Data Protection and Privacy Compliance in the Cloud:
Privacy Concerns Are Not Slowing the Adoption of Cloud Services, but Challenges Remain

Sponsored by Microsoft | Independently conducted by Ponemon Institute LLC | January 2020

Contents

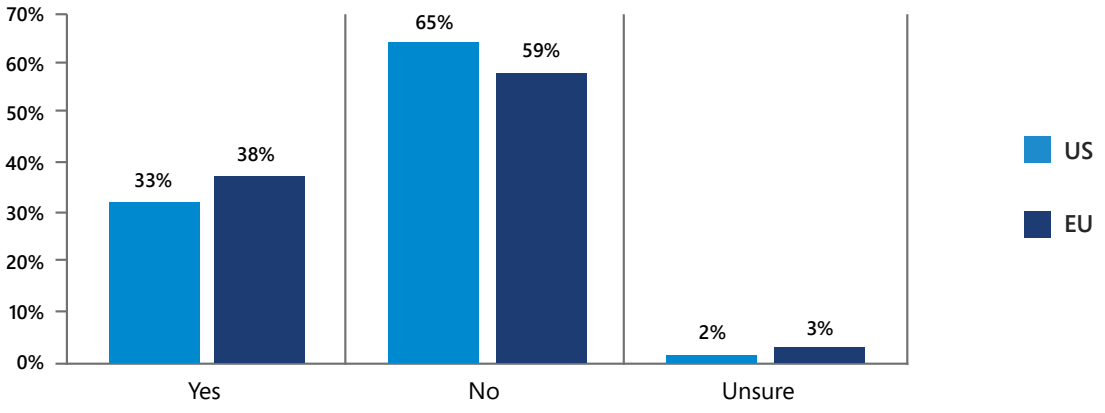
Executive Summary

The Ponemon Institute is pleased to present the findings of Data Protection and Privacy Compliance in the Cloud, sponsored by Microsoft. The purpose of this research to better understand how organizations undergo digital transformation while wrestling with the organizational impact of complying with such significant privacy regulations as the GDPR. This research explored the reasons organizations are migrating to the cloud, the security and privacy challenges they encounter in the cloud, and the steps they have taken to protect sensitive data and achieve compliance.

The Ponemon research qualified 1,049 IT and IT security participants from the United States and the European Union (EU). All of them were familiar with their organization's approach to privacy and data protection compliance and responsibility for ensuring that personal data is protected in the cloud environment. Fifty five percent of respondents operate a cloud infrastructure with one primary cloud service provider; 45 percent operate in multiple or hybrid cloud environments.

Privacy concerns are not slowing the adoption of cloud services. The importance of the cloud in reducing costs and speeding time to market seem to override privacy concerns. Only one-third of US respondents and 38 percent of EU respondents say they have stopped or slowed their adoption of cloud services because of privacy concerns, as shown in Figure 1.

Figure 1. Has your organization stopped or slowed its adoption of cloud services because of privacy concerns?



Most privacy-related activities are easier to deploy in the cloud. These include such governance practices as conducting privacy impact assessments, classifying or tagging personal data for sensitivity or confidentiality, and meeting legal obligations, such as those of the GDPR. However, managing incident response is considered easier to deploy on premises than in the cloud.

However, most organizations lack confidence in, visibility into, and a clear delineation of responsibility for managing privacy in the cloud.

- Despite the anticipated increase in the importance of the cloud in meeting privacy and data protection objectives, 53 percent of US and 60 percent of EU respondents are not confident that their organization currently meets their privacy and data protection requirements. This lack of confidence may be because most organizations are not vetting cloud-based software for privacy and data security requirements prior to deployment.
- Organizations are reactive and not proactive in protecting sensitive data in the cloud. Specifically, just 44 percent of respondents are vetting cloud-based software or platforms for privacy and data security risks, and only 39 percent are identifying information that is too sensitive to be stored in the cloud.
- Just 29 percent of respondents say their organizations have the necessary 360-degree visibility into the sensitive or confidential data collected, processed, and/or stored in the cloud. Organizations also lack confidence that they know all the cloud applications and platforms that they have deployed.
- In most organizations, the IT security and compliance teams are not responsible for ensuring security safeguards and compliance with privacy and data protection regulations. Thirty six percent of respondents expect the cloud service provider to ensure the security of SaaS applications. In contrast, 46 percent of respondents say the organization is responsible. Further, privacy and data protection teams are rarely involved in evaluating cloud applications or platforms when they are under consideration. Almost half of respondents (49 percent) rarely or never determine if certain cloud applications or platforms meet data protection and privacy requirements.

Key Findings

In this section of the report, we present a detailed analysis of the most salient findings.

- Privacy concerns are not slowing migration to the cloud, but organizations struggle to protect data.
- Organizations are having difficulty implementing privacy and data protection requirements.
- Organizations are using a variety of tools to protect sensitive data in the cloud.
- Comparing US and EU respondents' perceptions of data protection and compliance.
- Ten steps to achieving data protection and privacy in the cloud.

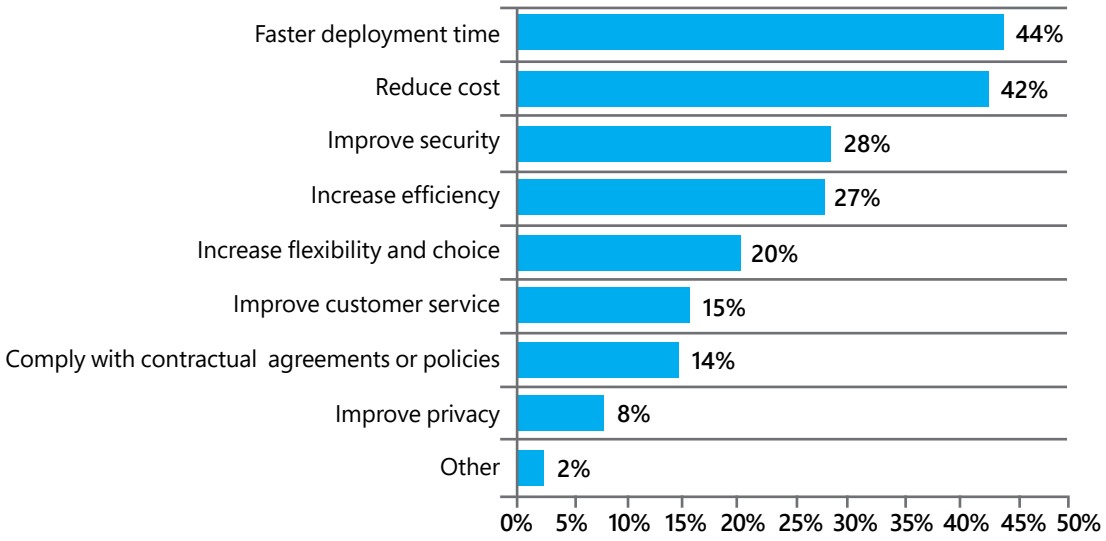
NOTE: *Unless otherwise indicated, the data analysis in the following figures and tables consolidates the findings from the United States and the European Union.*

1. Privacy concerns are not slowing migration to the cloud, but organizations struggle to ensure the protection of data

Cloud services or platforms are used to achieve faster deployment and reduce costs.

As shown in Figure 2, the top two reasons for using cloud services and platforms are faster deployment time and lower costs.

