



Security of Cloud Computing Providers Study

Sponsored by CA Technologies

Independently conducted by Ponemon Institute LLC

Publication Date: April 2011

Security of Cloud Computing Providers Study

Presented by Ponemon Institute, April 2011

I. Executive Summary

CA Technologies and Ponemon Institute are pleased to present the results of the *Security of Cloud Computing Providers Study*. This paper is the second in a two-part series about the state of security in the cloud. The first study released in May 2010 was entitled, *Security of Cloud Computing Users*.¹

The purpose of both studies is to learn how users and providers of cloud computing applications, infrastructure and platforms are addressing the need to safeguard information in the cloud. In Parts I and II of this report (Executive Summary and Key Findings), we present the results of the cloud provider study. In Part III, we compare and analyze the results of the cloud provider and cloud user studies.

Cloud computing has been defined as the use of a collection of distributed services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned using an on-demand utility-like model of allocation and consumption.² Cloud service delivery models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

We surveyed 103 cloud service providers in the US and 24 in six European countries for a total of 127 separate providers. Respondents from cloud provider organizations say SaaS (55 percent) is the most frequently offered cloud service, followed by IaaS (34 percent) and PaaS (11 percent). Sixty-five percent of cloud providers in this study deploy their IT resources in the public cloud environment, 18 percent deploy in the private cloud and 18 percent are hybrid.

Cloud computing providers: Most salient findings

Following is a summary of the most salient findings from our study of cloud computing providers. We expand upon these findings in the next section of the paper.

- The majority of cloud computing providers surveyed do not believe their organization views the security of their cloud services as a competitive advantage. Further, they do not consider cloud computing security as one of their most important responsibilities and do not believe their products or services substantially protect and secure the confidential or sensitive information of their customers.
- The majority of cloud providers believe it is their customer's responsibility to secure the cloud and not their responsibility. They also say their systems and applications are not always evaluated for security threats prior to deployment to customers.
- Buyer beware – on average providers of cloud computing technologies allocate 10 percent or less of their operational resources to security and most do not have confidence that customers' security requirements are being met.
- Cloud providers in our study say the primary reasons why customers purchase cloud resources are lower cost and faster deployment of applications. In contrast, improved security or compliance with regulations is viewed as an unlikely reason for choosing cloud services.

¹See *Security of Cloud Computing Users*, Ponemon Institute, May 2010.

²See *Security Guidance for Critical Areas of Focus in Cloud Computing*, Cloud Computing Architectural Framework, Cloud Security Alliance, p.15, April 2009.

- The majority of cloud providers in our study admit they do not have dedicated security personnel to oversee the security of cloud applications, infrastructure or platforms.
- Providers of private cloud resources appear to attach more importance and have a higher level of confidence in their organization's ability to meet security objectives than providers of public and hybrid cloud solutions.
- While security as a "true" service from the cloud is rarely offered to customers today, about one-third of the cloud providers in our study are considering such solutions as a new source of revenue sometime in the next two years.

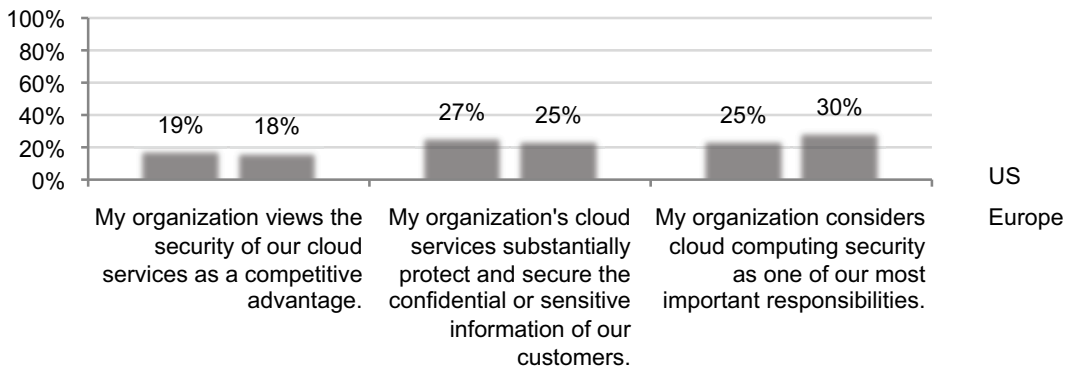
II. Key Findings

This section provides the most important findings of our cloud provider study. Whenever feasible, we provide a simple graph to illustrate the result. A tabular presentation may be provided as an alternative illustration when the result is too complex to graph.

Attributions about cloud computing security

Bar Chart 1 reports cloud providers' agreement with three attributions about cloud computing security. These findings indicate that respondents overwhelmingly believe it is the responsibility of users of cloud computing to ensure the security of cloud resources they provide. The majority does not believe their cloud services include the protection of sensitive data. Further, only 19 percent of US cloud providers and 18 percent of European cloud providers strongly agree or agree that their organization perceives security as a competitive advantage in the cloud marketplace.

Bar Chart 1: Cloud providers' attributions about cloud computing security

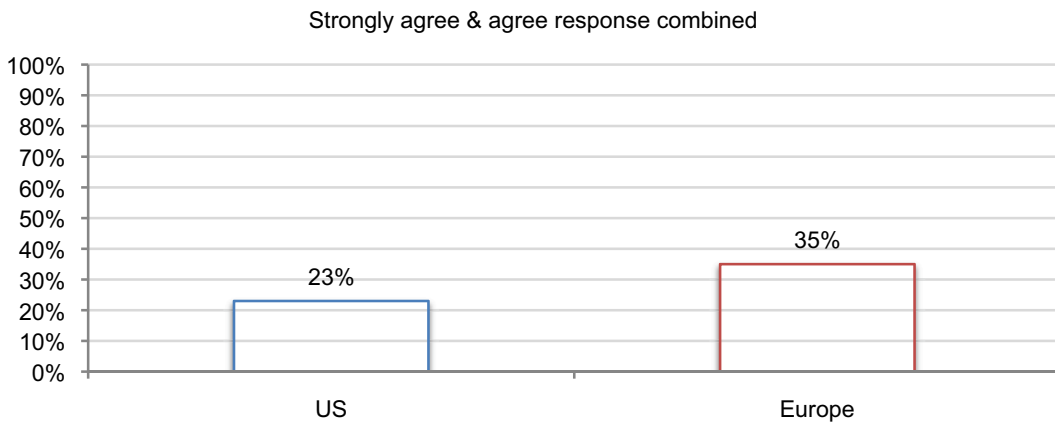


Who protects information in the cloud?

Only 23 percent of US and 35 percent of European cloud providers strongly agree and agree that IT leaders of their organizations are concerned about the security of cloud computing resources provided to their customers.

Bar Chart 2: Who is most concerned about cloud computing security

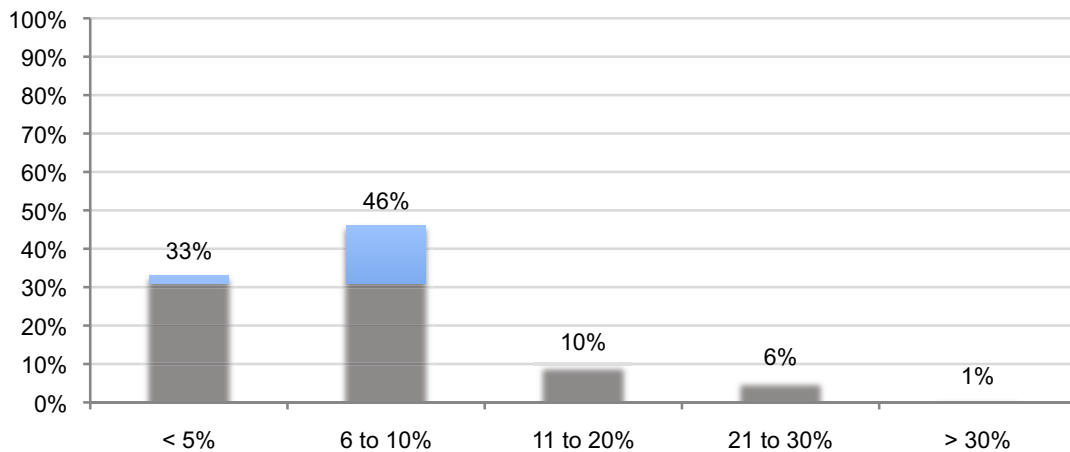
Q. IT leaders of my organization are concerned about the security of cloud computing resources provided to customers



Instead of security, cloud providers' focus on cost and speed of deployment.

