Ponemon INSTITUTE



The Cost of Cloud Compromise and Shadow IT

Sponsored by Proofpoint

Independently conducted by Ponemon Institute LLC

Publication Date: April 2021

The Cost of Cloud Compromise and Shadow IT
April 2021

Part 1. Introduction

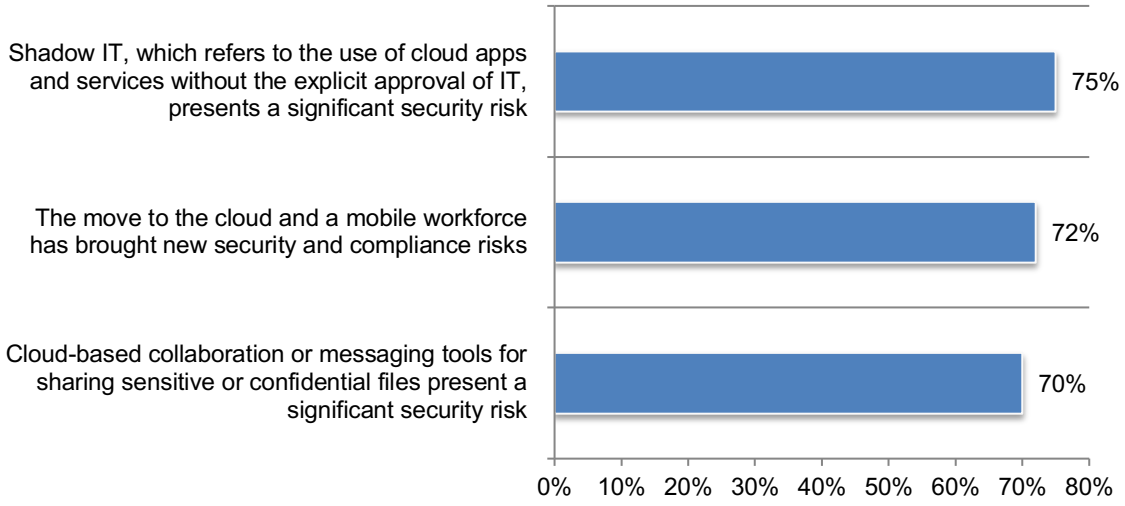
The purpose of this research is to learn important information about how organizations secure and protect confidential data and identities in the cloud environment. Sponsored by Proofpoint, Ponemon Institute surveyed 662 IT and IT security professionals in the US.

According to the research, security risks occur because only 44 percent of respondents say their organizations have established clearly defined roles and accountability for safeguarding of confidential or sensitive information in the cloud. One consequence is that only 39 percent of respondents say their organizations are vigilant in conducting assessments of cloud apps before deployment.

Compromised cloud accounts are costly incidents. The research revealed that the average yearly financial loss due to compromised cloud accounts per year for the organizations represented in this research is $6.2 million and in the past 12 months represented an average of 3.5 percent of their total revenues. In a year, organizations experienced an average of 138 hours of application downtime.

Shadow IT is a significant security risk for organizations. As shown in Figure 1, 75 percent of respondents say the use of cloud apps and services without the approval of IT is a serious security risk. Other practices that create risks to organizations are cloud-based collaboration or messaging tools for the sharing of sensitive or confidential files (70 percent of respondents) and the move to the cloud and mobile workforce (72 percent of respondents).

Figure 1. Perceptions about the risk of shadow IT and security in the cloud
Strongly agree and Agree responses combined



Part 2. Key findings

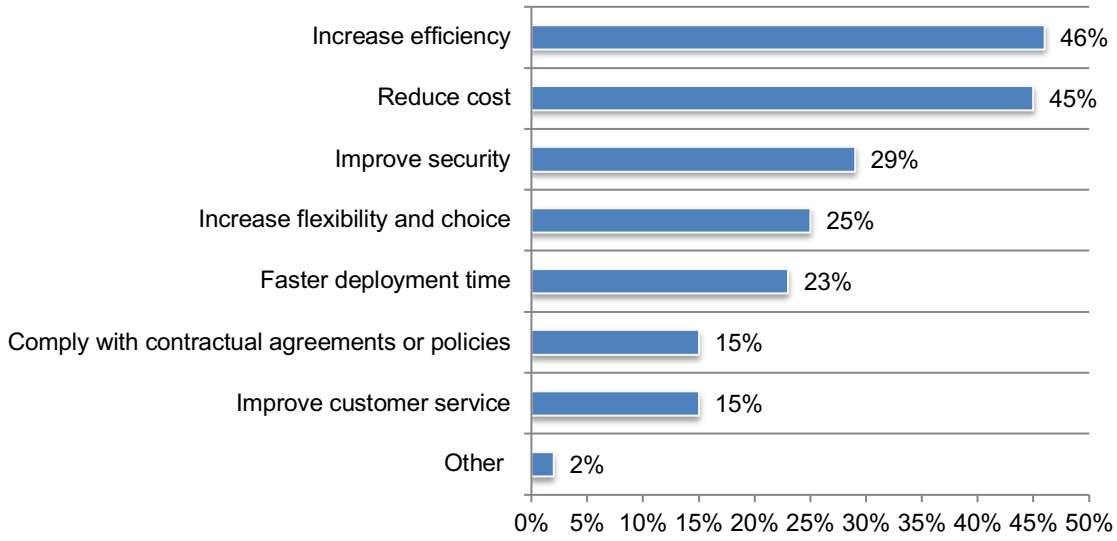
In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The following topics are covered in this report.