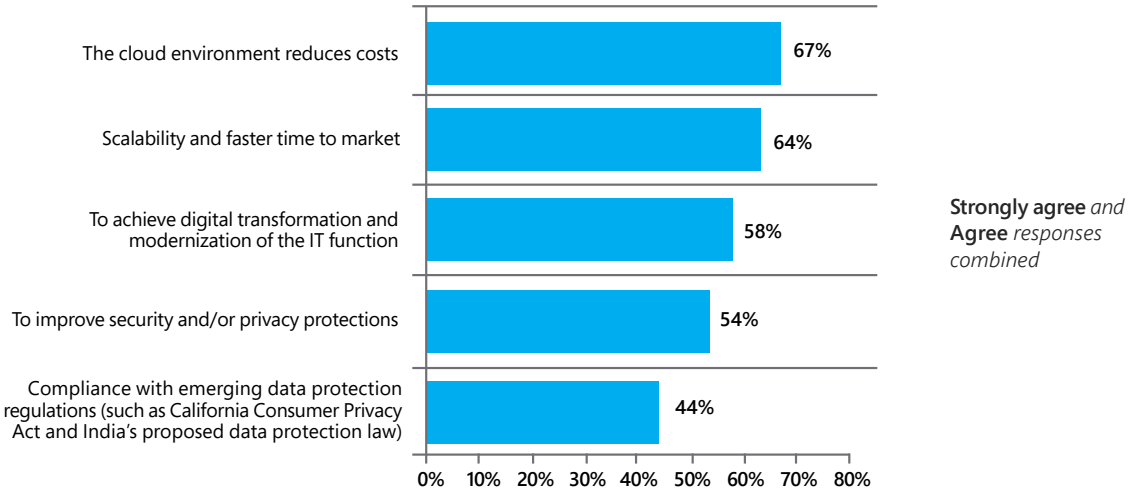
Figure 2. What are the primary reasons cloud services and/or platforms are used within your organization?



Cost savings, scalability, and faster time to market are the top reasons for migrating to the cloud.

As shown in Figure 3, 67 percent of respondents agree that migration results in cost savings and 64 percent of respondents agree that it enables scalability and faster time to market. More than half (54 percent) of the respondents believe migration will improve security and privacy protections.

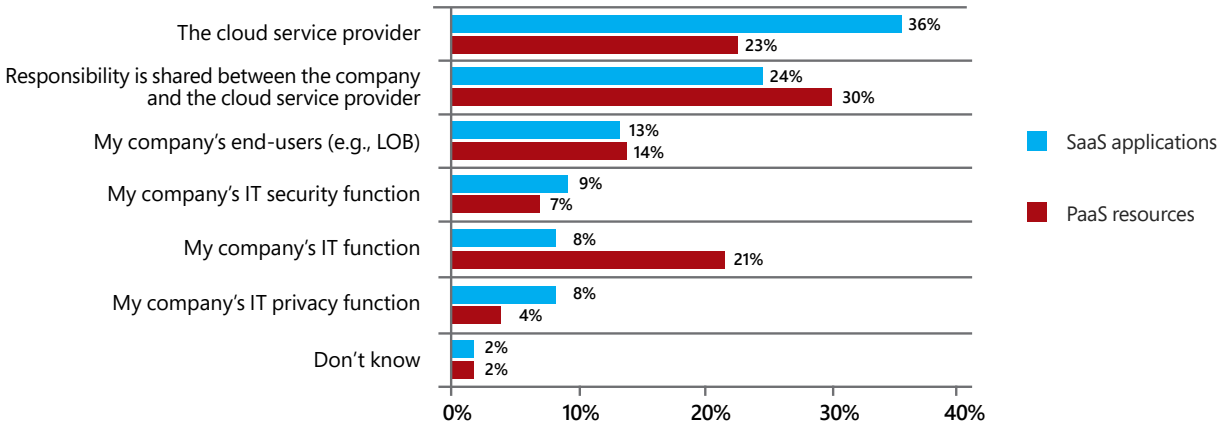
Figure 3. Reasons for migration to the cloud



There is no consensus about who is responsible for addressing privacy and data protection requirements.

Respondents were asked who in their organization would be most responsible for ensuring that SaaS and PaaS applications meet privacy and data protection requirements. As shown in Figure 4, some assigned this responsibility to the cloud service provider; some state that the company and the cloud service provider share the responsibility; others allocate the responsibility within the company among end users and IT.

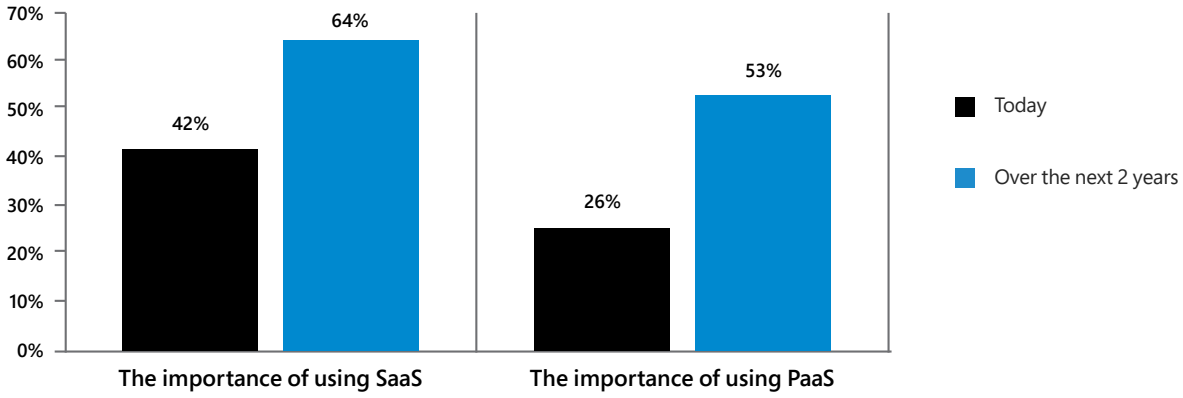
Figure 4. Who is most responsible for ensuring that SaaS and PaaS applications used in your organization meet privacy and data protection requirements?



The importance of both SaaS and PaaS in meeting privacy and data protection objectives will increase significantly.

As shown in Figure 5, 64 percent of respondents say that deploying SaaS will be essential or very important in meeting privacy and data protection objectives over the next two years. Fifty-three percent of respondents say using PaaS will be essential or very important.

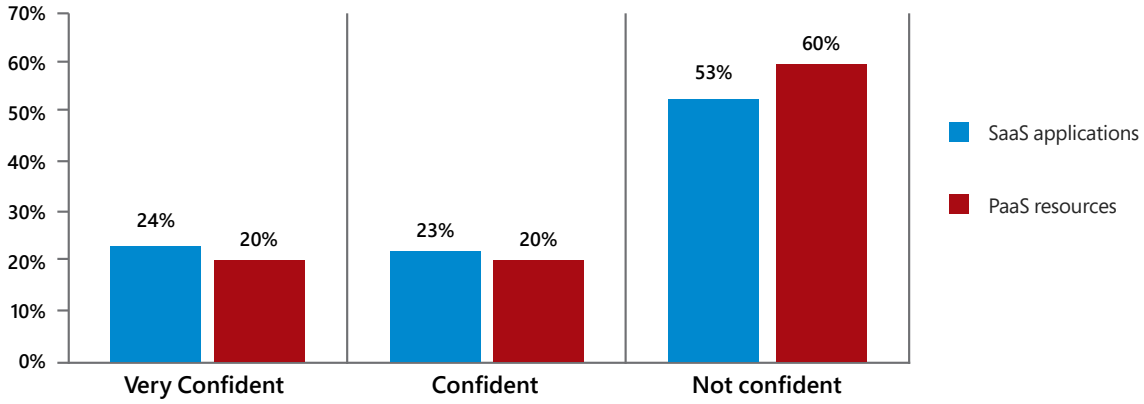
Figure 5. How important is the use of SaaS and PaaS in meeting your organization's privacy and data protection objectives today and in two years?