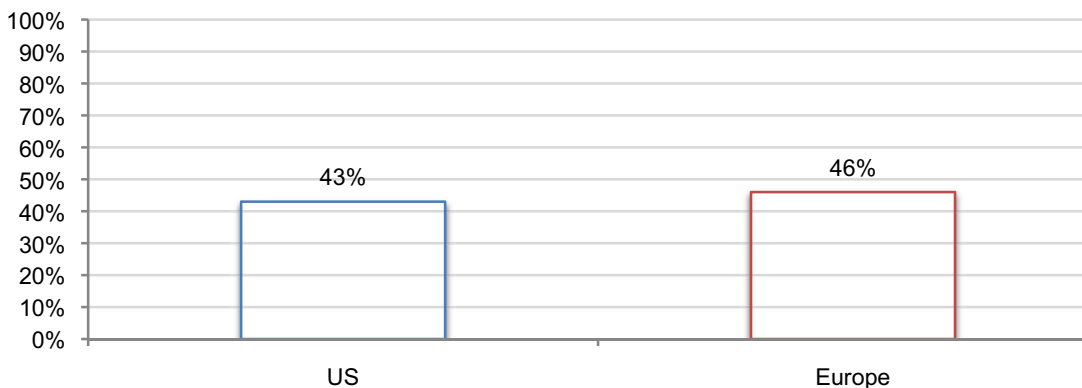
As shown in Bar Chart 3, the majority of cloud providers (79 percent) say their organizations allocate 10 percent or less of IT resources or efforts to security and control-related activities. This is consistent with the finding in Bar Chart 2 that less than half of providers in US and Europe strongly agree or agree that security in the cloud is a priority.

Bar Chart 3: Percent of resources dedicated to security and control-related activities
US & Europe results combined



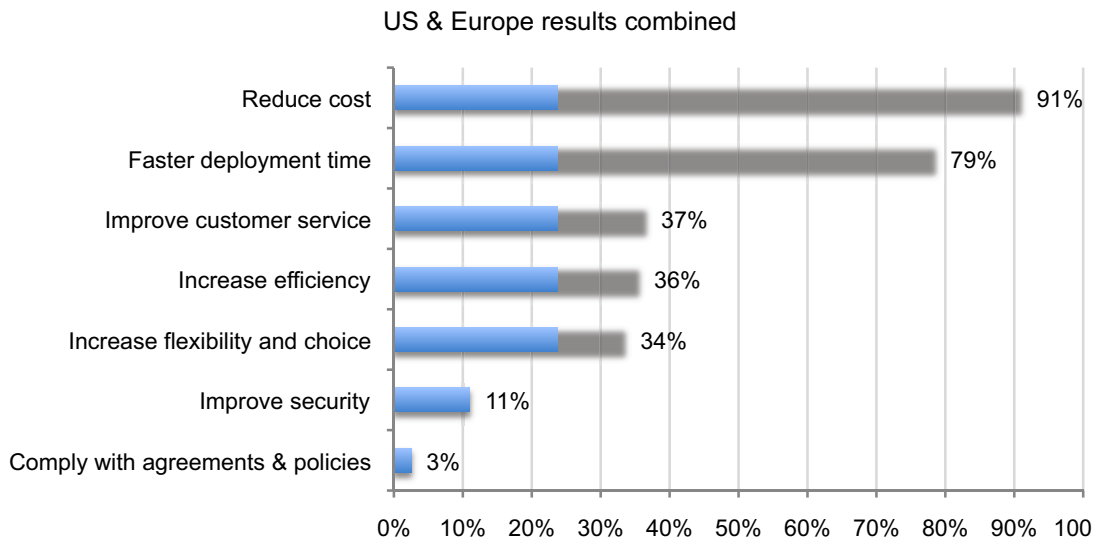
Bar Chart 4 shows that less than half of US (43 percent) and European (46 percent) cloud providers perceive security as very important or important for meeting their organization's IT and data processing objectives.

Bar Chart 4: How important is security for meeting IT and data processing objectives?
Very important & important response combined



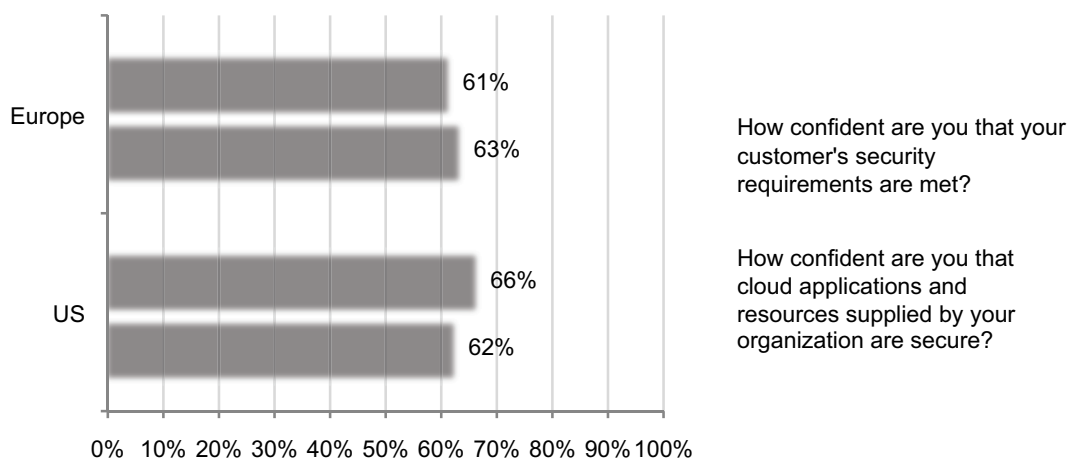
The cloud providers in our study do not think security is a reason for customers to use their services. As shown in Bar Chart 5, when asked why companies purchase cloud computing services, the top choices are reduced cost, faster deployment time, improved customer service and increased efficiency. The least cited reasons are improved security and compliance with contractual agreements or policies.

Bar Chart 5: Reasons customers migrate to the cloud computing environment



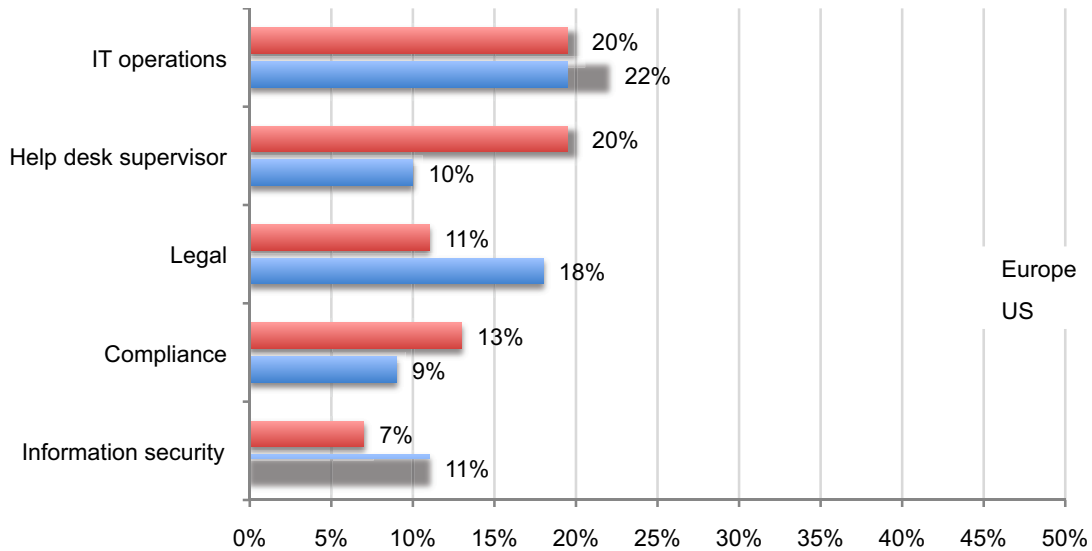
We conclude that the focus on cost and speed and not on security or data protection creates a security hole. This may explain why 62 percent of US and 63 percent of European providers are not confident or unsure that cloud applications are sufficiently secured. As noted in Bar Chart 6, two thirds of US cloud providers and 61 percent of European cloud providers are not confident or are unsure that their customer’s security requirements are met. Similarly, there is a lack of confidence that their cloud applications and other resources are secure.

