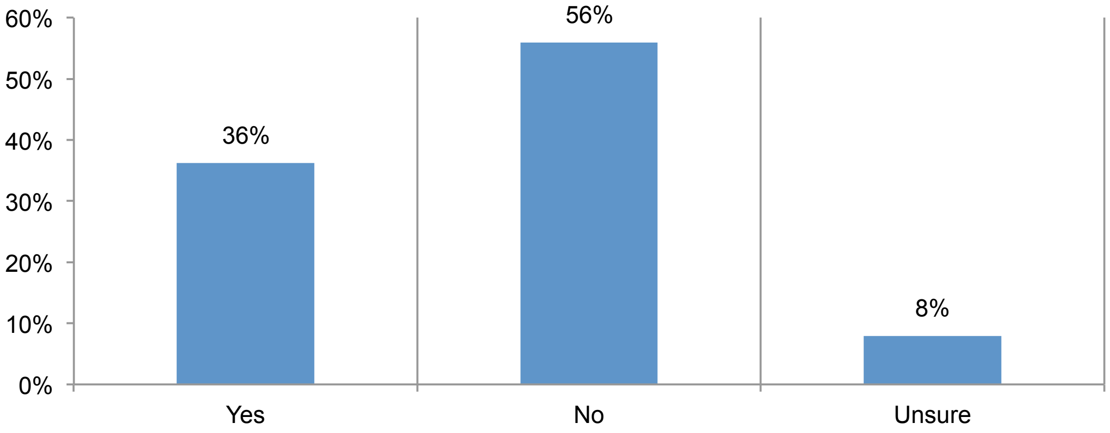
Figure 12. How data is protected in the cloud
More than one response permitted



Encryption is considered critical but in reality it is not often used. Seventy-one percent of respondents say the ability to encrypt or tokenize sensitive or confidential data is important and 79 percent say it will become more important over the next two years.

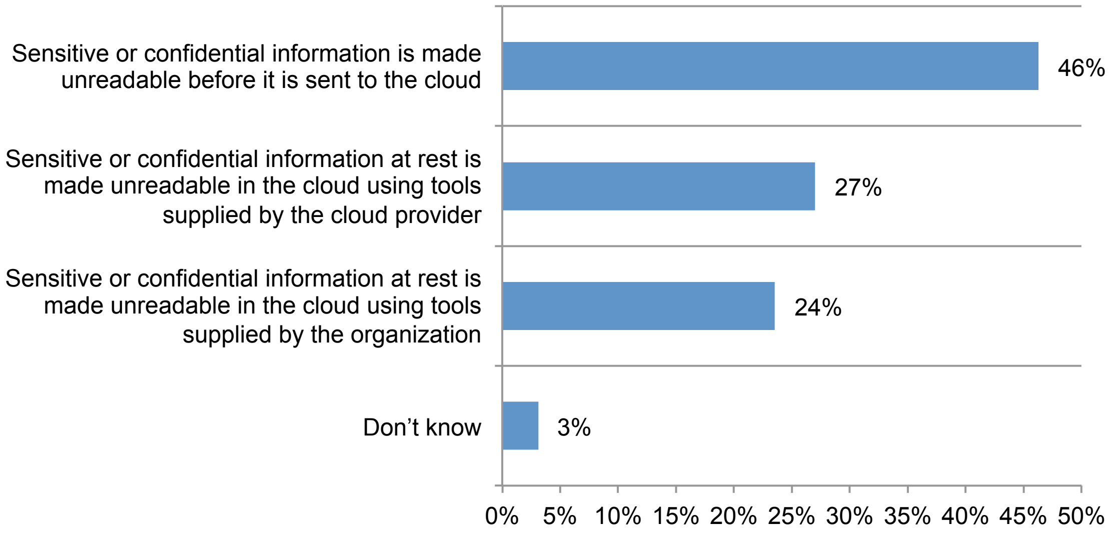
However, according to Figure 13, only 36 percent of respondents say their organization uses encryption, tokenization or other cryptographic solutions to secure sensitive or confidential information at rest. More respondents say encryption is used when it is sent and received by the cloud provider (55 percent). Only 28 percent say they encrypt or tokenize sensitive or confidential data directly within cloud applications such as SaaS.