Respondents are not confident that their current use of SaaS and PaaS meets privacy and data protection requirements.

Currently the majority of respondents are not confident that their SaaS applications and PaaS resources meet privacy and data protection requirements. More respondents (60 percent) lack confidence in the privacy and data protection capabilities of PaaS.

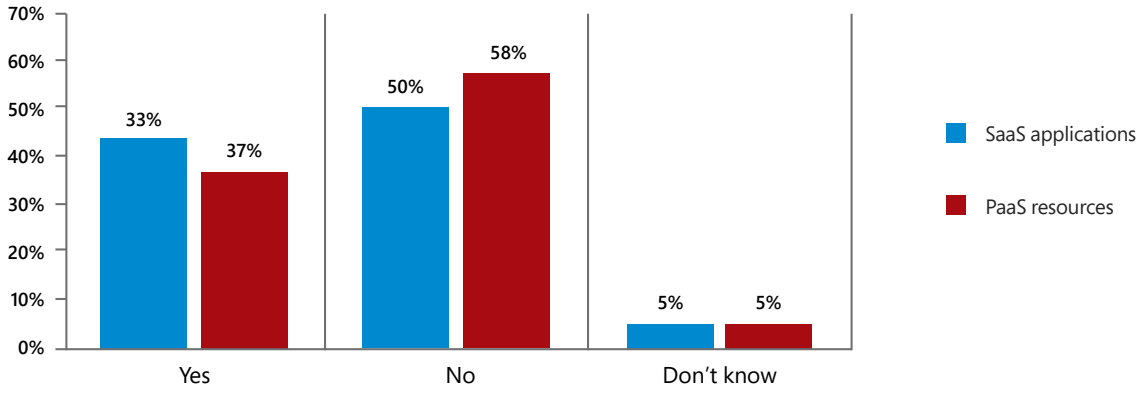
Figure 6. How confident are you that SaaS and PaaS applications used within your organization meet privacy and data protection requirements?



Confidence in SaaS and PaaS applications is low because most organizations are not vetting them for privacy and data security requirements prior to deployment.

As discussed previously, there is a lack of confidence in the ability of SaaS and PaaS applications to protect and secure data. The reason is shown in Figure 7. Fifty percent of respondents say their organizations are not vetting their SaaS applications before deployment and 58 percent say PaaS resources are not being vetted.

Figure 7. Are SaaS and PaaS applications evaluated for privacy and data security requirements prior to deployment within your organization?



2. Organizations are having difficulty implementing privacy and data protection requirements

Organizations are reactive and not proactive in protecting sensitive and confidential information in the cloud environment.

As discussed previously, most respondents are not confident in the security of their SaaS applications and PaaS processes. Moreover, those organizational functions that are most knowledgeable about compliance and security issues in the cloud are not responsible for ensuring the protection of sensitive and confidential data and compliance with regulations. In response to a question about the steps taken to protect data in the cloud environment, respondents who both "strongly agreed" and "agreed":

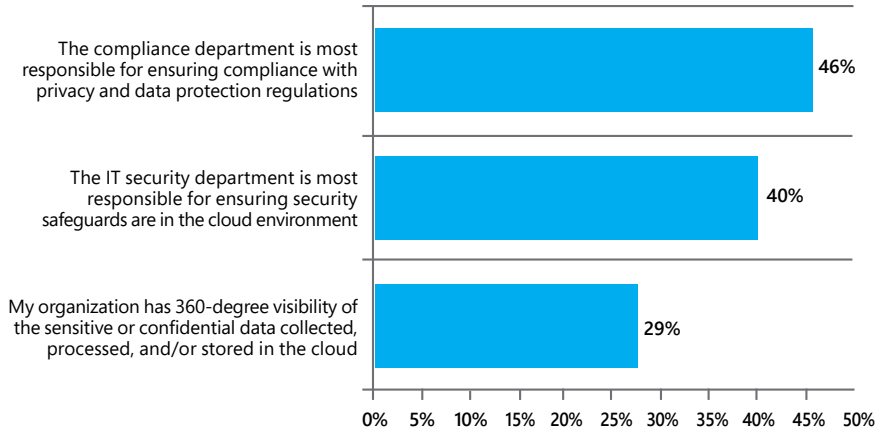
- Forty percent of organizations represented in this research did not evaluate cloud-based software and platforms to find out if they create privacy and data security risks.
- Thirty nine percent of respondents say their organizations are proactive in identifying information that is too sensitive to be stored in the cloud.
- Thirty eight percent say they are proactive in assessing the impact that cloud services may have on the ability to protect and secure confidential or sensitive information.

Organizations lack visibility into how sensitive data is collected, processed, and stored in the cloud.

Only 29 percent of respondents say their organizations have 360-degree visibility into how sensitive or confidential data is collected, processed, or stored in the cloud.

It is important to have knowledgeable individuals responsible to ensure compliance with privacy and data protection regulations and that the necessary security safeguards are in place, and yet:

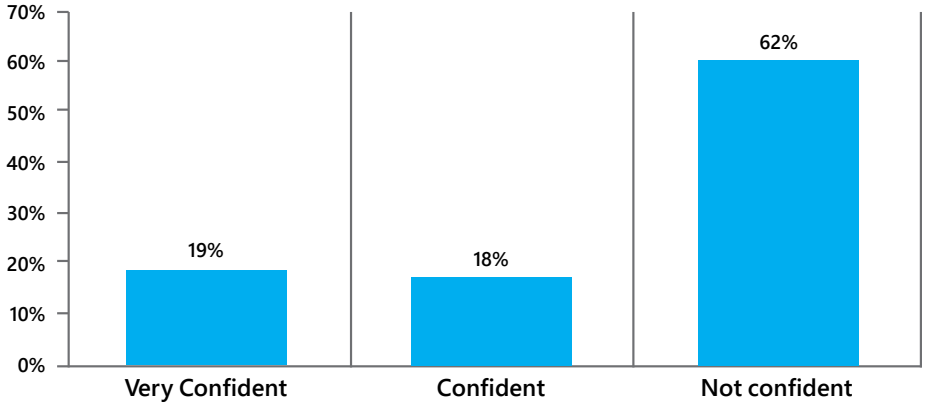
- Only 40 percent of respondents say the IT security department is most responsible for ensuring that security safeguards are in place in the cloud environment.
- Fewer than half (46 percent) say the compliance department is most responsible for ensuring compliance with privacy and data protection regulations.



Organizations also lack confidence that they know all the cloud applications in use in their organization.

In addition to the lack of visibility as described above, a roadblock to protecting data and complying with privacy regulations is that many organizations—62 percent—aren't confident that they even know all the cloud applications and platforms that they are currently using.