Bar Chart 6: Lack of confidence in the security of cloud resources provided
Not confident & unsure response combined



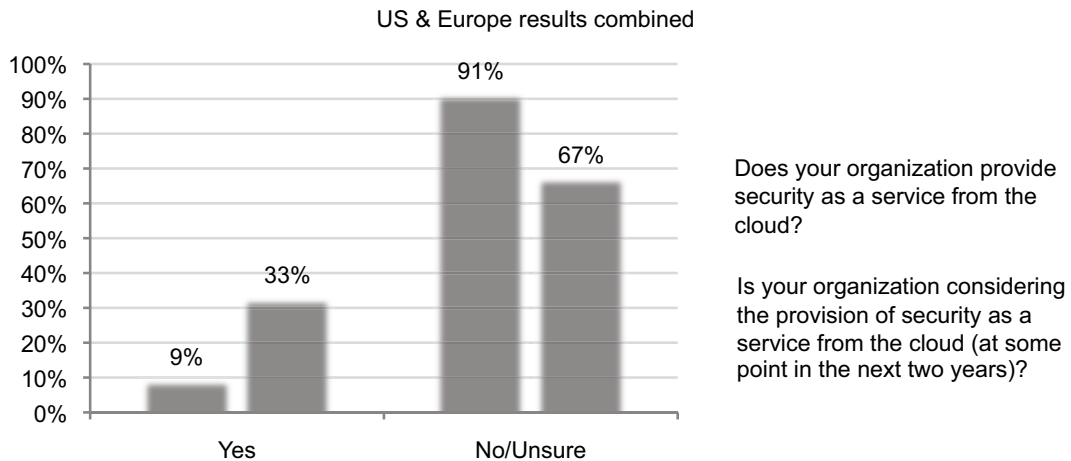
Bar Chart 7 reports the functional areas within the provider organization that are believed to be most responsible for ensuring that customer security requirements are sufficient. As can be seen, only 11 percent of US respondents and seven percent of European respondents see information security practitioners as being in-charge of provider security requirements.

Bar Chart 7: Who is most responsible for ensuring security of the providers' solutions



Bar Chart 8 provides responses to two separate but related questions about the provisioning of IT security services as a possible product offering. Most cloud providers (91 percent) do not provide security as a service from the cloud today, but about one-third are considering offering this type of service at some point in the next two years.

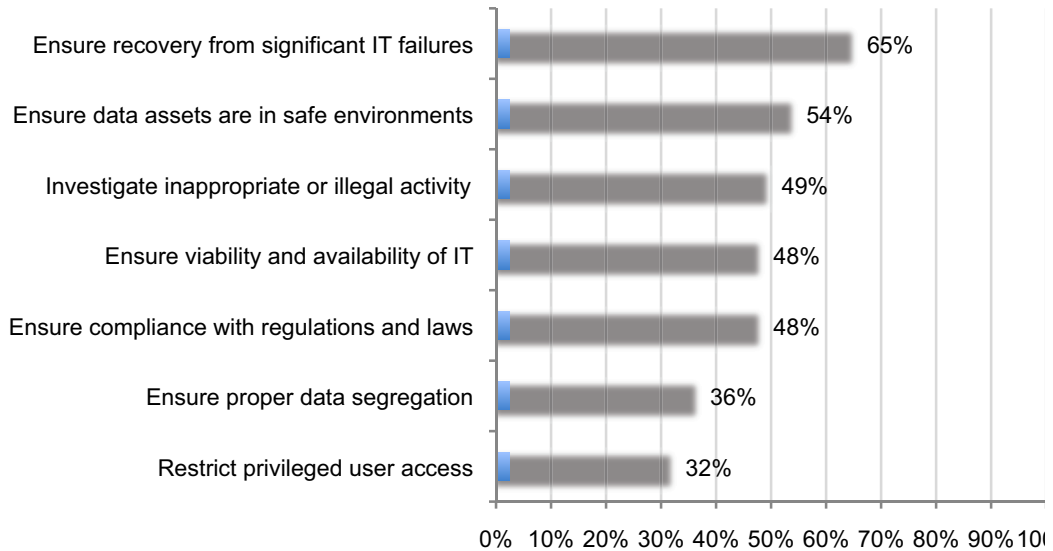
Bar Chart 8: Security as a service from the cloud



Bar Chart 9 shows seven cloud computing security risks that have been cited in the security literature. With respect to these seven risk areas, cloud providers are most confident about their ability to ensure recovery from significant IT failures and ensure the physical location of data assets are in secure environments. They are least confident in their ability to restrict privileged user access to sensitive data and ensure proper data segregation requirements are met.

Bar Chart 9: Cloud computing security risks

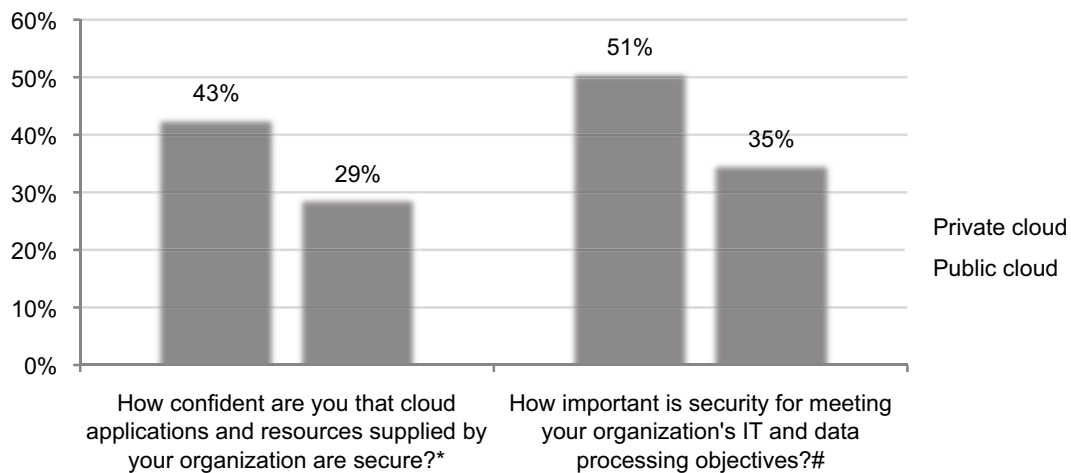
US & Europe results combined



Bar Chart 10 presents the combined responses of US and European cloud providers to two questions about the importance and level of confidence in achieving security objectives. As can be seen, IT service providers that enable private clouds attach more importance and a higher level of confidence in their organization's security posture than providers of public cloud solutions.

Bar Chart 10: Cloud computing security risks

US & Europe results combined



*Very confident and confident response combined.
 #Very important and important response combined.

Most important technologies and control activities for cloud providers

In this section, we conducted a rating of the cloud providers' security posture using 25 attributes or features of a typical security program or initiative. Table 1 lists well-known information security

objectives, where each percentage represents the confidence that providers have in their ability to meet each objective.