Figure 13. Use of encryption, tokenization or other cryptographic solution



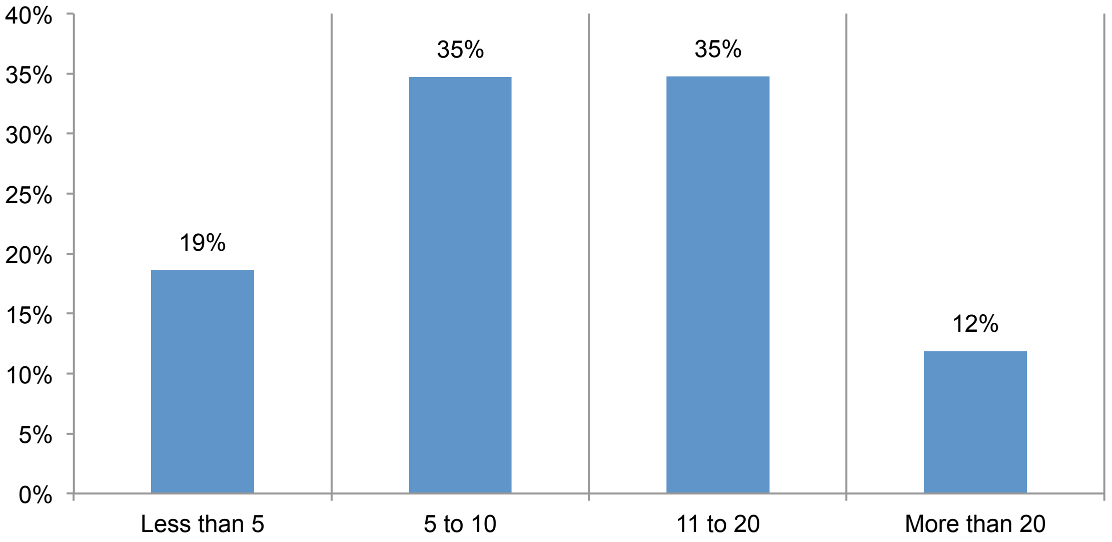
If data at rest is encrypted, as shown in Figure 14, 46 percent say the data is made unreadable before it is sent to the cloud. The remaining respondents say it is made unreadable in the cloud using tools supplied by their organization or the cloud provider.

Figure 14. How encryption is applied



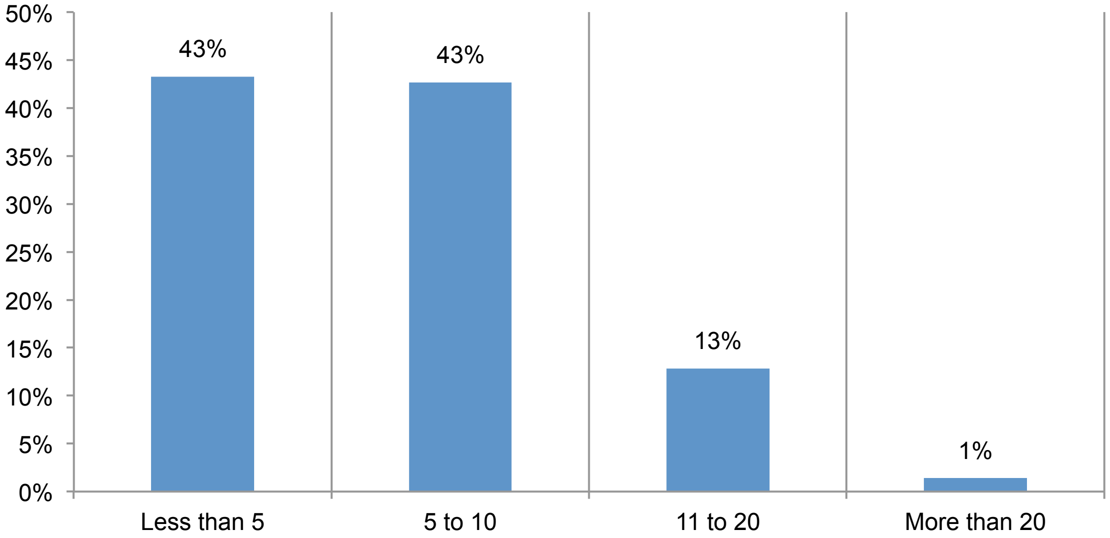
There is a lack of encryption of cloud applications (SaaS). According to the study, Software as a Service (SaaS) is used more frequently than Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Seventy-three percent business applications such as document sharing tools and 72 percent say they use online backup**.** However, only 28 percent of respondents say their organization encrypts or tokenizes sensitive or confidential data directly within these applications. According to Figure 15, an average of 11 applications require encryption.

Figure 15. How many applications require encryption?
Extrapolated value 11.3



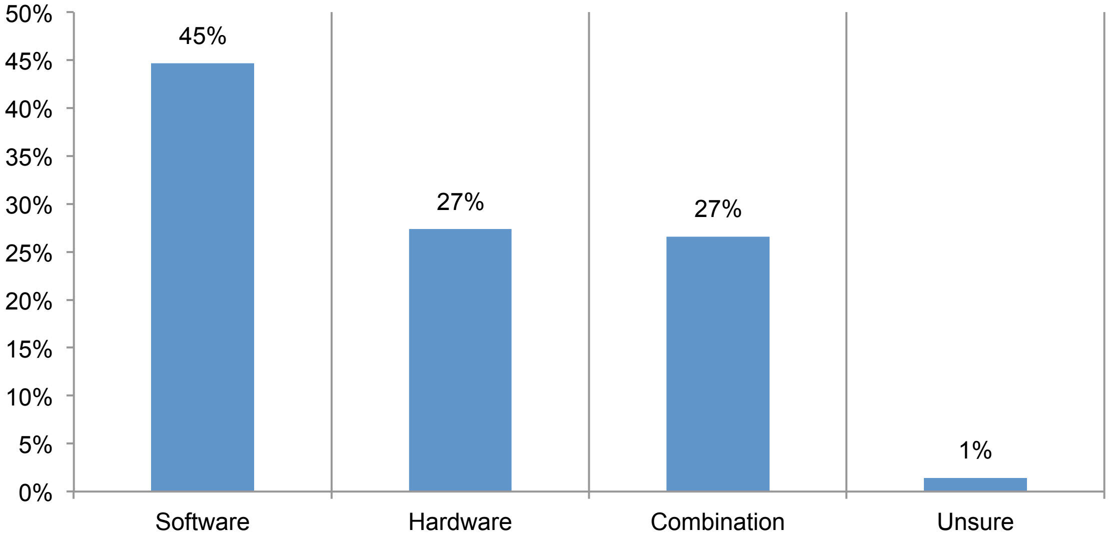
How prevalent is the use key management systems and where encryption keys are stored. Figure 16 reveals that on average organizations have 7 key management systems or encryption platforms**.**