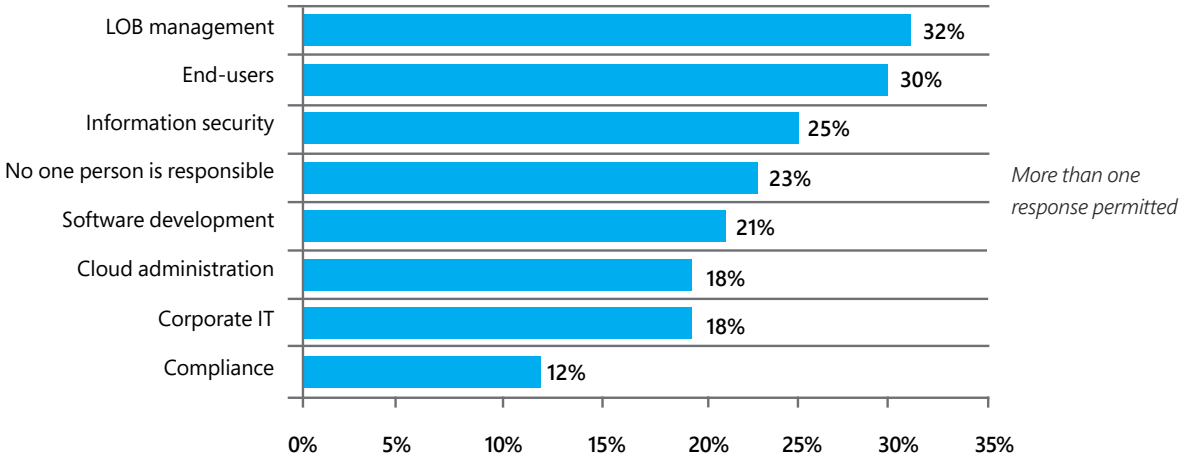
Figure 8. How confident are you that your organization knows all cloud applications and platforms in use today?



Information security and compliance functions are in most instances not responsible for meeting privacy and data protection requirements.

As shown in Figure 9, responsibility for meeting privacy and data protection requirements are dispersed throughout the organization. Sixty-two percent of respondents say it is the line of business management or end users who are responsible.

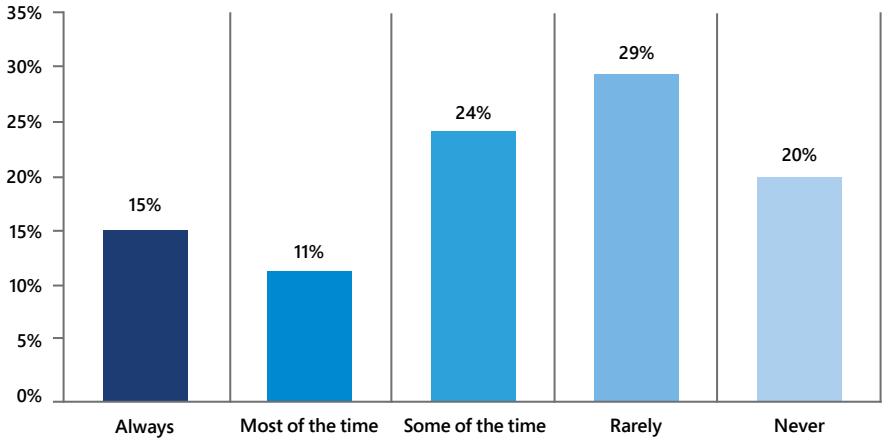
Figure 9. Which individuals or functions within your organization are responsible for ensuring cloud services and platforms meet privacy and data protection requirements?



Privacy and data protection teams are not determining the acceptability of cloud applications or platforms.

Almost half of respondents (49 percent) report that their privacy and data protection teams are rarely or never involved in determining if certain cloud applications or platforms meet data protection and privacy requirements.

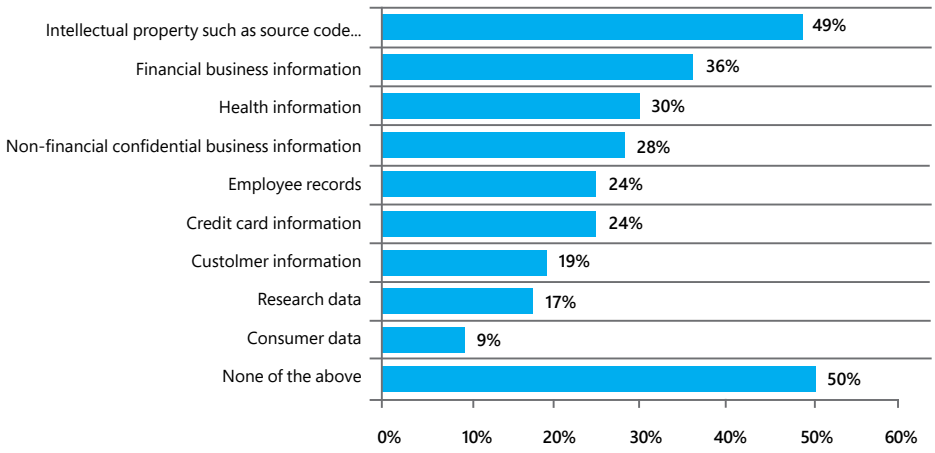
Figure 10. Are members of your privacy and data protection teams involved in determining the acceptability of certain cloud applications or platforms?



Intellectual property is considered the riskiest data to store in the cloud.

Consistent with the other findings in this research, organizations are not letting privacy and security concerns affect migration to the cloud. As shown in Figure 11, half of the respondents (50 percent) do not seem to be concerned about the risk of storing sensitive information in the cloud, and only 19 percent say customer information is too risky to store in the cloud. However, almost half of respondents (49 percent) did say IP is too vulnerable to be stored in the cloud.

Figure 11. What types of confidential or sensitive information does your organization consider too risky to be housed in the cloud?

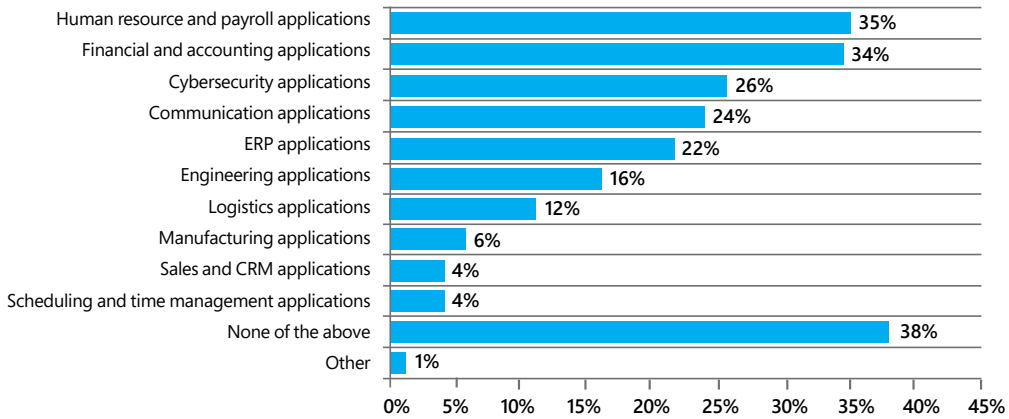


More than one response permitted

Human resource and payroll applications are considered the riskiest applications to process and store in the cloud.

Although 41 percent of respondents say human resource and payroll applications are too risky to be processed and stored in the cloud, more than a third of the respondents (38 percent) do not believe it would be too risky to put any business applications in the cloud.

Figure 12. What types of business applications does your organization consider too risky to be processed and housed in the cloud?