Table 1: How confident are you in meeting security objectives?
US & Europe results combined

| Security objectives | Very confident & confident combined |
|--|-------------------------------------|
| Access to highly qualified IT security personnel | 81% |
| Prevent or curtail viruses and malware infection | 80% |
| Secure sensitive or confidential information in motion | 71% |
| Achieve compliance with leading self-regulatory frameworks | 70% |
| Conduct training and awareness for all system users | 70% |
| Comply with all legal requirements | 69% |
| Ensure security governance processes are effective | 69% |
| Prevent or curtail system downtime and business interruption | 67% |
| Limit physical access to IT infrastructure | 66% |
| Enforce security policies | 64% |
| Conduct independent audits | 62% |
| Monitor network/traffic intelligence | 61% |
| Secure endpoints to the network | 59% |
| Prevent or curtail data loss or theft | 57% |
| Know where information assets are physically located | 57% |
| Control all live data used in development and testing | 56% |
| Perform patches to software promptly | 54% |
| Prevent or curtail system-level connections from insecure endpoints | 54% |
| Secure sensitive or confidential information at rest | 52% |
| Ensure security program is adequately managed | 49% |
| Determine the root cause of cyber attacks | 48% |
| Encrypt sensitive or confidential information assets whenever feasible | 48% |
| Prevent or curtail external attacks | 42% |
| Secure vendor relationships before sharing information assets | 42% |
| Identify and authenticate users before granting access | 37% |

In general, cloud providers are most confident about their ability to accomplish the following stated security requirements:

- Access to highly qualified IT security personnel
- Prevent or curtail viruses and malware infection
- Secure sensitive or confidential information in motion
- Achieve compliance with leading self-regulatory frameworks
- Conduct training and awareness for all system users

In contrast, cloud providers are least confident about the following security requirements:

- Identify and authenticate users before granting access
- Secure vendor relationships before sharing information assets
- Prevent or curtail external attacks
- Encrypt sensitive or confidential information assets whenever feasible
- Determine the root cause of cyber attacks

The following table lists enabling security technologies that providers presently deploy within their organizations (or plan to deploy over the next year).

Table 2: Enabling security technologies deployed by cloud providers
 Percentage reflects technologies presently used or that will be deployed in the next 12 months
 US & Europe results combined

| Enabling security technologies | Percent deployed or will be deployed |
|--|--------------------------------------|
| Firewalls | 94% |
| Anti-virus & anti-malware | 78% |
| Encryption for data in motion | 58% |
| Patch management | 47% |
| Log management | 44% |
| Encryption for data at rest | 43% |
| Whitelisting solutions | 38% |
| Intrusion detection or prevention | 38% |
| Database scanning and monitoring | 34% |
| Identity & access management (IAM) | 31% |
| ID & credentialing system | 31% |
| Service oriented architecture (SOA) security | 27% |
| Network intelligence systems | 25% |
| Virtual private network (VPN) | 25% |
| Privileged password management | 23% |
| Endpoint solutions | 22% |
| Web application firewalls (WAF) | 21% |
| Perimeter or location surveillance | 19% |
| User management and provisioning | 15% |
| Encryption for wireless communication | 15% |
| Access governance systems | 13% |
| Correlation or event management | 10% |
| Data loss prevention (DLP) | 8% |
| Single sign-on (SSO) | 6% |

The enabling security technologies most often used by US and European providers in the cloud computing environment are:

- Firewalls
- Anti-virus and anti-malware
- Encryption for data in motion
- Patch management
- Log management

The enabling security technologies least used by US and European providers in the cloud computing environment are:

- Single sign-on
- Data loss prevention
- Correlation or event management
- Access governance systems
- Encryption for wireless communication

III. Cloud Providers & Cloud Users: A Comparison

Looking at cloud computing from both sides now reveals the factors that put information at risk in the cloud. Comparing the findings from both studies reveals that neither the company that provides the services nor the company that uses cloud computing seem willing to assume responsibility for security in the cloud.

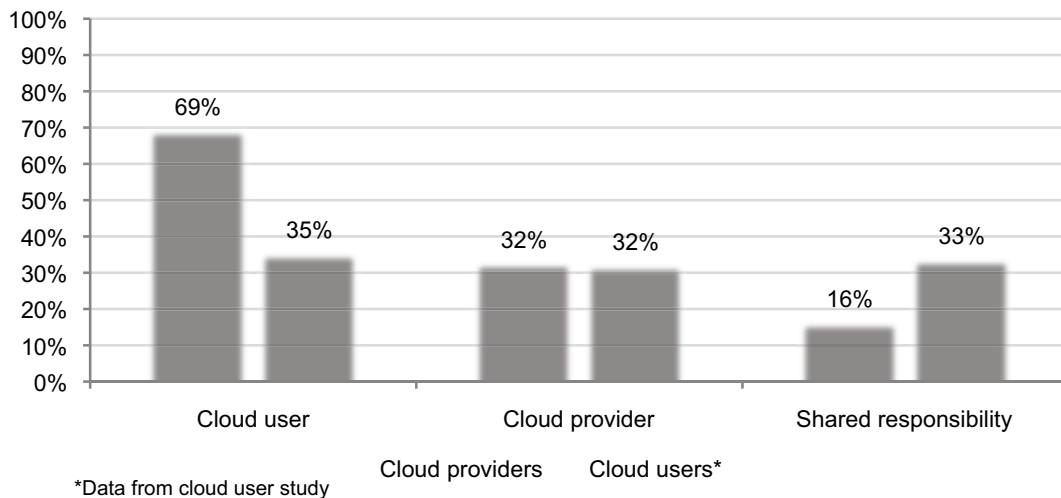
In addition, cloud computing users admit they are not vigilant in conducting audits or assessments of cloud computing providers before deployment. They also seem to be frustrated because decisions to use certain applications are made by end-users who may not have the knowledge or expertise to properly evaluate security risks.

In May 2010, CA Technologies and Ponemon Institute released the *Security of Cloud Computing Users* study, involving 642 US and 283 European cloud-computing users.

The purpose of this earlier study was to learn from IT and IT security practitioners the current state of cloud computing security in their organizations and the most significant changes anticipated as computing resources migrate from on-premises to the cloud.

Bar Charts 11 shows the different perceptions about who is responsible for security in the cloud. According to this chart, both 32 percent of cloud users and cloud providers believe the **cloud provider** is most responsible for ensuring the security of cloud services. In sharp contrast, 69 percent of cloud providers see the **cloud user** as most responsible for security, while only 35 percent of users believe they are most responsible for ensuring security.

Bar Chart 11: Who is most responsible for ensuring the security of cloud resources by cloud providers?

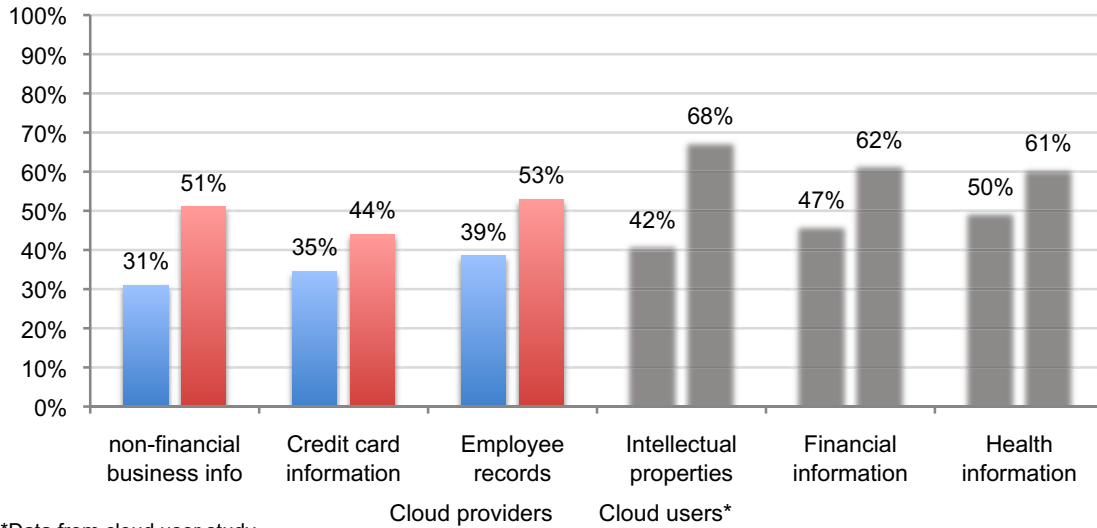


These different perceptions between cloud providers and cloud users about who is responsible for securing the cloud means organizations may be over relying on their cloud vendors to ensure safe cloud computing. Despite the risks to data in the cloud, it is interesting that providers do not consider the security of cloud services as a competitive advantage.