Figure 16. How many key management systems or encryption platforms does your organization have?
Extrapolated value 7.2



As shown in Figure 17, most encryption keys are stored in software followed by hardware or a combination of hardware and software. Fifty-four percent say their organization controls the encryption keys when data is encrypted in the cloud. Twenty percent say it is the cloud provider and 17 percent say a third part controls the encryption keys (neither the organization or cloud provider).

Figure 17. Where encryption keys are stored

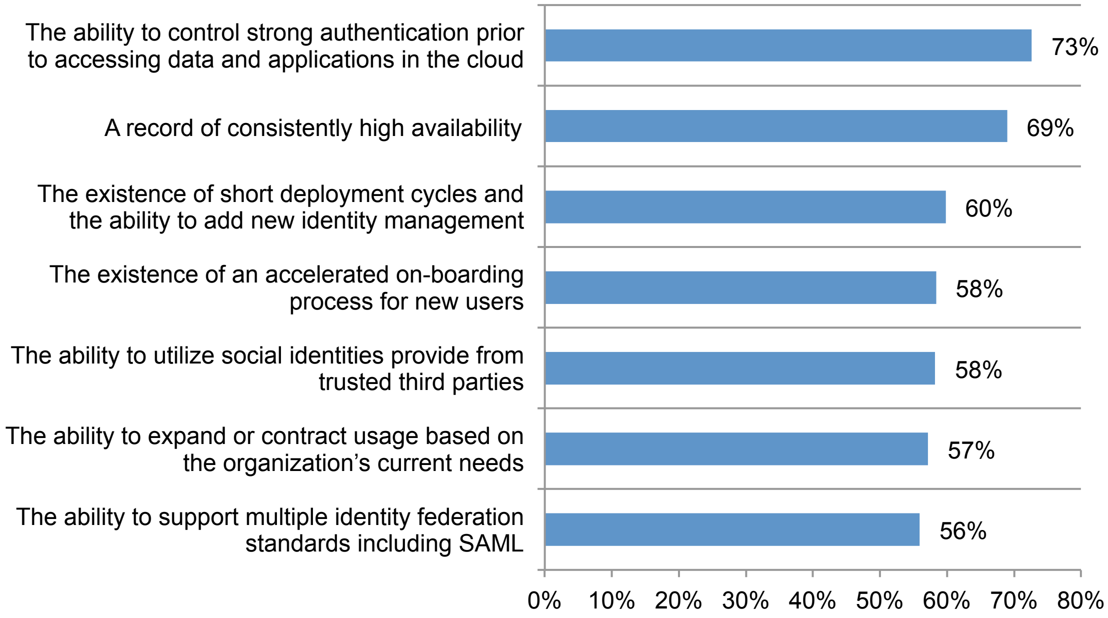


The cloud complicates identity and access management policies

Strong authentication measures are important. Sixty-eight percent of respondents say the management of user identities is more difficult in the cloud than the on-premise environment. However, organizations are not adopting measures that are easy to implement and could increase cloud security.

The most important features to controlling and securing access to cloud resources are shown in Figure 18. Most important is the ability to control strong authentication prior to accessing data and applications in the cloud. A record of consistently high availability is important according to 69 percent of respondents.

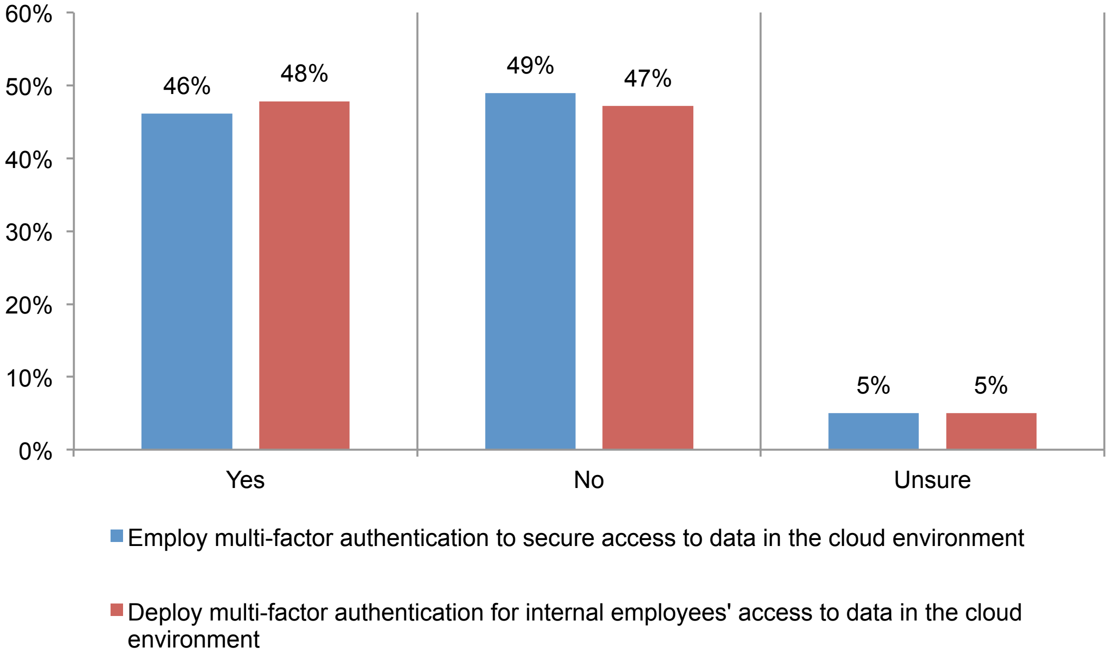
Figure 18. Most important identity and access management features
Essential and very important responses combined