- The state of cloud usage in organizations
- Security risks and practices to secure the cloud
- Cloud compromises and the end user risk
- The cost of compromised cloud accounts

The state of cloud usage in organizations

Increased efficiency and reduced costs are the reasons cloud services are used within their organization. According to Figure 2, 46 percent of respondents say an increase in efficiency and 45 percent of respondents say it is to reduce costs. Only 29 percent of respondents say the primary reason for cloud services is an improvement in the security posture of their organizations.

Figure 2. What are the primary reasons cloud resources are used within your organization?
Two responses permitted

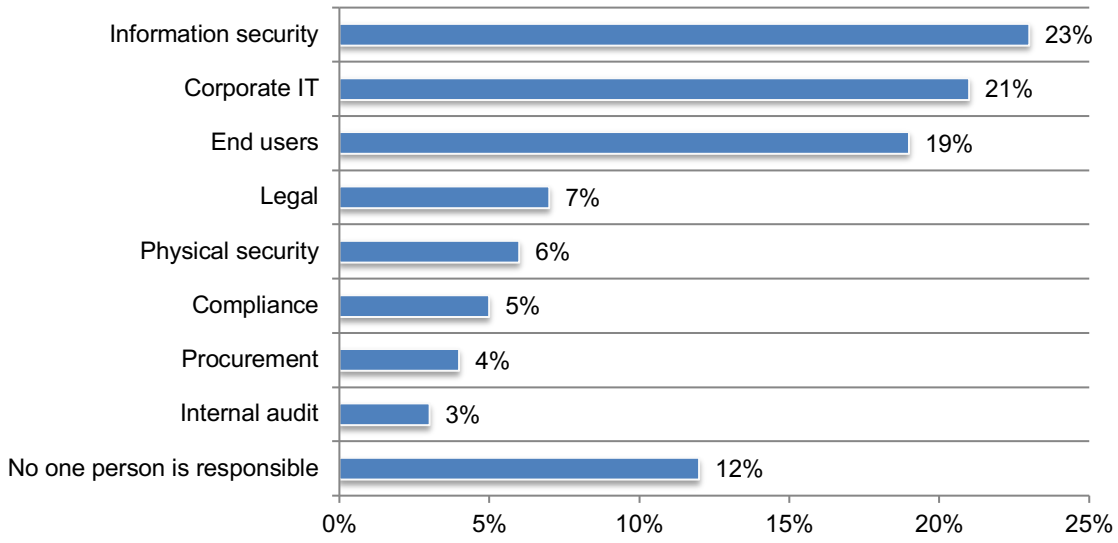


Multicloud is the use of multiple cloud computing and storage services in a single heterogeneous architecture. This also refers to the distribution of cloud assets, software, applications, etc. across several cloud-hosting environments. With a typical multicloud architecture utilizing two or more public clouds as well as multiple private clouds, a multicloud environment aims to eliminate the reliance on any single cloud provider. It differs from hybrid cloud in that it refers to multiple cloud services rather than multiple deployment modes (public, private, legacy).

Most organizations are deploying a multicloud strategy currently or in the near future. Sixty-eight percent of respondents say their organizations have a multicloud architecture or strategy and on average these organizations have about 4 different clouds. Of the 32 percent of respondents who say they currently don't have such a strategy, 52 percent of respondents say they will have it in six months and 26 percent say they will have it within the next 12 months. Only 22 percent of these respondents say they will not have such a strategy.