Both cloud users and providers share similar perceptions about which data is most risky in the cloud. Bar Chart 12 reports six categories of data that may be housed in cloud environments. As reported, 61 percent of cloud users and 50 percent of cloud providers see health information as too risky for the cloud. In addition, 62 percent of cloud users and 47 percent of cloud providers see financial information as too risky for the cloud. The widest gap in perceptions concerns intellectual properties. Sixty-eight percent of cloud users see information containing intellectual

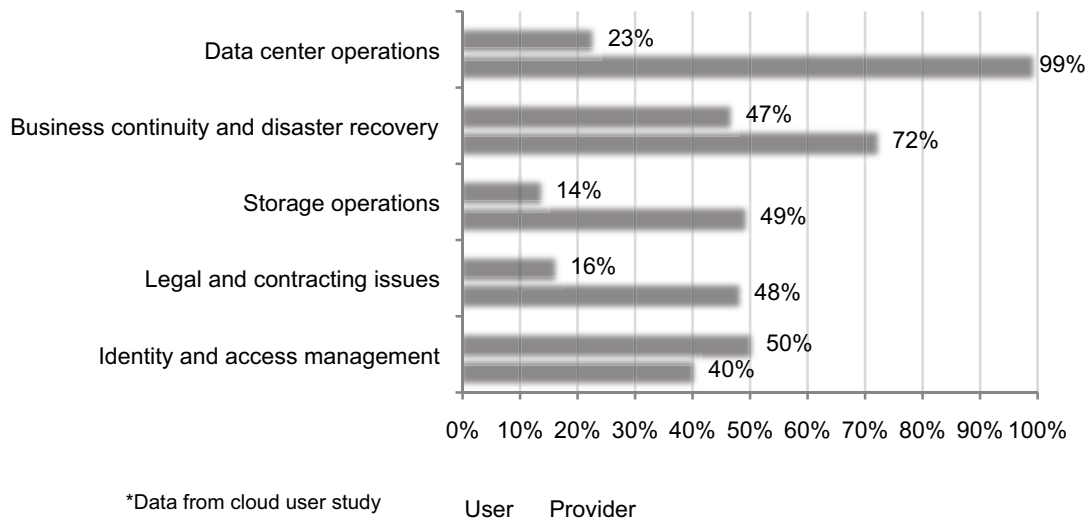
properties as too risky for the cloud, while only 42 percent of cloud providers see this type of information asset as too risky.

Bar Chart 12: Types of information too risky for the cloud
US & Europe results combined



The Cloud Security Alliance (CSA) has advanced 14 IT operation areas as “critical areas of focus” for organizations deploying cloud computing resources.³ We asked respondents in both the cloud user study and cloud provider studies to select the IT operation from the 14 areas they believe are critical areas of focus for the security of their operations. The five top-rated critical IT operations according to both cloud users and cloud providers are shown in Bar Chart 13. As can be seen, cloud providers and cloud users have different priorities for their security practices.

Bar Chart 13: Critical areas of security for cloud providers
US & Europe results combined



³See question 21 in the attached Appendix to see all 14 critical areas of focus included in our study.

Specifically, nearly all cloud providers see data center operations as a critical area of focus, as compared to only 23 percent of cloud users. In addition, more than 72 percent of cloud providers see business continuity and disaster recovery as a critical area of focus in comparison to 47 percent of cloud users. With respect to storage operations, 49 percent of cloud providers versus 14 percent of cloud users see this as a critical security priority. As shown in the above bar chart, 50 percent of cloud users in comparison to 40 percent of cloud providers report identity and access management as a critical area of focus.

In the cloud users study, we learned that users of cloud computing are not any more diligent in protecting cloud resources. Only 36 percent of US and 57 percent of European cloud computing users strongly agree or agree that their organization is vigilant in conducting audits or assessments of cloud computing providers before deployment.⁴

⁴ Ibid 1, see Table 1 entitled, "Attributions about cloud computing security" p.3.

IV. Methods

Our study involved two independent judgmental consisting of IT practitioners who represent cloud computing providers (companies) located throughout the United States and six European nations.

Using proprietary contact methods, 1,180 companies in the US and 263 companies in certain European countries were identified as possible participants in a web/telephone survey. Table 3, shows our final samples the US and Europe are 103 and 24 separate organizations, respectively. Appropriate screening criteria were used to ensure respondents were employed by companies that presently provided cloud computing services publicly, privately or as a hybrid service.

| Table 3: Sample response | US | Europe |
|---------------------------------|-------|--------|
| Organizations | 1,180 | 263 |
| Contacts made (by phone) | 879 | 240 |
| Returned surveys | 130 | 32 |
| Rejections for reliability | 27 | 8 |
| Final sample | 103 | 24 |

Pie Chart 1 reports the countries where 24 European companies are located. As can be seen, UK (46 percent) and Germany (25 percent) represent the two largest segments for this small European sample of provider companies.

Pie Chart 1: Country locations of respondents in the European sample

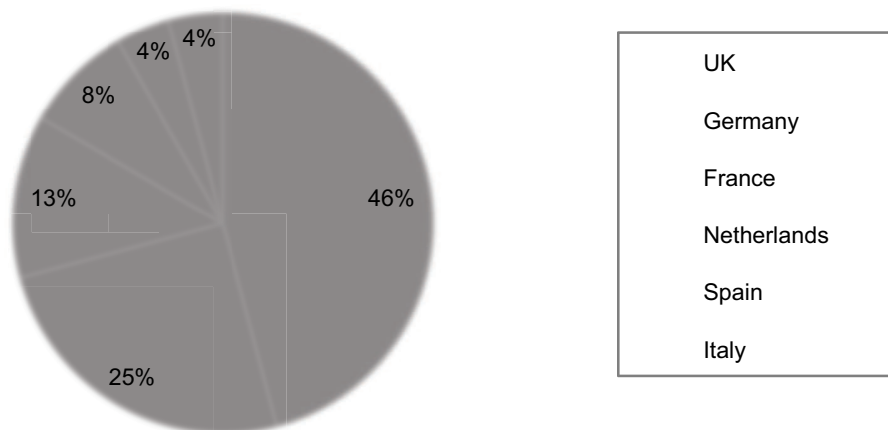


Table 4 reports the organizational level of respondents in both the US and European samples. As shown, a majority of respondents are at or above the supervisory level in their organizations.

| Table 4: Respondents' organizational level | US | Europe |
|---|------|--------|
| Senior Executive | 2% | 5% |
| Vice President | 2% | 5% |
| Director | 28% | 30% |
| Manager | 16% | 22% |
| Supervisor | 10% | 0% |
| Staff or technician | 39% | 26% |
| Contractor or other | 3% | 12% |
| Total | 100% | 100% |

Table 5 reports the respondents' reporting channel. As can be seen, a majority of respondents report through their organization's CIO, CTO, CISO and others.