Most organizations permit third-party users to access data in the cloud. Sixty-two percent of respondents say their organizations have third parties accessing the cloud. However, as shown in Figure 19, 49 percent say their organization does not use multi-factor authentication to secure access to data in the cloud environment and 5 percent are unsure.

About the same percentage of respondents say their organizations do not use multi-factor authentication for employees' access to the cloud. When asked the percent of cloud applications that have user-enabled access controls, the average is only 18 percent.

Figure 19. Use of multi-factor authentication for third-party access



Part 3. Recommendations on improving cloud governance

The findings reveal that global organizations have challenges when securing data in the cloud due to the lack of critical governance and security practices in place. Following are steps that will lead to a more secure cloud environment.

- Confirm if the cloud provider or cloud user is most accountable and responsible for cloud security. If it is the cloud provider, involve IT security in vetting and evaluating its security practices. If the organization assumes responsibility, make sure there are clearly defined roles for the business functions using cloud services. Again, including IT security in establishing security policies and procedures is important.

- Increase visibility into the use of cloud applications, platforms and infrastructure to reduce the Shadow IT risk.

- Protect data at risk in the cloud. According to respondents, payment and customer information are some of the data types most often stored in the cloud and are also considered most at risk in an unsecure cloud.

- Business cloud applications such as document sharing are growing in popularity. However, policies about the secure use of these applications are not being communicated. Organizations should make employees aware of the risks with specialized training about not circumventing security policies when using SaaS applications.

- Organizations need to consider the adoption of encryption, tokenization or other cryptographic solutions to secure sensitive data transferred and stored in the cloud.

- Improve compliance with data security and privacy regulations with the use of encryption and identity and access management solutions such as multi-factor authentication.

- Even if the cloud provider has overall responsibility for data stewardship, companies should look to maintain control over their encryption keys for ultimate protection.

- Companies should store their encryption keys in hardware to ensure their keys are secured and stored separately from the encrypted data they are protecting, which is often what happens with software key storage.

- Given the wide variety of cloud-based services being used, companies should consider “bring your own encryption” solutions that enable them to encrypt data and store keys centrally across multiple cloud environments.

- With the increasing use cases of encryption, companies will need solutions that enable them to centralize key management across multiple encryption platforms in order to ensure better control and security of their encryption keys.

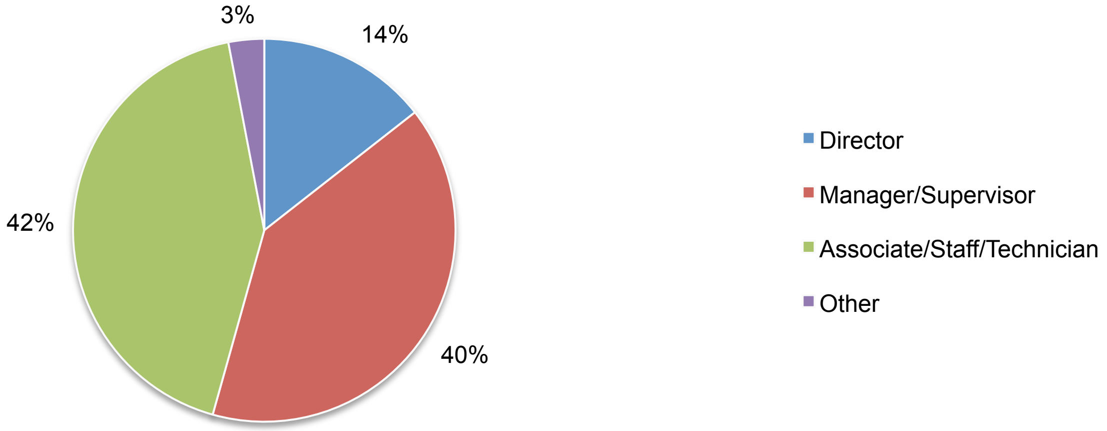
Part 4. Methods

A sampling frame of 62,511 experienced IT and IT security practitioners located in the United States, United Kingdom, EMEA and APJ were selected as participants to this survey. To ensure knowledgeable responses, all participants in this research are familiar and involved in their company's use of both public and private cloud resources. Table 1 shows 2,201 total returns. Screening and reliability checks required the removal of 337 surveys. Our final sample consisted of 1,864 surveys or a 3.0 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	62,511	100.0%
Total returns	2,201	3.5%
Rejected or screened surveys	337	0.5%
Final sample	1,864	3.0%