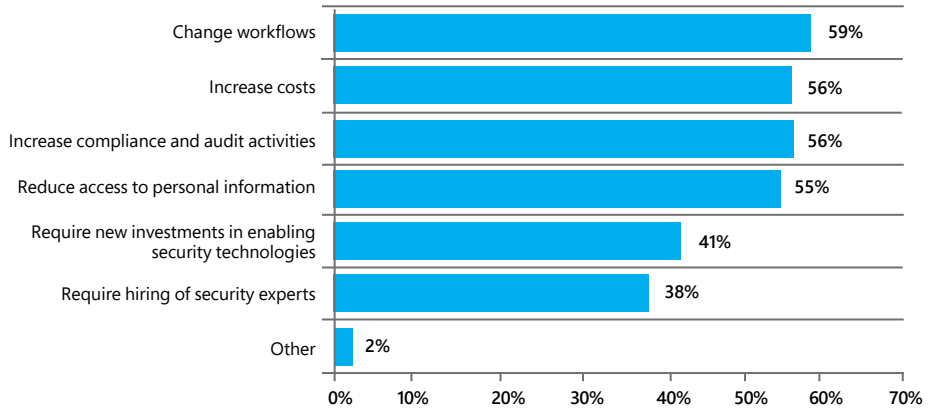
More than one response permitted

Compliance with the GDPR is a burden for many organizations.

Survey participants were asked how confident they were that their organization complies with the GDPR: 52 percent stated that they are not confident their organizations have achieved GDPR compliance.

Figure 13 shows some of the reasons for this lack of confidence. The majority of respondents (59 percent) say the new regulation has required them to change workflows. Other consequences include increases both in costs and in compliance and audit activities (56 percent respectively). They also stated that the GDPR also reduces access to personal information (55 percent of respondents).

Figure 13. How does the GDPR affect your organization's privacy and data protection activities?



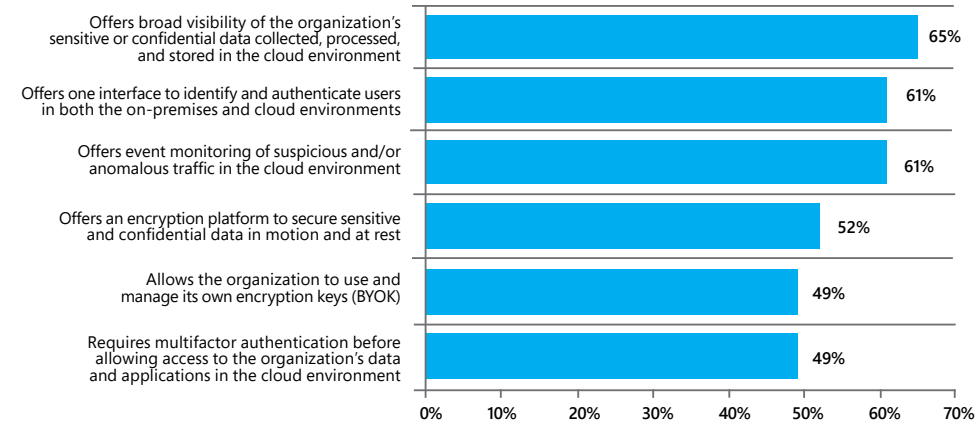
More than one response permitted

3. Organizations are using a variety of tools to protect sensitive data in the cloud

Visibility, a streamlined process for authenticating users, and event monitoring are considered the most important features for protecting sensitive data in the cloud.

A challenge to protecting data is the lack of visibility into how confidential data is collected, processed, and stored in the cloud environment. Figure 14 shows that 65 percent of respondents say broad visibility is an essential or very important feature. Sixty-one percent say that implementing a single interface to identify and authenticate users in both on-premises and cloud environments, and event monitoring of suspicious or anomalous traffic in the cloud environment are also essential and very important.

Figure 14. Cloud provider features and capabilities considered essential and very important



Essential *and* **Very important** *responses combined*

Most privacy-related activities are easier to deploy in the cloud than on premises.

Respondents were asked to rate the ease in meeting regulatory privacy requirements in the cloud and on premises on a scale from 1 = easier to deploy in the cloud to 10 = harder to deploy in the cloud. Table 1 presents a comparison of the differences in deploying privacy-related activities in the cloud and on premises. As shown, it is easier to conduct a privacy impact assessment, classify, or tag personal data for sensitivity or confidentiality, and meet legal obligations such as the GDPR in the cloud. Managing incident response is considered easier to deploy on premises than in the cloud.

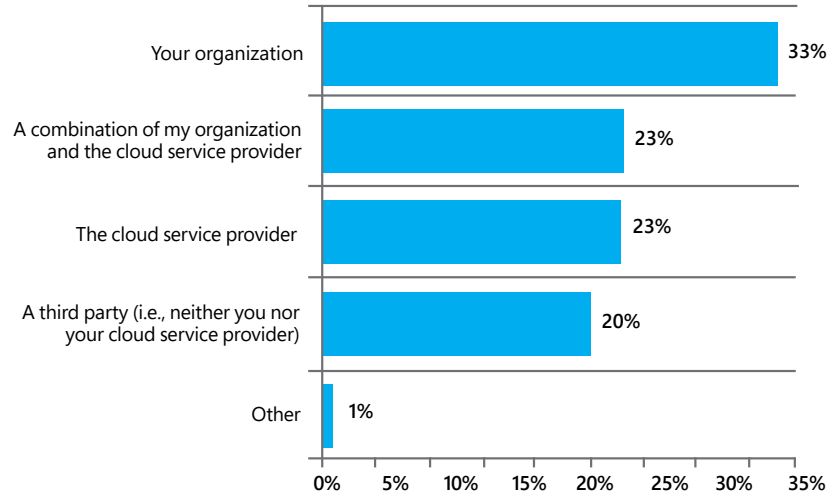
Table 1. The Ease in deploying privacy-related activities

	Consolidated US and EU responses	
Please rate the following privacy-related activities based on the relative difficulty to deploy within your organization.	Easier to deploy in the cloud	Easier to deploy on premises
Obtaining required compliance certifications	34%	29%
Implementing a data management regime	36%	40%
Meeting legal obligations, such as the GDPR	52%	44%
Issuing breach reach notifications	41%	40%
Managing incident response	32%	37%
Creating supporting privacy documentation	43%	39%
Retrievability of data to comply with regulations	46%	40%
Conducting audits	29%	30%
Obtaining consent	39%	36%
Executing data subject request or customer request for provision, change or deletion of personal data	41%	39%
Securing data	42%	40%
Conducting a privacy impact assessment	51%	39%
Responding to a privacy inquiry from a regulator	43%	44%
Ensuring appropriate residency of data	43%	41%
Classifying or tagging personal data for sensitivity or confidentiality	45%	36%
Restricting employee access to sensitive data	37%	34%

A 10-point scale from 1 = easier to deploy in the cloud than the on-premises to 10 = harder to deploy in the cloud than on premises

As Figure 15 shows, 33 percent of respondents say their organizations control encryption keys when data is encrypted in the cloud and another 23 percent of respondents say it is a combination of the organization and cloud service provider. Only 23 percent of respondents say the cloud service provider controls the encryption keys.

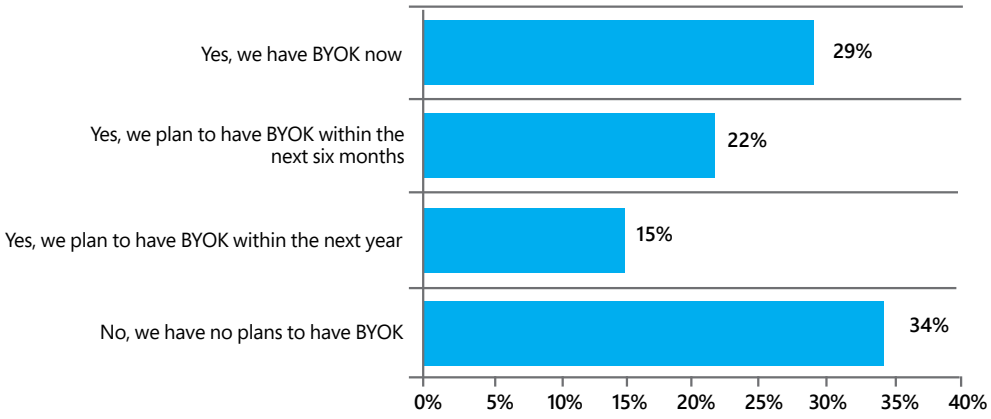
Figure 15. Who is in control of encryption keys when data is encrypted in the cloud?