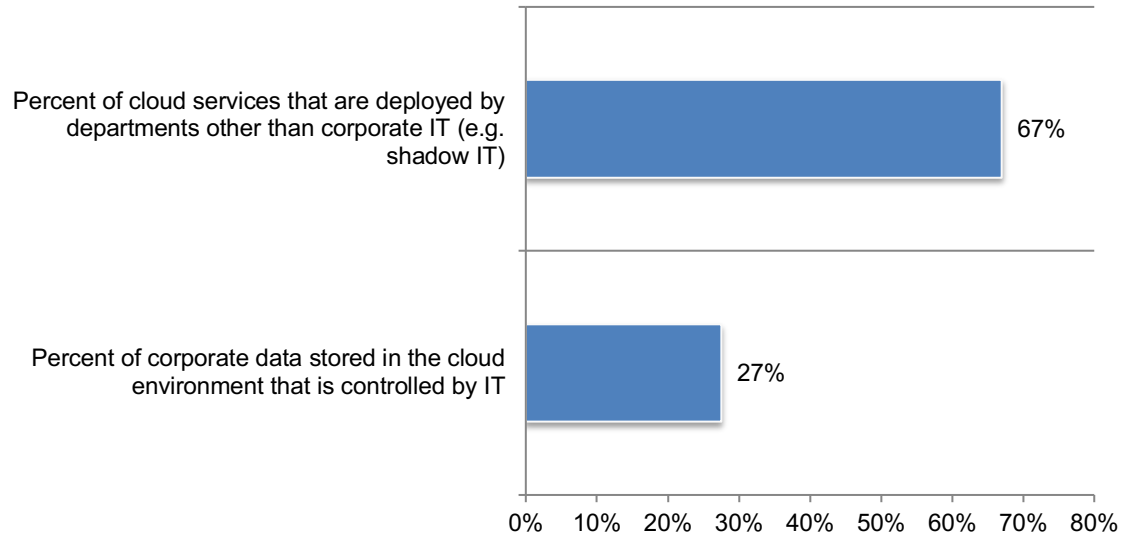
Responsibility for evaluating the cloud provider's security capabilities is dispersed throughout the organization. As shown in Figure 3, not one function is clearly accountable for evaluating the cloud provider's security capabilities. Information security (23 percent of respondents) and corporate IT (21 percent of respondents) are most responsible.

Figure 3. Who in your organization is most responsible for evaluating the cloud provider's security capabilities?



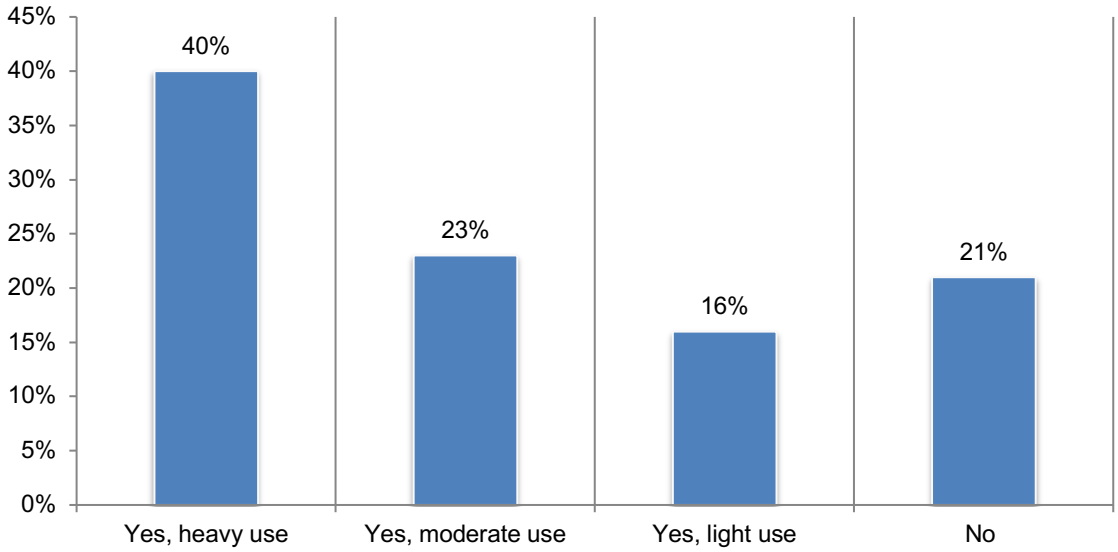
Very little corporate data in the cloud is controlled by IT. An average of 42 percent of corporate data is stored in the cloud. However, only an average of 27 percent of corporate data stored in the cloud environment is controlled by IT, as shown in Figure 4. Sixty-seven percent of cloud services are deployed by departments other than corporate IT (Shadow IT).

Figure 4. The average percent of corporate data stored in the cloud environment controlled by IT and the average percent of cloud services deployed by departments other than corporate IT (e.g. shadow IT)
Extrapolated values presented



The importance of SaaS grows. As shown in Figure 5**,** 79 percent of respondents say their organizations are heavy users (40 percent), moderate users (23 percent) or light users (16 percent) of SaaS. An average of 36 percent of an organization's business-critical applications use SaaS versus on-premises software applications.