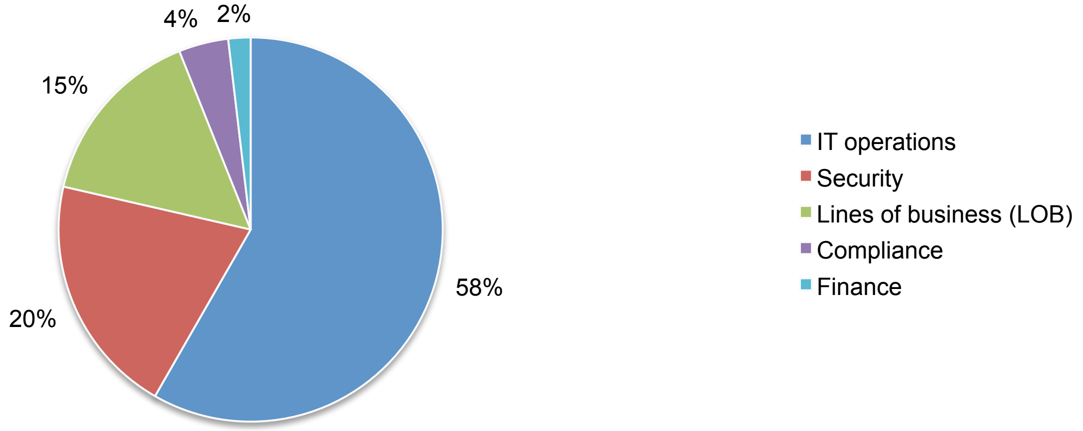
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 54 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



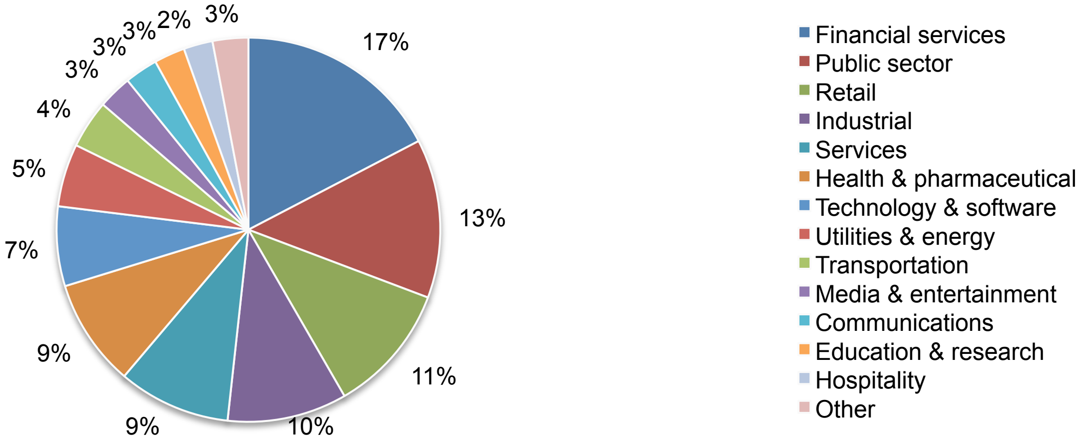
As shown in Pie Chart 2, 58 percent of respondents reported their functional area as IT operations, 20 percent reported security and 15 percent report lines of business (LOB).

Pie Chart 2. Functional area within the organization



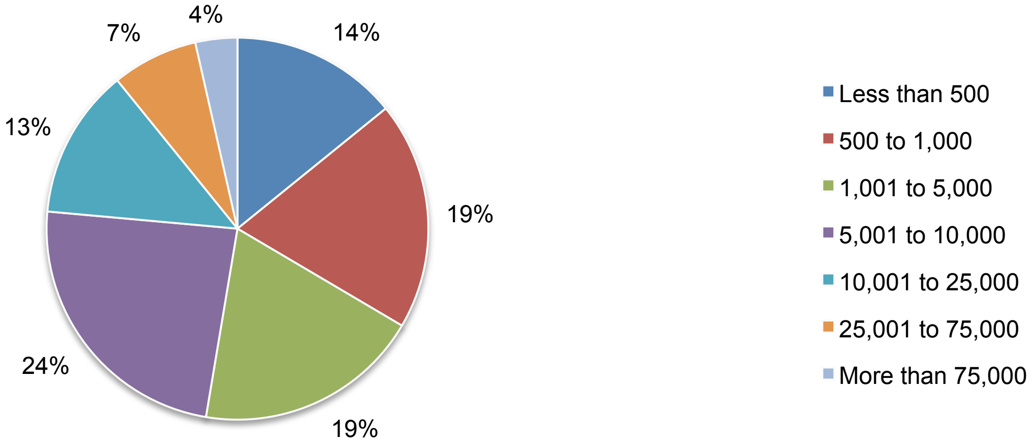
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by public sector (13 percent) and retail (11 percent).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 4, 67 percent of respondents are from organizations with a global headcount of more than 1,000 employees

Pie Chart 4. Global employee headcount



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 August 2014.