Most organizations have adopted or will adopt Bring Your Own Key (BYOK).

Sixty-six percent of respondents either have adopted BYOK or plan to adopt it in the next six months or within the next year.

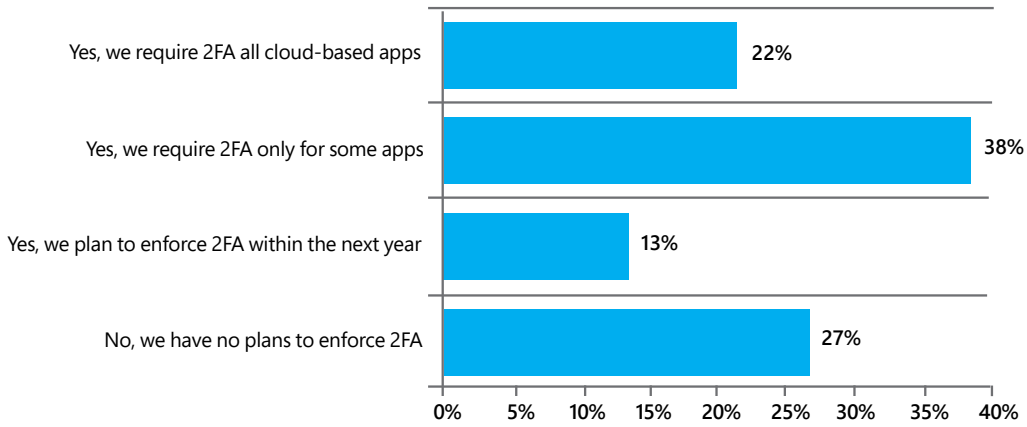
Figure 16. Has your organization adopted BYOK?



Most organizations have deployed two-factor authentication (2FA) for all or some cloud-based applications.

As shown in Figure 17, 73 percent of respondents say their organizations have deployed 2FA for all or some cloud-based apps or they plan to do so within the next year.

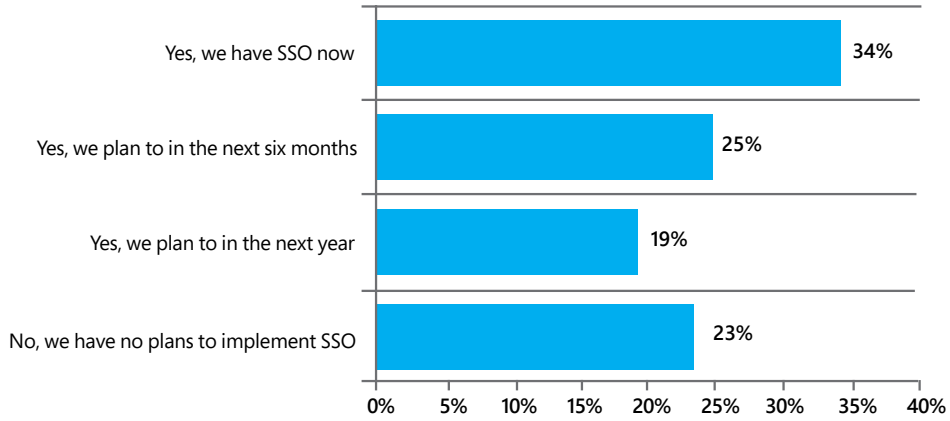
Figure 17. Has your organization deployed two-factor authentication to secure apps and data?



Most organizations use or plan to use single sign-on (SSO).

Seventy-eight percent either use SSO or plan to implement it within the next six months or year.

Figure 18. Has your organization implemented single sign-on (SSO) across your application infrastructure?



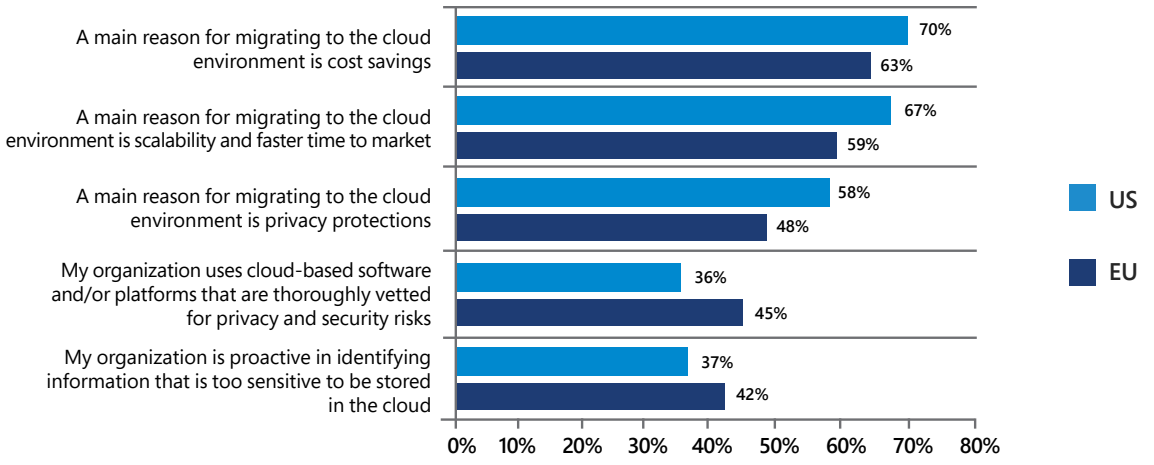
4. Comparing US and EU respondents' perceptions of data protection and compliance in the cloud

More EU respondents say their organizations are proactive in protecting sensitive information in the cloud environment.

As shown in Figure 19, 42 percent of EU respondents compared to 37 percent of those in the US say their organizations are proactive in identifying information that is too sensitive to be stored in the cloud. The gap is even more significant (45 percent of EU respondents compared with 36 percent from the US) in the use of cloud-based software or platforms that are thoroughly evaluated for privacy and data security risks.

Figure 19 also shows that US respondents are more likely than those in the EU to say they are migrating to the cloud to reduce costs (70 percent compared with 63 percent) and achieve scalability and faster time to market (67 percent compared with 59 percent). It is interesting that more US respondents also say their organization migrated to the cloud to improve security and privacy protections.

Figure 19. Perceptions about privacy and data protection in the cloud



Strongly agree *and* **Agree** *responses combined*

US and EU respondents concur that it is easier to conduct a privacy impact assessment in the cloud than on premises.

Respondents were asked to rate the ease in deploying privacy-related activities in the cloud and on premises on a scale from 1 to 10. Table 2 presents the activities and the differences in the ease of conducting a privacy impact assessment between the cloud and on premises in the US and EU.

As shown in Table 2, both US and EU respondents agree that conducting a privacy assessment, meeting legal obligations such as the GDPR, and classifying or tagging personal data for sensitivity or confidentiality is easier in the cloud. US respondents are more likely to believe executing data subject or customer requests to provide, change, or delete personal data, securing data, and responding to a privacy inquiry from a regulator is easier in the cloud. EU respondents believe it is easier in the cloud to obtain required compliance certifications and ensure appropriate residency of data.