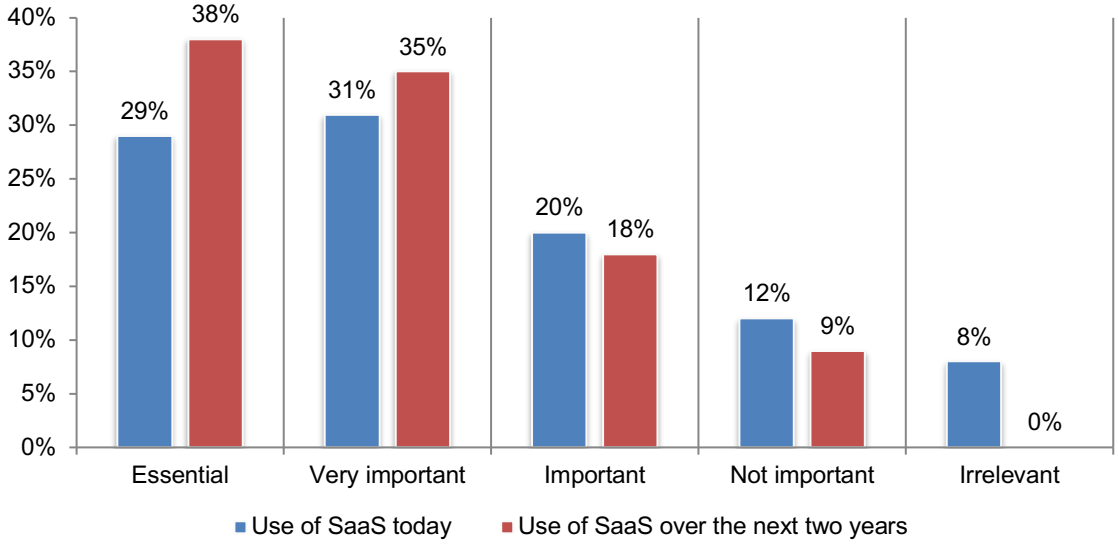
Figure 5. Does your organization use SaaS resources from cloud service providers?



Security risks in the cloud

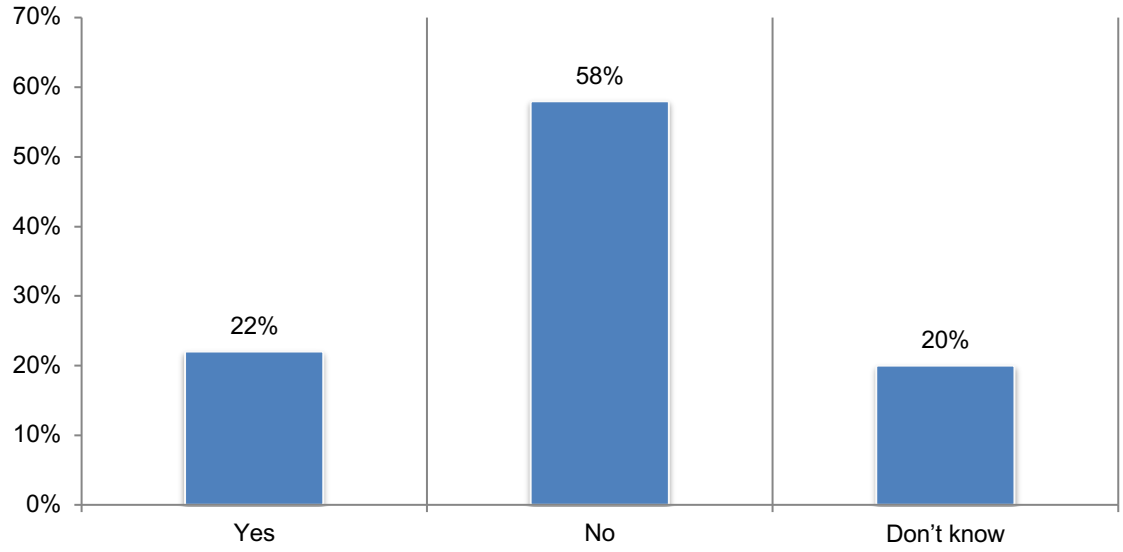
The increased use of SaaS makes it critical to evaluate the security of SaaS applications. According to Figure 6, 80 percent of respondents say the use of SaaS in meeting IT data processing objectives is essential (29 percent), very important (31 percent) and important (20 percent). Over the next two years, 91 percent of respondents say SaaS will be essential (38 percent), very important (35 percent) and important (18 percent).

Figure 6. The importance of SaaS in meeting your organization's IT and data processing objectives today and in two years