Survey response	Freq	Pct%
Total sampling frame	62,511	100.0%
Total returns	2,201	3.5%
Rejected or screened surveys	337	0.5%
Final sample	1,864	3.0%
Number of countries	31	31

Part 1. Screening

Q1. What best describes your organization's use of cloud resources?	Pct%
Heavy	26%
Moderate	46%
Light	28%
None (stop)	0%
Total	100%

Q2. What percent of your organization's total use of cloud resources involves public versus private clouds?	Pct%
All or mostly public cloud	51%
About equal public and private cloud	49%
All or mostly private cloud (stop)	0%
Total	100%

Part 2. Attributions about the cloud: Strongly agree and Agree responses combined	Pct%
Q3a. My organization is committed to protecting confidential or sensitive information in the cloud.	62%
Q3b. My organization has established clearly defined roles and accountability for safeguarding of confidential or sensitive information stored in the cloud.	38%
Q3c. My organization is careful about sharing confidential or sensitive information with third parties such as business partners, contractors, and providers in the cloud environment.	43%
Q3d. My organization is proactive in managing compliance with privacy and data protection regulations in the cloud environment.	43%
Q3e. It is more complex to manage privacy and data protection regulations in a cloud environment than on-premise networks within my organization.	70%

Part 3. Cloud experience
Software as a service (SaaS)

Q4. What cloud computing applications does your organization presently use? Please select all that apply.	Pct%
Business applications (such as document sharing tools)	73%
Infrastructure applications (such as online backup)	54%
Email, texting and other communication tools	72%
Virtual desktop	26%
Other	3%
We don't use SaaS	19%
Total	246%

Platform as a service (PaaS)

Q5. What cloud computing platforms does your organization presently use? Please select all that apply.	Pct%
Services (such as identity management, payments, search and others)	25%
Solution stacks (such as Java, PHP, Python, ColdFusion and others)	26%
Other	9%
We don’t use PaaS	53%
Total	113%

Infrastructure as a Service (IaaS)

Q6. What cloud computing infrastructure services does your organization presently use? Please select all that apply.	Pct%
Computing	36%
Storage	33%
Other	11%
We don’t use IaaS	41%
Total	120%

Q7. Approximately, what percent of your organization’s total IT and data processing requirements are met by using cloud resources today?	Pct%
Less than 1%	1%
Between 1% to 10%	15%
Between 11% to 25%	29%
Between 26% to 50%	31%
Between 51% to 75%	21%
Between 76% to 100%	3%
Total	100%
Extrapolated value	33%

Q8. In your opinion (best guess), what percent of your organization’s total IT and data processing requirements will be met by using cloud resources two years from today?	Pct%
Less than 1%	0%
Between 1% to 10%	9%
Between 11% to 25%	19%
Between 26% to 50%	37%
Between 51% to 75%	26%
Between 76% to 100%	8%
Total	100%
Extrapolated value	41%

Q9. How important is the use of cloud computing applications or platform solutions for meeting your organization’s business objectives?	
Q9a.Today	Pct%
Very important	38%
Important	33%
Not important	22%
Irrelevant	7%
Total	100%

Q9b. Over the next 2 years	Pct%
Very important	41%
Important	37%
Not important	17%
Irrelevant	5%
Total	100%

Q10. What are the primary reasons why cloud resources are used within your organization? Please select only two choices.	Pct%
Reduce cost	67%
Increase efficiency	39%
Improve security	12%
Faster deployment time	50%
Increase flexibility and choice	16%
Improve customer service	7%
Comply with contractual agreements or policies	7%
Other	1%
Total	200%

Q11. What factors are most important in the selection of a cloud provider? Please select only two choices.	Pct%
Cost	40%
Efficiency	41%
Security	15%
Deployment time	16%
Interoperability	9%
Flexibility and choice	8%
Customer service	28%
Reputation of the cloud provider	28%
Financial stability of the cloud provider	14%
Other	0%
Total	200%

Q12a. Are cloud providers evaluated for security capabilities prior to engagement or deployment within your organization?	Pct%
Yes	53%
No	38%
Don't know	9%
Total	100%

Q12b. If yes, who in your organization is most responsible for evaluating the cloud provider's security capabilities?	Pct%
End-users	25%
Corporate IT	27%
Compliance	5%
Legal	4%
Procurement	1%
Internal audit	1%
Information security	16%
Physical security	0%
Other	0%
No one person is responsible	20%
Total	100%

Q12c. If yes, how does your organization go about evaluating cloud providers? Please select all that apply.	Pct%
Word-of-mouth (market reputation)	54%
Contractual negotiation and legal review	51%
Availability of information security tools	49%
Proof of security compliance (such as SOC 2/3)	41%
Self-assessment checklist or questionnaire completed by provider	33%
Assessment by in-house security team	24%
Third-party assessment by security expert or auditor	19%
Other	4%
Total	276%

Q12d. If no, why does your organization permit cloud resources to be deployed without first evaluating for security? Please select all that apply.	Pct%
No one is in-charge	35%
Not considered a priority	39%
Not enough resources to conduct evaluation	58%
Not able to control end-users	61%
Other	2%
Don't know	9%
Total	204%

Q13. How confident are you that your IT organization knows all cloud computing applications, platform or infrastructure services in use today?	Pct%
Very confident	19%
Confident	26%
Not confident	55%
Total	100%