Table 2. Comparing the US and the EU in the ease of addressing privacy-related requirements

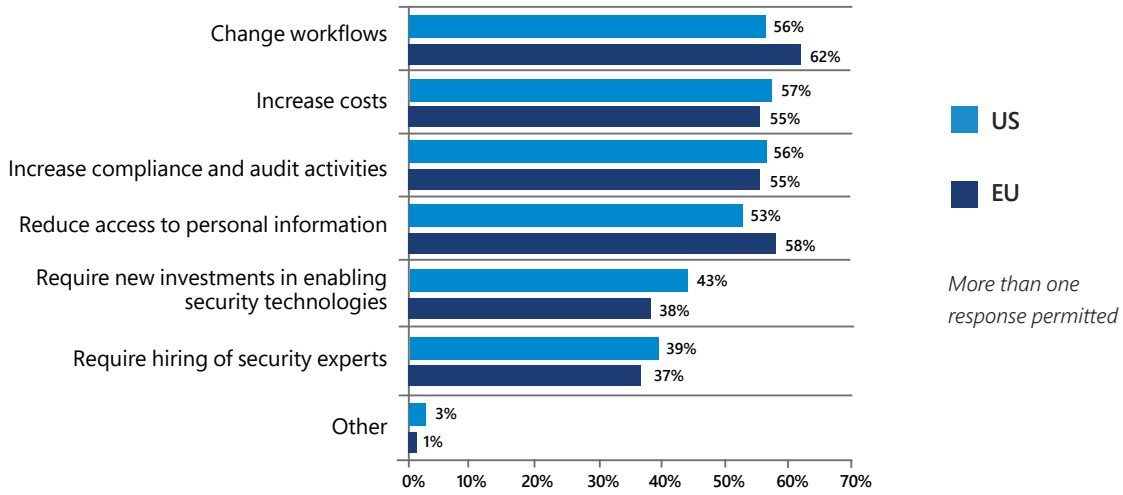
	United States		European Union	
Please rate the following privacy-related activities based on the relative difficulty to deploy within your organization.	Easier to deploy in the cloud	Easier to deploy on premises	Easier to deploy in the cloud	Easier to deploy on premises
Obtaining required compliance certifications	33%	30%	36%	28%
Implementing a data management regime	39%	41%	33%	40%
Meeting legal obligations, such as the GDPR	47%	39%	56%	48%
Issuing breach reach notifications	43%	39%	39%	40%
Managing incident response	31%	35%	32%	38%
Creating supporting privacy documentation	45%	41%	41%	36%
Retrievability of data to comply with regulations	45%	40%	48%	40%
Conducting audits	27%	34%	30%	26%
Obtaining consent	40%	37%	37%	35%
Executing data subject request or customer request for provision, change or deletion of personal data	41%	38%	41%	39%
Securing data	48%	41%	36%	39%
Conducting a privacy impact assessment	50%	37%	52%	40%
Responding to a privacy inquiry from a regulator	46%	39%	40%	49%
Ensuring appropriate residency of data	38%	41%	49%	41%
Classifying or tagging personal data for sensitivity or confidentiality	48%	36%	43%	37%
Restricting employee access to sensitive data	34%	32%	39%	35%

A 10-point scale from 1 = easier to deploy in the cloud than the on-premises to 10 = harder to deploy in the cloud than on premises

Both EU and US organizations find it challenging to meet GDPR requirements.

Fifty-four percent of US respondents and 49 percent of EU respondents are not confident that their organizations have achieved compliance with the GDPR. Furthermore, 59 percent of US respondents and 63 percent of EU respondents say the GDPR required them to significantly change or make some change to the way their organizations collect, use, and protect sensitive or confidential data in the cloud. Figure 20 shows some of the specifics of these organizational changes the GDPR has required, including change in workflows, increased cost, and increased compliance and audit activities.

Figure 20. How does the GDPR affect your organization's privacy and data protection activities?



Recommendations: Ten steps to improving protection and compliance in the cloud

Most organizations are migrating to the cloud to reduce costs and achieve scalability and faster time to market. Respondents also predict that in the next two years their use of SaaS and PaaS will significantly increase to meet privacy and data protection objectives.

However, respondents' confidence in the ability of their organizations to protect data and achieve compliance with privacy regulations in the cloud is low. The following are recommended steps that organizations can take to address these concerns.

1. Improve visibility into the organization's sensitive or confidential data collected, processed, or stored in the cloud environment.
2. Educate themselves about all the cloud applications and platforms already in use in the organization.
3. Simplify the authentication of users in both on-premises and cloud environments.
4. Ensure the cloud provider offers event monitoring of suspicious and anomalous traffic in the cloud environment.
5. Implement the capability to encrypt sensitive and confidential data in motion and at rest.
6. Make sure that the organization uses and manages its own encryption keys (BYOK).
7. Implement multifactor authentication before allowing access to the organization's data and applications in the cloud environment.
8. Assign responsibility for ensuring compliance with privacy and data protection regulations and security safeguards in the cloud to those most knowledgeable: the compliance and IT security teams. Privacy and data protection teams should also be involved in evaluating any cloud applications or platforms under consideration.
9. Identify information that is too sensitive to be stored in the cloud and assess the impact that cloud services may have on the ability to protect and secure confidential or sensitive information.
10. Thoroughly evaluate cloud-based software and platforms for privacy and security risks.

Study methodology and limitations

Ponemon fielded this research in the United States and the European Union, completing it in September 2019. The combined sampling frame includes 30,152 IT or IT security practitioners. All respondents were familiar with their organization's approach to privacy and data protection compliance and responsible for ensuring that personal data is protected in the cloud environment. The total number of completed survey returns is 1,154, of which 105 were rejected because of failed reliability. This resulted in a final sample size of 1,049 qualified respondents—or a 3.5 percent response rate.

Table 3. Survey responses

	US	EU	Consolidated
Total sampling frame	16,487	13,665	30,152
Total returns	659	495	1,154
Rejected surveys	57	48	105
Final sample	602	447	1,049
Response rate	3.7%	3.3%	3.5%

Figure 22. Position of respondents

The following pie chart summarizes the positions of the qualified respondents. At 36 percent, the largest segment contains those who are rank-and-file employees (i.e., staff or technicians). All the rest— employees who are at or above the supervisory level—comprise 64 percent.

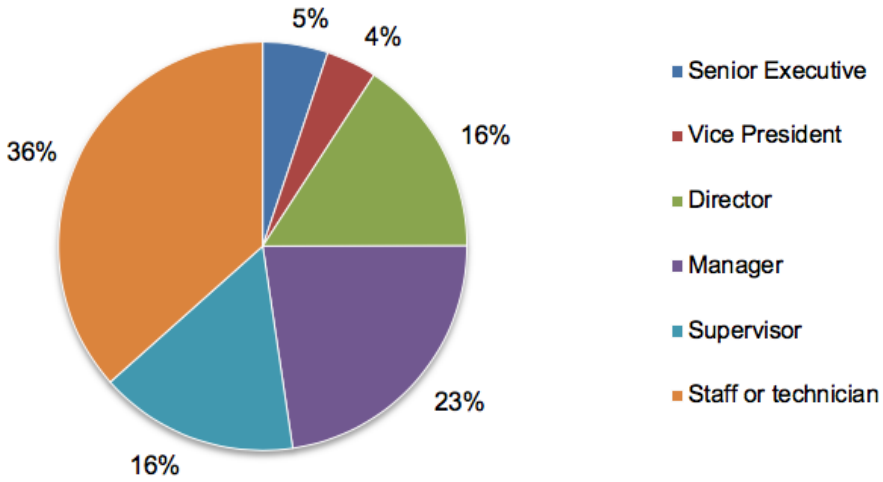


Figure 23. Primary person you or your IT security leader reports to within the organization

Figure 23 shows the respondents' direct reporting channels. Thirty-four percent of respondents report to the chief information officer, 17 percent report to the chief information security officer, and 7 percent of respondents each report to the compliance officer and chief security officer, respectively.