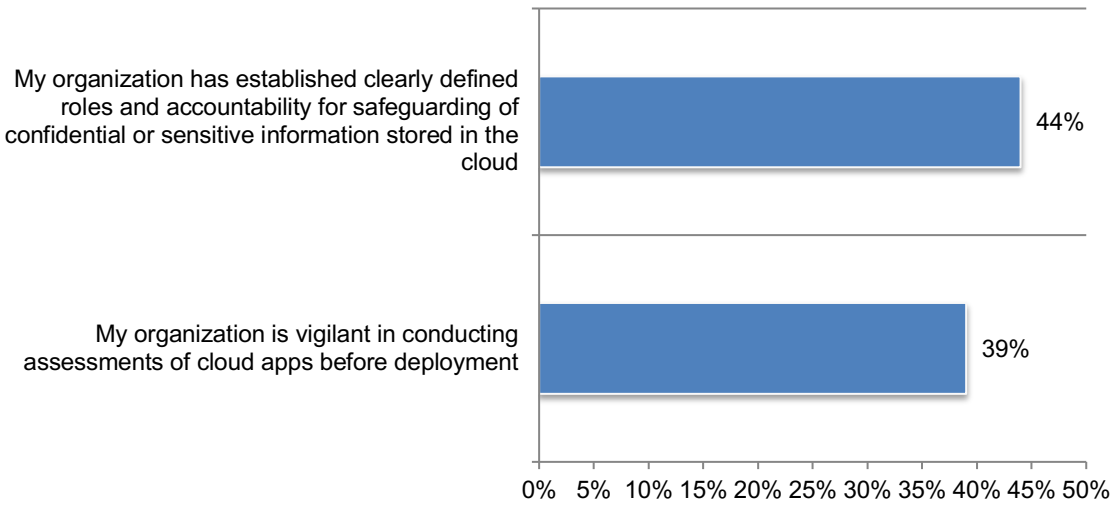
However, few organizations are evaluating the security of SaaS applications prior to deployment. According to Figure 7, 78 respondents say their organizations do not (58 percent) or don't know (20 percent) if SaaS applications are evaluated for security prior to deployment within their organization.

Figure 7. Are SaaS applications evaluated for security prior to deployment within your organization?



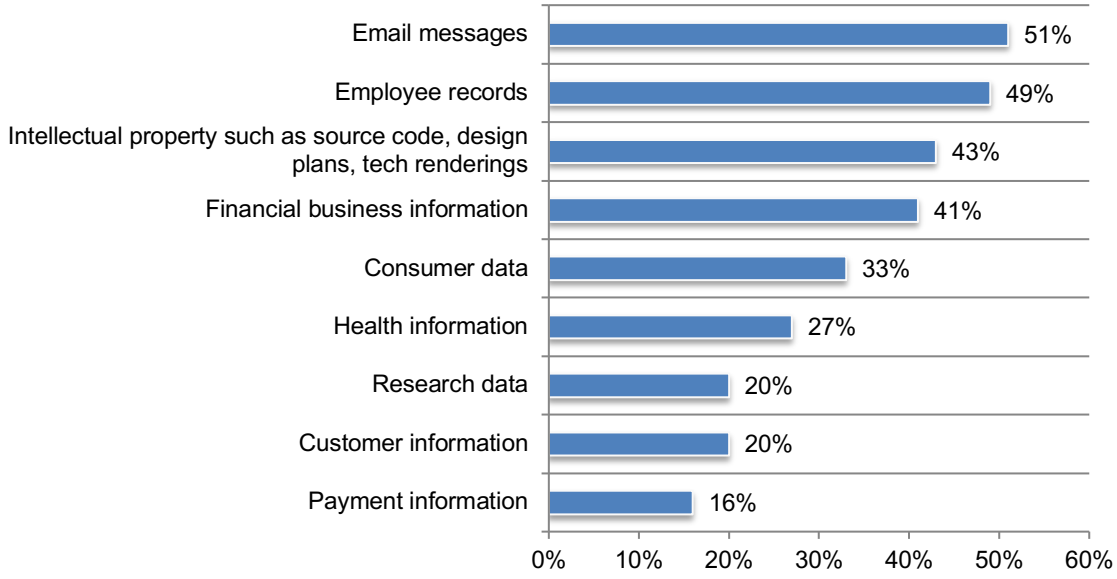
Perceptions about security risks in the cloud. As shown in Figure 8, only 44 percent of respondents say their organizations have established clearly defined roles and accountability for safeguarding of confidential or sensitive information stored in the cloud. One consequence is that only 39 percent of respondents say their organizations are vigilant in conducting assessments of cloud apps before deployment.

Figure 8. Security risks in the cloud
Strongly agree and Agree responses combined