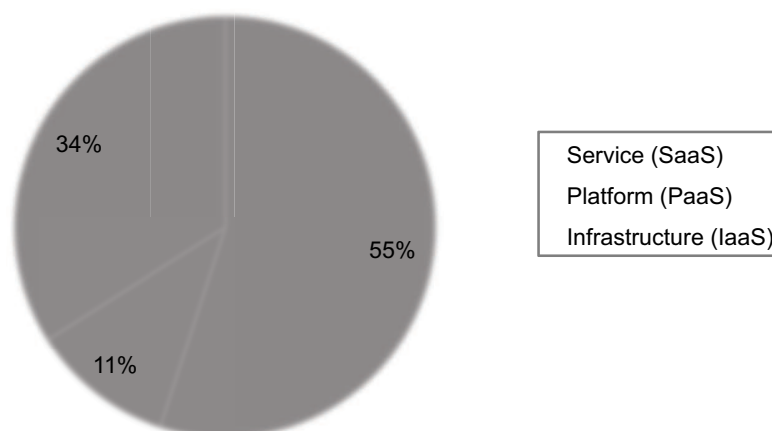
| Table 5: Respondents' reporting channel or chain-of-command | US | Europe |
|---|------|--------|
| Chief Information Officer | 67% | 65% |
| Chief Technology Officer | 8% | 15% |
| Chief Information Security Officer | 3% | 5% |
| Chief Financial Officer | 6% | 5% |
| CEO/Executive Committee | 9% | 5% |
| Compliance Officer | 0% | 5% |
| Chief Risk Officer | 5% | 0% |
| Other | 2% | 0% |
| Total | 100% | 100% |

Table 6 reports the worldwide headcount of respondent organizations, which is used as a surrogate for organizational size. As reported, a majority of respondents work in organizations with more than 1,000 employees.

| Table 6: Worldwide headcount of respondents' organization? | US | Europe |
|--|------|--------|
| Less than 500 people | 23% | 29% |
| 500 to 1,000 people | 19% | 21% |
| 1,001 to 5,000 people | 28% | 16% |
| 5,001 to 10,000 people | 20% | 27% |
| 10,001 to 25,000 people | 4% | 0% |
| 25,001 to 75,000 people | 4% | 0% |
| More than 75,000 people | 2% | 7% |
| Total | 100% | 100% |

Pie Chart 2: Cloud services provided by respondents' organizations

Pie Chart 2 reports the distribution of cloud computing services provided by organizations in this study. As can be seen, software as a service represents the largest business segment, followed by infrastructure services and platform services.



V. Caveats & Conclusion

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 surveys.

- Non-response bias: The current findings are based on a judgmental sample and 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 practitioners employed in cloud computing provider organizations. We also acknowledge bias caused by compensating subjects to complete this research within a short holdout period. In addition, 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 a truthful response.

VI. Final thoughts

The key finding in this study is that providers of cloud computing resources are not focused on security in the cloud. Rather, their priority is delivering the features their customers want such as low cost solutions with fast deployment that improves customer service and increases the efficiency of the IT function. As a result, providers in our study conclude that they cannot warrant or provide complete assurance that their products or services are sufficiently secure.

Given the well-publicized concerns about the potential risks to organizations' sensitive and confidential information in the cloud, we believe it is only a matter of time when users of cloud computing solutions will demand enhanced security features. However, until this happens users of cloud computing should be aware of their responsibility to assess the risks before migrating to the cloud.

It is important that end-users, who are making many of the decisions to work in the cloud, should be educated about the need to thoroughly vet applications for their ability to safeguard information in the cloud. Finally, cloud users and providers should consider the importance of working together to create a secure and less turbulent computing environment.

Appendix 1. Detailed Survey Findings

Ponemon Institute independently conducted all research. All survey responses are provided in the following frequency or percentage frequency tables.

| Sample response | US | Europe | Total |
|--|-------|--------|-------|
| Judgmental sample (separate organizations) | 1,180 | 263 | 1,443 |
| Contacts made | 879 | 240 | 1,119 |
| Returned surveys | 130 | 32 | 162 |
| Rejections for reliability | 27 | 8 | 35 |
| Final sample | 103 | 24 | 127 |
| Participation rate | 8.7% | 9.1% | 8.8% |

| I. Background | | | |
|---|-----|--------|-------|
| Q1. What types of cloud computing resources do you offer? Note that a company may provide more than one service type. | US | Europe | Total |
| Software as a service (SaaS) | 65 | 25 | 90 |
| Platform as a service (PaaS) | 13 | 5 | 18 |
| Infrastructure as a service (IaaS) | 49 | 7 | 56 |
| Total | 127 | 37 | 164 |

| Q2. What types of cloud computing resources do you offer? | US | Europe | Average |
|---|------|--------|---------|
| Software as a service (SaaS) | 51% | 68% | 55% |
| Platform as a service (PaaS) | 10% | 14% | 11% |
| Infrastructure as a service (IaaS) | 39% | 19% | 34% |
| Total | 100% | 100% | 100% |

| Q3. What best describes your organization's primary cloud computing deployment approach? Normalized to sum to 100%. | US | Europe | Total |
|---|------|--------|-------|
| Private cloud | 12% | 23% | 18% |
| Public cloud | 74% | 56% | 65% |
| Hybrid | 14% | 21% | 18% |
| Total | 100% | 100% | 100% |

| II. Attributions about cloud computing security (strongly agree & agree combined) | | | |
|--|-----|--------|---------|
| | US | Europe | Average |
| Q4a. My organization's cloud services substantially protect and secure the confidential or sensitive information of our customers. | 27% | 25% | 26% |
| Q4b. My organization considers cloud computing security as one of our most important responsibilities. | 25% | 30% | 28% |
| Q4c. My organization views the security of our cloud services as a competitive advantage. | 19% | 18% | 19% |

| Q5. In your opinion, who is most responsible for ensuring the security of cloud resources provided by your organization? | US | Europe | Average |
|---|------|--------|---------|
| The cloud computing service provider | 15% | 16% | 16% |
| The cloud computing user | 75% | 62% | 69% |
| Shared responsibility between the provider and user of cloud services | 10% | 22% | 16% |
| Total | 100% | 100% | 100% |

| Q6. What percent of your organization's resources or effort is dedicated to security and control-related activities? | US | Europe | Average |
|--|------|--------|---------|
| Less than 5% | 35% | 31% | 33% |
| Between 6 to 10% | 47% | 45% | 46% |
| Between 11 to 20% | 6% | 13% | 10% |
| Between 21 to 30% | 5% | 6% | 6% |
| Between 31 to 40% | 1% | 0% | 1% |
| Between 41 to 50% | 0% | 0% | 0% |
| More than 50% | 0% | 0% | 0% |
| Don't know | 6% | 5% | 6% |
| Total | 100% | 100% | 100% |
| Extrapolated value | 7% | 8% | 8% |

| Q7. How important is security for meeting your organization's IT and data processing objectives? | US | Europe | Average |
|--|-----|--------|---------|
| Very important | 13% | 14% | 14% |
| Important | 30% | 32% | 31% |
| Combined | 43% | 46% | 45% |

| Q8. How confident are you that cloud applications and resources supplied by your organization are secure? | US | Europe | Average |
|---|-----|--------|---------|
| Very confident | 18% | 15% | 17% |
| Confident | 20% | 22% | 21% |
| Combined | 38% | 37% | 38% |

| Q9. Are new cloud applications evaluated for security prior to deployment for customer organizations? | US | Europe | Average |
|---|------|--------|---------|
| Always | 11% | 16% | 14% |
| Most of the time | 30% | 28% | 29% |
| Some of the time | 43% | 50% | 47% |
| Rarely | 5% | 0% | 3% |
| Never | 11% | 6% | 9% |
| Total | 100% | 100% | 100% |

| Q10. In your opinion (best guess), what are the primary reasons why companies engage your organization for cloud computing services? Please select only three choices. | US | Europe | Average |
|--|------|--------|---------|
| Reduce cost | 90% | 92% | 91% |
| Increase efficiency | 35% | 36% | 36% |
| Improve security | 9% | 13% | 11% |
| Faster deployment time | 77% | 80% | 79% |
| Increase flexibility and choice | 38% | 29% | 34% |
| Improve customer service | 35% | 38% | 37% |
| Comply with contractual agreements or policies | 5% | 0% | 3% |
| Other | 0% | 0% | 0% |
| Total | 289% | 288% | 289% |

| Q11. How confident are you that your customer's security requirements are met? | US | Europe | Average |
|--|-----|--------|---------|
| Very confident | 11% | 15% | 13% |
| Confident | 23% | 24% | 24% |
| Combined | 34% | 39% | 37% |

| Q12. Who in your organization is most responsible for ensuring that your customer's security requirements are met? | US | Europe | Average |
|--|------|--------|---------|
| IT operations | 22% | 20% | 21% |
| Information security | 11% | 7% | 9% |
| Compliance | 9% | 13% | 11% |
| Legal | 18% | 11% | 15% |
| Internal audit | 0% | 0% | 0% |
| Help desk supervisor | 10% | 20% | 15% |
| No one person | 30% | 29% | 30% |
| Total | 100% | 100% | 100% |