Q14. What percent of total corporate IT spending is controlled by the IT department?	Pct%
Less than 1%	0%
Between 1% to 10%	4%
Between 11% to 25%	12%
Between 26% to 50%	34%
Between 51% to 75%	34%
Between 76% to 100%	17%
Total	100%
Extrapolated value	51%

Q15. What percent of cloud services is deployed by departments other than corporate IT?	Pct%
Less than 1%	0%
Between 1% to 10%	4%
Between 11% to 25%	11%
Between 26% to 50%	38%
Between 51% to 75%	31%
Between 76% to 100%	16%
Total	100%
Extrapolated value	50%

Q16. What percent of corporate data is stored in the cloud environment?	Pct%
Less than 1%	12%
Between 1% to 10%	17%
Between 11% to 25%	22%
Between 26% to 50%	28%
Between 51% to 75%	15%
Between 76% to 100%	6%
Total	100%
Extrapolated value	30%

Q17. What percent of corporate data stored in the cloud environment is not managed or controlled by the IT department?	Pct%
Less than 1%	0%
Between 1% to 10%	7%
Between 11% to 25%	20%
Between 26% to 50%	37%
Between 51% to 75%	22%
Between 76% to 100%	14%
Total	100%
Extrapolated value	44%

Q18. What type of corporate data does your organization store in the cloud? Please select all that apply.	Pct%
Email	47%
Consumer data	39%
Customer information	53%
Payment information	37%
Employee records	39%
Health information	15%
Financial business information	36%
Intellectual property	24%
Research data	7%
Other	1%
None of the above	33%
Total	332%

Q19. What type of corporate data presents the greatest security risk to your organization when storing in the cloud? Please select only two choices.	Pct%
Email	23%
Consumer data	34%
Customer information	50%
Payment information	56%
Employee records	9%
Health information	7%
Financial business information	14%
Intellectual property	5%
Research data	2%
Other	0%
Total	200%

Part 4. Information governance in the cloud

Q20. How does your organization go about protecting confidential or sensitive information in the cloud? Please select all that apply.	Pct%
We use private data network connectivity	43%
We use premium security services provided by the cloud provider	29%
We use encryption, tokenization or other cryptographic tools to protect data in the cloud	39%
Don't know	33%
Other	5%
Total	148%

Q21a. Does cloud services make it more difficult to protect confidential or sensitive information?	Pct%
Yes	60%
No	35%
Don't know	5%
Total	100%

Q21b. If yes, why does it make it more difficult to protect confidential or sensitive information in the cloud? Please select all that apply.	Pct%
It is more difficult to inspect cloud computing provider for security compliance directly	70%
It is more difficult to apply conventional information security in the cloud computing environment	71%
It is more difficult to control or restrict end-user access	48%
Don't know	5%
Other	2%
Total	196%

Q22. How does your organization educate employees about safeguarding sensitive or confidential information when using cloud applications?	Pct%
Specialized training for each cloud application	14%
General data security training includes discussion of cloud applications	39%
General data security training without specific discussion about cloud applications	56%
Informal awareness effort	28%
Other	2%
Total	125%

Q23. Does your organization have a policy that requires the use of security safeguards such as encryption as a condition to using certain cloud computing applications?	Pct%
Yes	34%
No	62%
Don't know	3%
Total	100%

Q24. In your opinion, how does the use of cloud resources affect compliance risk – that is, the organization's inability to comply with privacy and data protection regulations or legal requirements around the globe?	Pct%
Increases compliance risk	61%
Decreases compliance risk	8%
Does not affect compliance risk	31%
Total	100%

Q25. Are members of your security team involved in the decision-making process about allowing the use of certain cloud applications or platforms?	Pct%
Always	9%
Most of the time	11%
Some of the time	34%
Rarely	38%
Never	9%
Total	100%

Part 5. Encryption, tokenization or other cryptographic solutions in the cloud

Q26. In your opinion, who is most responsible for protecting sensitive or confidential data stored in the cloud?	Pct%
The cloud provider	32%
The cloud user	33%
Shared responsibility	35%
Total	100%

Q27a. Does your organization use encryption, tokenization or other cryptographic solution to secure sensitive or confidential information at rest in the cloud environment?	Pct%
Yes	36%
No	56%
Unsure	8%
Total	100%

Q27b. If yes, how is encryption, tokenization or other cryptographic solution applied?	Pct%
Sensitive or confidential information is made unreadable before it is sent to the cloud	46%
Sensitive or confidential information at rest is made unreadable in the cloud using tools supplied by your organization	24%
Sensitive or confidential information at rest is made unreadable in the cloud using tools supplied by the cloud provider	27%
Don’t know	3%
Total	100%

Q28a. Does your organization use encryption to secure sensitive of confidential information as it is sent and received by the cloud provider?	Pct%
Yes	55%
No	41%
Unsure	4%
Total	100%

Q28b. If yes, what percentage of all sensitive or confidential information transferred to the cloud environment is protected by encryption, tokenization or other cryptographic solution?	Pct%
Less than 1%	0%
Between 1% to 10%	18%
Between 11% to 25%	30%
Between 26% to 50%	24%
Between 51% to 75%	21%
Between 76% to 100%	5%
Total	100%
Extrapolated value	33%