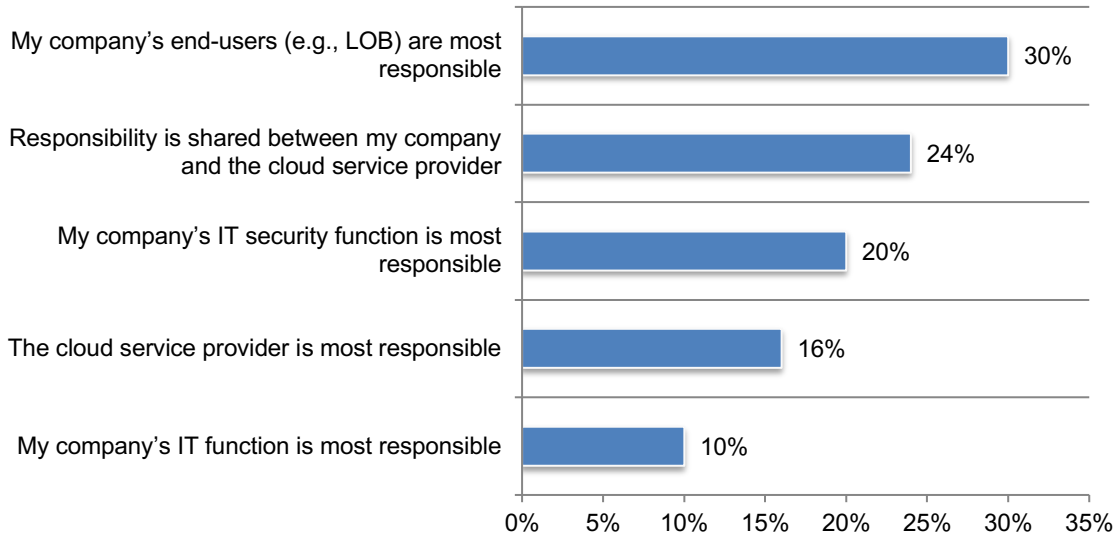
According to Figure 9, e-mail messages, employee records and intellectual property such as source code, design plans and tech renderings are the types of corporate data that are at greatest risk when stored in the cloud, according to 51 percent, 49 percent and 43 percent of respondents respectively.

Figure 9. What type of corporate data presents the greatest security risk to your organization when stored in the cloud?
Three responses permitted



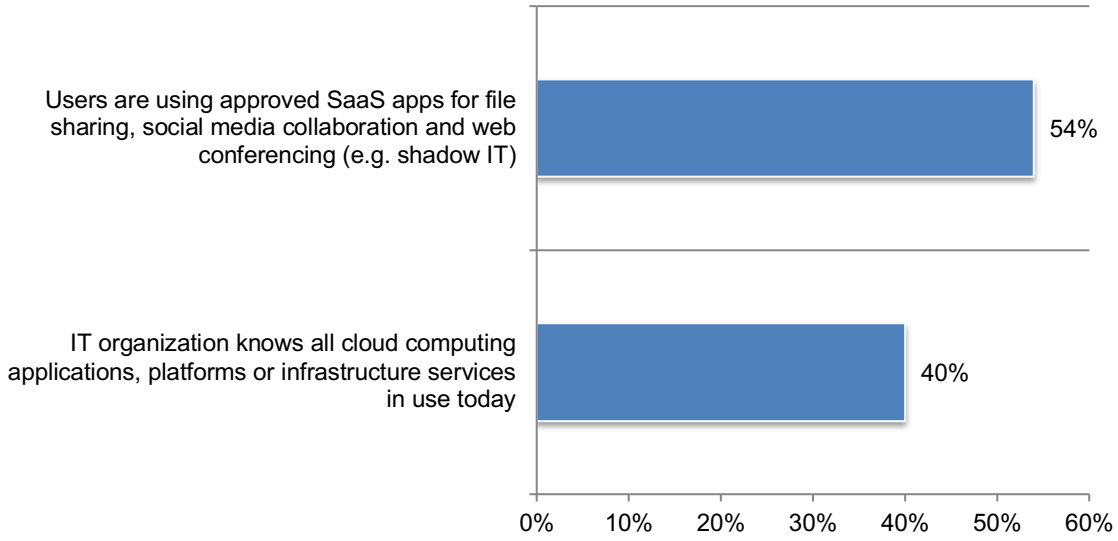
There is no centralized accountability for the security of SaaS applications. As shown in Figure 10, end-users are most responsible for the security of SaaS applications used within their organization (30 percent of respondents). Twenty-four percent of respondents say responsibility is shared between the company and the cloud service provider. This is followed by the IT security function (20 percent of respondents), the cloud service provider (16 percent of respondents) or the IT function (10 percent of respondents).

Figure 10. Who is most responsible for ensuring the security of SaaS applications within your organization?