IV. Security posture

Q13. The following matrix lists 25 attributions that define an effective IT security environment. Please assess the effectiveness of your organization's cloud computing security environment with respect to applications, platforms and infrastructure you provide to customer organizations. The four-point scale provided to the right of each attribute should be used to define your level of confidence in being able to accomplish the stated security requirement. 1 = very confident, 2 = confident, 3 = somewhat confident, 4 = not confident.

| Security objectives (confident & very confident combined) | US | Europe | Average |
|--|-----|--------|---------|
| Determine the root cause of cyber attacks | 50% | 46% | 48% |
| Know where information assets are physically located | 83% | 31% | 57% |
| Secure sensitive or confidential information at rest | 64% | 40% | 52% |
| Secure sensitive or confidential information in motion | 69% | 73% | 71% |
| Secure endpoints to the network | 63% | 55% | 59% |
| Identify and authenticate users before granting access | 39% | 35% | 37% |
| Secure vendor relationships before sharing information assets | 39% | 44% | 42% |
| Prevent or curtail data loss or theft | 61% | 53% | 57% |
| Prevent or curtail external attacks | 38% | 45% | 42% |
| Limit physical access to IT infrastructure | 85% | 46% | 65% |
| Ensure security governance processes are effective | 76% | 61% | 69% |
| Prevent or curtail system downtime and business interruption | 66% | 68% | 67% |
| Prevent or curtail system-level connections from insecure endpoints | 59% | 48% | 53% |
| Comply with all legal requirements | 69% | 69% | 69% |
| Achieve compliance with leading self-regulatory frameworks including | 76% | 63% | 69% |
| Prevent or curtail viruses and malware infection | 85% | 74% | 80% |
| Perform patches to software promptly | 47% | 60% | 53% |
| Control all live data used in development and testing | 53% | 58% | 55% |
| Enforce security policies | 70% | 58% | 64% |
| Access to highly qualified IT security personnel | 81% | 80% | 80% |
| Conduct training and awareness for all system users | 79% | 60% | 69% |
| Conduct independent audits | 67% | 57% | 62% |
| Ensure security program is adequately managed | 58% | 39% | 49% |
| Monitor network/traffic intelligence | 67% | 54% | 61% |
| Encrypt sensitive or confidential information assets whenever feasible | 48% | 48% | 48% |

Q14. Please review the following list of 25 enabling security technologies. Then select each technology that your organization presently deploys in the cloud computing environment. Please include those technologies that are presently in-process of being deployed in the next 12 months.

| Important and very important combined | US | Europe | Average |
|--|-----|--------|---------|
| Access governance systems | 15% | 10% | 13% |
| Anti-virus & anti-malware | 73% | 82% | 77% |
| Correlation or event management | 13% | 7% | 10% |
| Data loss prevention (DLP) | 16% | 0% | 8% |
| Database scanning and monitoring | 45% | 23% | 34% |
| Encryption for data at rest | 35% | 50% | 43% |
| Encryption for data in motion | 36% | 79% | 58% |
| Encryption for wireless communication | 19% | 10% | 14% |
| Endpoint solutions | 25% | 19% | 22% |
| Firewalls | 96% | 91% | 94% |
| Identity federation | 0% | 0% | 0% |
| ID & credentialing system | 26% | 35% | 30% |
| Identity & access management (IAM) | 35% | 27% | 31% |
| Intrusion detection or prevention | 40% | 35% | 38% |
| Log management | 42% | 45% | 43% |
| Network intelligence systems | 25% | 24% | 25% |
| Patch management | 50% | 43% | 47% |
| Perimeter or location surveillance | 16% | 22% | 19% |
| Privileged password management | 26% | 20% | 23% |
| Service oriented architecture (SOA) security | 27% | 27% | 27% |
| Single sign-on (SSO) | 11% | 0% | 6% |
| User management and provisioning | 13% | 17% | 15% |
| Virtual private network (VPN) | 27% | 22% | 24% |
| Whitelisting solutions | 38% | 37% | 38% |
| Web application firewalls (WAF) | 23% | 19% | 21% |
| Average | 31% | 30% | 30% |

Q15a. Does your organization provide security as a service from the cloud?

| | US | Europe | Average |
|--------|------|--------|---------|
| Yes | 8% | 10% | 9% |
| No | 91% | 90% | 91% |
| Unsure | 1% | 0% | 0% |
| Total | 100% | 100% | 100% |

Q15b. Is your organization considering the provision of security as a service from the cloud (at some point in the next two years)?

| | US | Europe | Average |
|--------|------|--------|---------|
| Yes | 30% | 35% | 33% |
| No | 30% | 38% | 34% |
| Unsure | 40% | 27% | 34% |
| Total | 100% | 100% | 100% |

Q16. Please review the following list of 17 system control activities. Then select each activity that your organization presently deploys in the cloud computing environment. Please include those activities that are presently in-process of being deployed in the next 12 months.

| Important and very important combined | US | Europe | Average |
|--|-----|--------|---------|
| Background checks of privileged users | 6% | 0% | 3% |
| Certifications (such as PCI DSS, ISO, NIST and others) | 56% | 32% | 44% |
| Crisis communication procedures | 41% | 26% | 34% |
| Controls assessment | 36% | 18% | 27% |
| External audit | 12% | 13% | 13% |
| Helpdesk activities | 89% | 63% | 76% |
| IT audit | 39% | 13% | 26% |
| Monitoring changes in regulatory requirements | 10% | 12% | 11% |
| Policies and procedures | 56% | 73% | 65% |
| Quality assurances | 60% | 43% | 52% |
| Redress and enforcement | 9% | 25% | 17% |
| Surveillance | 45% | 13% | 29% |
| Training of data handlers | 36% | 33% | 35% |
| Training of end users | 5% | 5% | 5% |
| Training of security practitioners | 8% | 0% | 4% |
| Vetting and monitoring of third parties | 31% | 13% | 22% |
| Average | 34% | 24% | 29% |

Q17. Gartner has advanced seven cloud computing security risks. Please rate your organization's ability to mitigate or significantly curtail this risk for IT operations in the cloud. The four-point scale provided to the right of each attribute should be used to define your level of **confidence** in being able to mitigate or curtail each risk area: 1 = very confident, 2 = confident, 3 = somewhat confident, 4 = not confident.