Q29a. Does your organization encrypt or tokenize sensitive or confidential data directly within cloud applications (SaaS)?	Pct%
Yes	28%
No	59%
Unsure	13%
Total	100%

Q29b. If yes, how many applications require encryption?	Pct%
Less than 5	19%
5 to 10	35%
11 to 20	35%
More than 20	12%
Total	100%
Extrapolated value	11.3

Q29c. If yes, how important is the ability to encrypt or tokenize sensitive or confidential data to your organization's decision to use cloud resources?	
Q29c-1 Today	Pct%
Very important	36%
Important	35%
Not important	26%
Irrelevant	3%
Total	100%

Q29c-2 Over the next 2 years	Pct%
Very important	38%
Important	41%
Not important	20%
Irrelevant	2%
Total	100%

Q30. How many key management systems or encryption platforms does your organization have?	Pct%
Less than 5	43%
5 to 10	43%
11 to 20	13%
More than 20	1%
Total	100%
Extrapolated value	7.2

Q31. In general, where does your organization store encryption keys?	Pct%
Hardware	27%
Software	45%
Combination	27%
Unsure	1%
Total	100%

Q32. Who is in control of encryption keys when data is encrypted in the cloud?	Pct%
Your organization	54%
The cloud provider	20%
A third-party (i.e. neither you or your cloud provider)	17%
A combination of my organization and the cloud provider	8%
Other	1%
Total	100%

Part 6. Identity management in the cloud

Q33. What best describes your organization's approach to user access and identity management in the cloud environment?	Pct%
Separate identity management interfaces for the cloud and on-premise environment	49%
Unified identity management interface for both the cloud and on-premise environment	33%
Hybrid – combination of the above two choices	13%
Don't know	6%
Total	100%

Q34. How important are each of the following features to your organization's ability to control and secure access to cloud resources? Please use the five-point scale provided below each feature. Essential and Very important ratings combined.	Pct%
Q34a. The ability to support multiple identity federation standards including SAML	56%
Q34b. The ability to control strong authentication prior to accessing data and applications in the cloud	73%
Q34c. The ability to utilize social identities provide from trusted third parties	58%
Q34d. The ability to expand or contract usage based on the organization's current needs	57%
Q34e. The existence of short deployment cycles and the ability to add new identity management services quickly	60%
Q34f. The existence of an accelerated on-boarding process for new users	58%
Q34g. A record of consistently high availability	69%

Q35. Please rate the following statements about identity management in the cloud environment using the five-point scale provided below the item.	Pct%
Q35a. The management of user identities is more difficult in the cloud than the on-premise environment.	68%
Q35b. The use of social identities in regulating access to cloud resources increases security risk.	42%

Q36a. Does your organization permit third party users to access data in the cloud?	Pct%
Yes	62%
No	34%
Unsure	4%
Total	100%

Q36b. If yes, does your organization employ multi-factor authentication to secure access to data in the cloud environment?	Pct%
Yes	46%
No	49%
Unsure	5%
Total	100%

Q37. Does your organization deploy multi-factor authentication for internal employees' access to data in the cloud environment?	Pct%
Yes	48%
No	47%
Unsure	5%
Total	100%

Q38. What percent of cloud applications used in your organization provide user-enabled access controls?	Pct%
Less than 1%	5%
Between 1% to 10%	34%
Between 11% to 25%	42%
Between 26% to 50%	14%
Between 51% to 75%	5%
Between 76% to 100%	1%
Total	100%
Extrapolated value	18%

Q39. How often does your organization update its data protection security policies and/or methods based on threat intelligence it received?	Pct%
Very frequently	10%
Frequently	30%
Not frequently	43%
Rarely	16%
Never	2%
Total	100%

Part 7. Organization characteristics and respondent demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	1%
Director	14%
Manager/Supervisor	40%
Associate/Staff/Technician	42%
Other	1%
Total	100%

D2. Select the functional area that best describes your organizational location.	Pct%
IT operations	58%
Security	20%
Compliance	4%
Finance	2%
Lines of business (LOB)	15%
Other	0%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Defense & aerospace	1%
Education & research	3%
Financial services	17%
Health & pharmaceutical	9%
Hospitality	2%
Industrial	10%
Media & entertainment	3%
Public sector	13%
Retail	11%
Services	9%
Technology & software	7%
Transportation	4%
Utilities & energy	5%
Other	1%
Total	100%

D4. What range best defines the global employee headcount of your organization?	Pct%
Less than 500	14%
500 to 1,000	19%
1,001 to 5,000	19%
5,001 to 10,000	24%
10,001 to 25,000	13%
25,001 to 75,000	7%
More than 75,000	4%
Total	100%
Extrapolated value	11,271

Countries	Pct%
Australia	50
Benelux	11
Denmark	8
France	65
Germany	76
Greece	8
Hong Kong	15
India	62
Ireland	21
Israel	15
Italy	39
Japan	58
Malaysia	23
Netherlands	45
New Zealand	10
Norway	5
Philippines	23
Poland	19
Russian Federation	23
Saudi Arabia	37
Singapore	22
South Africa	20
South Korea	57
Spain	36
Sweden	8
Switzerland	12
Tawian	24
Thailand	6
United Arab Emirates	19
United Kingdom	431
United States	607
Vietnam	9
Total	1864
Count	31

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.