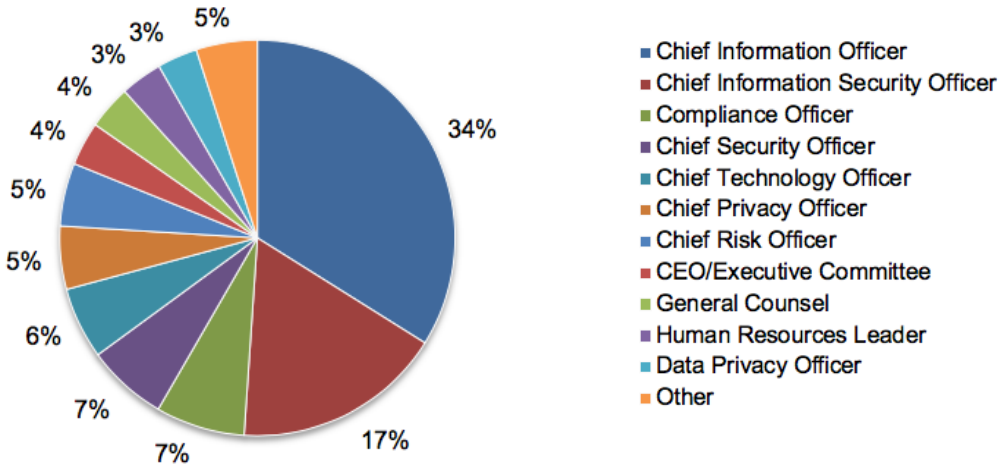


Figure 24. Primary industry sector of respondents' companies

Figure 24 shows the percentage distribution of respondents' companies among 15 industries. As can be seen, financial services represent the largest industry sector at 17 percent, and include banking, insurance, brokerage, investment management, and payment processing companies.

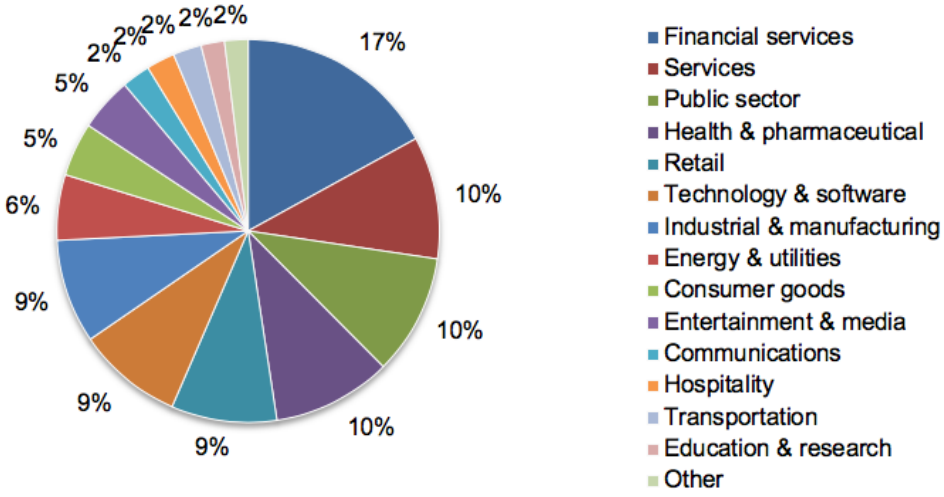


Figure 25. Global headcount of respondents' companies

Figure 25 summarizes the total worldwide headcount of respondents' companies. Half of the respondents (50 percent) are from organizations with a worldwide headcount of 5,000 or more employees.

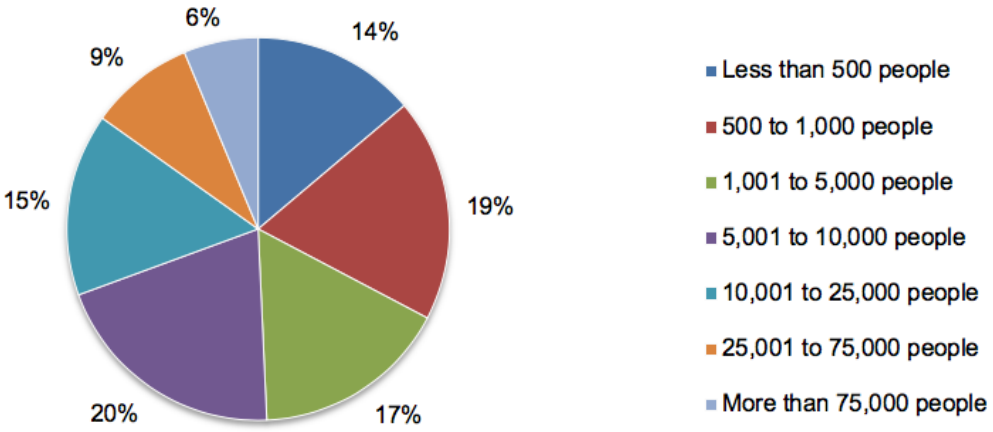
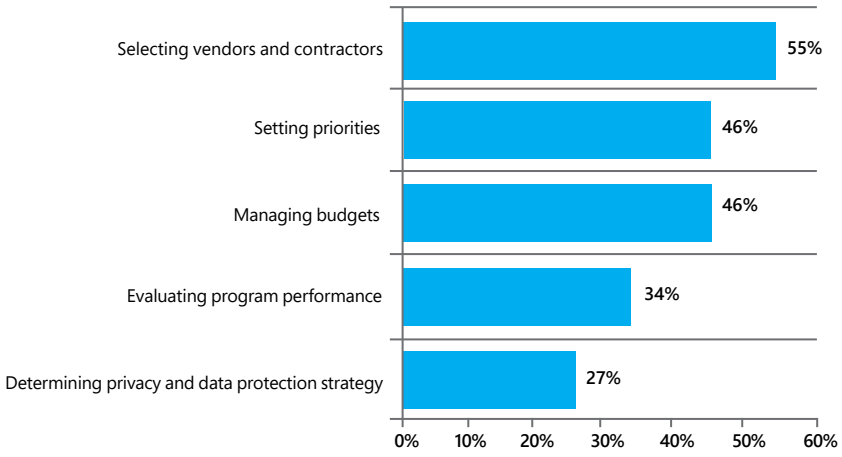


Figure 26. Respondents' role in managing data protection and security risk in your organization

As shown in Figure 26, more than half (55 percent) of respondents identified their role as selecting vendors and contractors. Forty-six percent of respondents define their role as setting priorities or managing budgets.



Study limitations

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following specific limitations 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 respond and participate are substantially different in terms of underlying beliefs from those who completed the survey.
- **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 located in the United States and the European Union. 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.

For more information about this study, please contact Ponemon Institute by sending an email to **research@ponemon.org** or calling us at **1.800.887.3118**.

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.

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.


Microsoft


Ponemon
INSTITUTE