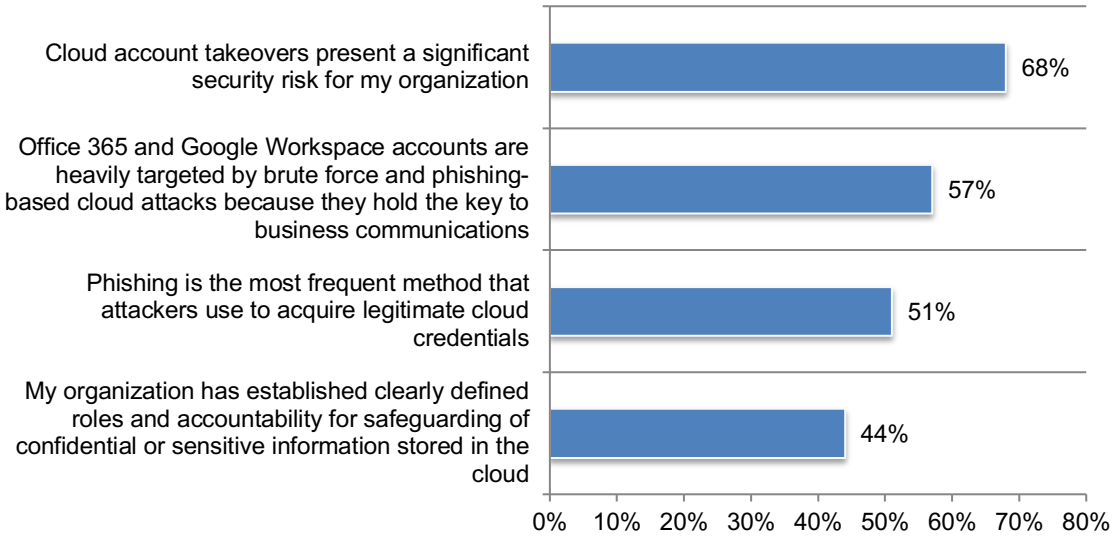
As shown in Figure 11, slightly more than half of respondents (54 percent) are very confident (24 percent) or confident (30 percent) that users are using approved SaaS apps for file sharing, social media collaboration and web conferencing (e.g. shadow IT). However, only 40 percent of respondents are very confident (19 percent) or confident (21 percent) that their organizations know all cloud computing applications, platforms or infrastructure services in use today.

Figure 11. Confidence in the use of approved SaaS apps and visibility into the cloud
Very confident and confident responses combined



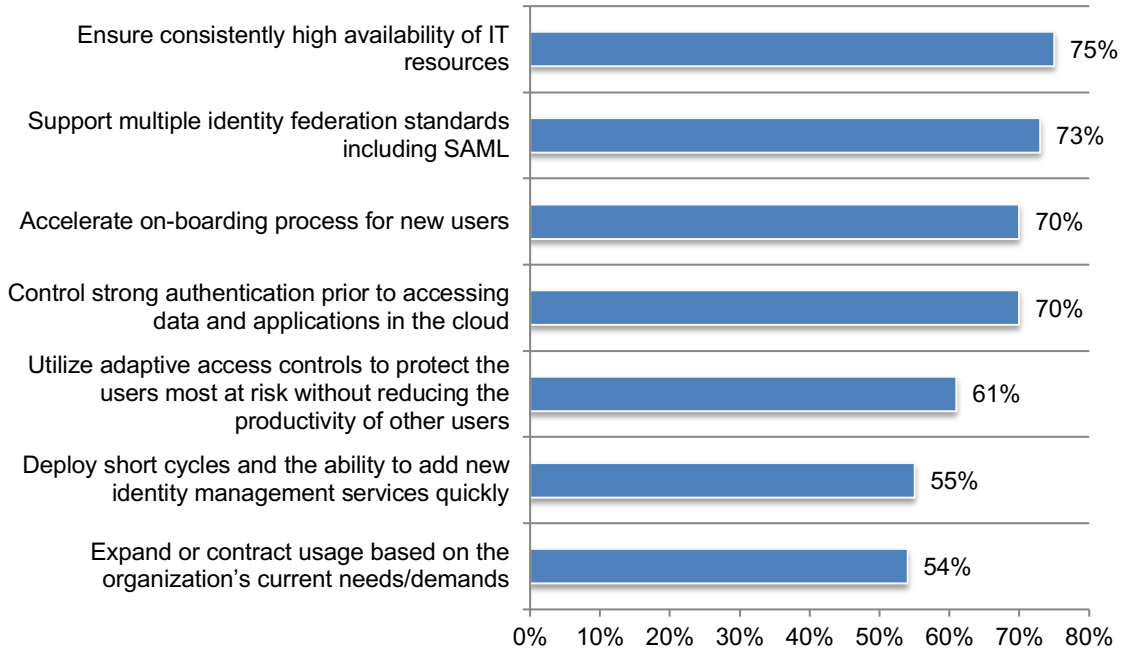
Cloud account takeovers are a significant security risk to organizations. According to Figure 12, 68 percent of respondents say cloud account takeovers present a significant security risk for their organizations. According to 57 percent of respondents, Microsoft Office 365 and Google Workspace accounts are heavily targeted by brute force and phishing-based cloud attacks. More than half (51 percent) of respondents say phishing is the most frequent method that attackers use to acquire legitimate cloud credentials.