| Confident & very confident (combined) | US | Europe | Average |
|--|-----|--------|---------|
| Restrict privileged user access to sensitive data | 34% | 29% | 32% |
| Ensure compliance with all applicable privacy and data protection regulations and laws | 50% | 45% | 48% |
| Ensure the physical location of data assets are in secure environments | 60% | 47% | 54% |
| Ensure proper data segregation requirements are met | 42% | 30% | 36% |
| Ensure recovery from significant IT failures | 70% | 59% | 65% |
| Investigate inappropriate or illegal activity | 53% | 45% | 49% |
| Ensure long-term viability and availability of IT resources | 53% | 42% | 48% |
| Average | 52% | 42% | 47% |

| Q18. What types of confidential or sensitive information does your customers consider too risky to be stored in the cloud? | US | Europe | Average |
|---|-----|--------|---------|
| Consumer data | 10% | 12% | 11% |
| Customer information | 15% | 22% | 19% |
| Credit card information | 30% | 39% | 35% |
| Employee records | 42% | 35% | 39% |
| Health information | 49% | 51% | 50% |
| Non-financial confidential business information | 36% | 26% | 31% |
| Financial business information | 56% | 43% | 50% |
| Intellectual properties | 34% | 49% | 42% |
| Research data | 8% | 19% | 14% |
| Other (please specify) | 0% | 0% | 0% |
| None of the above | 41% | 48% | 45% |
| Average | 29% | 31% | 30% |

| Q19. What types of business applications do your customers consider too risky to be processed and housed in the cloud? | US | Europe | Average |
|---|-----|--------|---------|
| Sales and CRM applications | 19% | 30% | 25% |
| ERP applications | 25% | 28% | 27% |
| Human resource and payroll applications | 33% | 50% | 42% |
| Financial and accounting applications | 51% | 56% | 54% |
| Engineering applications | 12% | 15% | 14% |
| Manufacturing applications | 9% | 0% | 5% |
| Logistics applications | 0% | 7% | 4% |
| Scheduling and time management applications | 3% | 0% | 2% |
| Communication applications | 14% | 7% | 11% |
| Other | 3% | 0% | 2% |
| Average | 17% | 19% | 18% |

| Q20. Does your organization have a fully dedicated security team to oversee the security of cloud applications or platforms? | US | Europe | Average |
|--|-----|--------|---------|
| Yes | 26% | 19% | 23% |

| Q21. The Cloud Security Alliance (CSA) has advanced the following 14 areas as “critical areas of focus” for organizations deploying cloud computing resources. Please check each IT operation that your organization accomplishes or provides for your cloud computing customers. | | | |
|---|-----|--------|---------|
| Critical areas of focus | US | Europe | Average |
| Governance and enterprise risk management | 26% | 20% | 23% |
| Legal and contracting issues | 43% | 52% | 48% |
| Procedures for electronic discovery | 40% | 29% | 35% |
| Compliance and audit | 39% | 13% | 26% |
| Information lifecycle management | 20% | 7% | 14% |
| Portability and interoperability | 41% | 19% | 30% |
| Business continuity and disaster recovery | 68% | 75% | 72% |
| Data center operations | 98% | 100% | 99% |
| Incident response, notification and remediation | 31% | 23% | 27% |
| Application security | 19% | 11% | 15% |
| Encryption and key management | 36% | 20% | 28% |
| Identity and access management | 41% | 38% | 40% |
| Storage operations | 53% | 45% | 49% |
| Virtualization operations | 15% | 11% | 13% |
| Average | 41% | 33% | 37% |

| Q22. IT leaders of my organization are concerned about the security the cloud computing resources provided to our customers. | | | |
|--|-----|--------|---------|
| | US | Europe | Average |
| Strongly agree & agree combined | 23% | 35% | 29% |

| V. Organization characteristics and respondent demographics | | | |
|---|------|--------|---------|
| D1. What organizational level best describes your current position? | US | Europe | Average |
| Senior Executive | 2% | 5% | 4% |
| Vice President | 2% | 5% | 4% |
| Director | 28% | 30% | 29% |
| Manager | 16% | 22% | 19% |
| Supervisor | 10% | 0% | 5% |
| Staff or technician | 39% | 26% | 33% |
| Contractor | 3% | 0% | 2% |
| Other | 0% | 12% | 6% |
| Total | 100% | 100% | 100% |

| D2. Check the Primary Person you or your supervisor reports to within your organization. | US | Europe | Average |
|---|------|--------|---------|
| CEO/Executive Committee | 2% | 5% | 4% |
| Chief Financial Officer | 6% | 5% | 6% |
| Chief Information Officer | 67% | 65% | 66% |
| Chief Information Security Officer | 10% | 5% | 8% |
| Compliance Officer | 0% | 5% | 3% |
| Chief Privacy Officer | 0% | 0% | 0% |
| Director of Internal Audit | 0% | 0% | 0% |
| General Counsel | 0% | 0% | 0% |
| Chief Technology Officer | 8% | 15% | 12% |
| Human Resources Leader | 0% | 0% | 0% |
| Chief Security Officer | 0% | 0% | 0% |
| Chief Risk Officer | 5% | 0% | 3% |
| Other | 2% | 0% | 1% |
| Total | 100% | 100% | 100% |

| D3. Geographic region (location of respondent) | US | Europe | Average |
|--|------|--------|---------|
| United States | 100% | 0% | 81% |
| United Kingdom | 0% | 46% | 9% |
| Germany | 0% | 25% | 5% |
| France | 0% | 13% | 2% |
| Netherlands | 0% | 8% | 2% |
| Switzerland | 0% | 0% | 0% |
| Spain | 0% | 4% | 1% |
| Italy | 0% | 4% | 1% |
| Other | 0% | 0% | 0% |
| Total | 100% | 100% | 100% |

| Experience | US | Europe | Average |
|---|------|--------|---------|
| D4a. Total years of business experience | 14.0 | 12.1 | 13.0 |
| D4b. Total years in IT or data security | 12.4 | 11.8 | 12.1 |
| D4c. Total years in current position | 3.9 | 6.0 | 5.0 |

| D5. What industries does your organization serve? | US | Europe | Average |
|---|------|--------|---------|
| Airlines | 0% | 0% | 0% |
| Automotive | 0% | 0% | 0% |
| Agriculture | 0% | 0% | 0% |
| Brokerage | 5% | 0% | 3% |
| Cable | 0% | 0% | 0% |
| Chemicals | 0% | 0% | 0% |
| Credit Cards | 0% | 0% | 0% |
| Defense | 0% | 0% | 0% |
| Education | 6% | 18% | 12% |
| Entertainment | 0% | 0% | 0% |
| Services | 4% | 11% | 8% |
| Health Care | 6% | 0% | 3% |
| Hospitality & Leisure | 3% | 0% | 2% |
| Manufacturing | 11% | 21% | 16% |
| Insurance | 6% | 0% | 3% |
| Internet & ISPs | 1% | 0% | 1% |
| Government | 0% | 0% | 0% |
| Pharmaceutical | 0% | 0% | 0% |
| Professional Services | 10% | 0% | 5% |
| Research | 4% | 0% | 2% |
| Retail | 15% | 33% | 24% |
| Banking | 9% | 0% | 5% |
| Energy | 0% | 0% | 0% |
| Telecommunications | 0% | 0% | 0% |
| Technology & Software | 20% | 17% | 19% |
| Transportation | 0% | 0% | 0% |
| Wireless | 0% | 0% | 0% |
| Total | 100% | 100% | 100% |

| D6. What best describes your role in managing data protection and security risk in your organization? Check all that apply. | US | Europe | Average |
|---|-----|--------|---------|
| Setting priorities | 60% | 60% | 60% |
| Managing budgets | 65% | 70% | 68% |
| Selecting vendors and contractors | 43% | 28% | 36% |
| Determining privacy and data protection strategy | 44% | 35% | 40% |
| Evaluating program performance | 58% | 67% | 63% |
| Average | 54% | 52% | 53% |

| D7. What is the worldwide headcount of your organization? | US | Europe | Average |
|---|------|--------|---------|
| Less than 500 people | 23% | 29% | 26% |
| 500 to 1,000 people | 19% | 21% | 20% |
| 1,001 to 5,000 people | 28% | 16% | 22% |
| 5,001 to 10,000 people | 20% | 27% | 24% |
| 10,001 to 25,000 people | 4% | 0% | 2% |
| 25,001 to 75,000 people | 4% | 0% | 2% |
| More than 75,000 people | 2% | 7% | 4% |
| Total | 100% | 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 800 887 3118.

Ponemon Institute

Advancing Responsible Information Management

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

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