Figure 12. More perceptions about security in the cloud



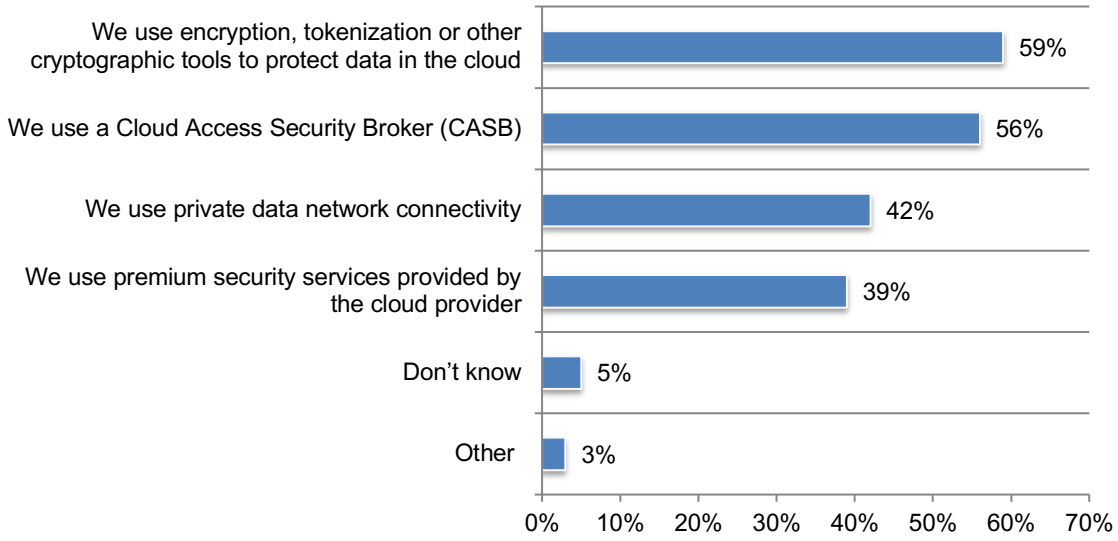
Certain features are essential in securing control and access to cloud resources. Figure 13 presents seven features important to control and secure access to cloud resources. The most important features for improving control and secure access to cloud resources are: ensuring consistently high availability of IT resources (75 percent of respondents) and supporting multiple identity federation standards including SAML (73 percent of respondents), controlling strong authentication prior to accessing data and applications in the cloud (70 percent of respondents), and accelerating on-boarding process for new users (70 percent of respondents).

Figure 13. How important are the following features to the ability to control and secure access to cloud resources?
Essential and Very important responses combined



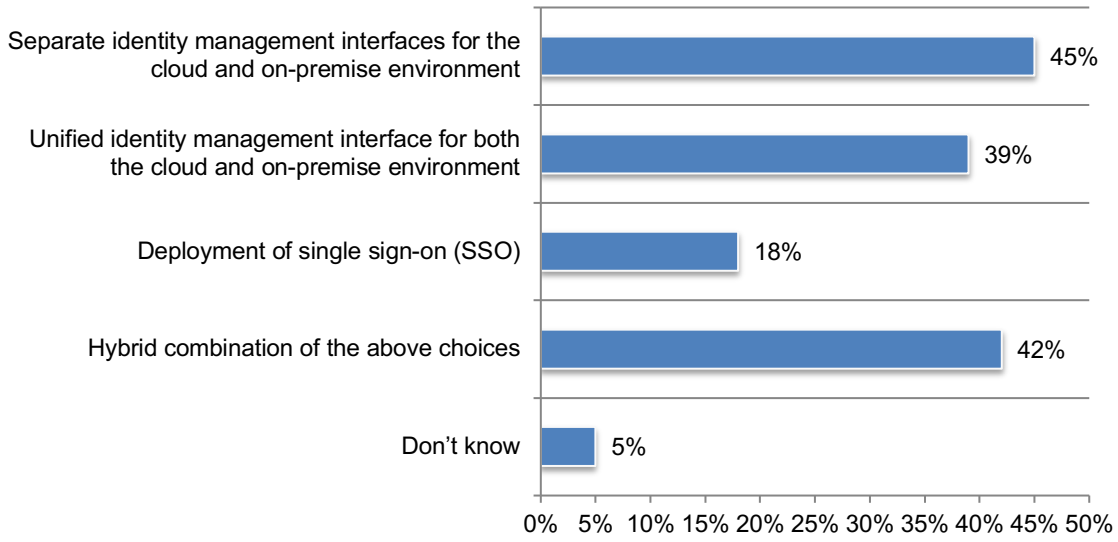
Encryption, tokenization or other cryptographic tools and CASBs are used to protect confidential or sensitive information in the cloud, as shown in Figure 14.

Figure 14. How does your organization protect confidential or sensitive information in the cloud?
More than one response permitted



According to Figure 15, organizations' primary approaches to user access and identity management in the cloud environment are separate identity management interfaces for the cloud and on-premise environment (45 percent of respondents) or, according to 42 percent of respondents, it is a combination of unified identity management interface for both the cloud and on-premise environment and deployment of single sign-on (SSO).

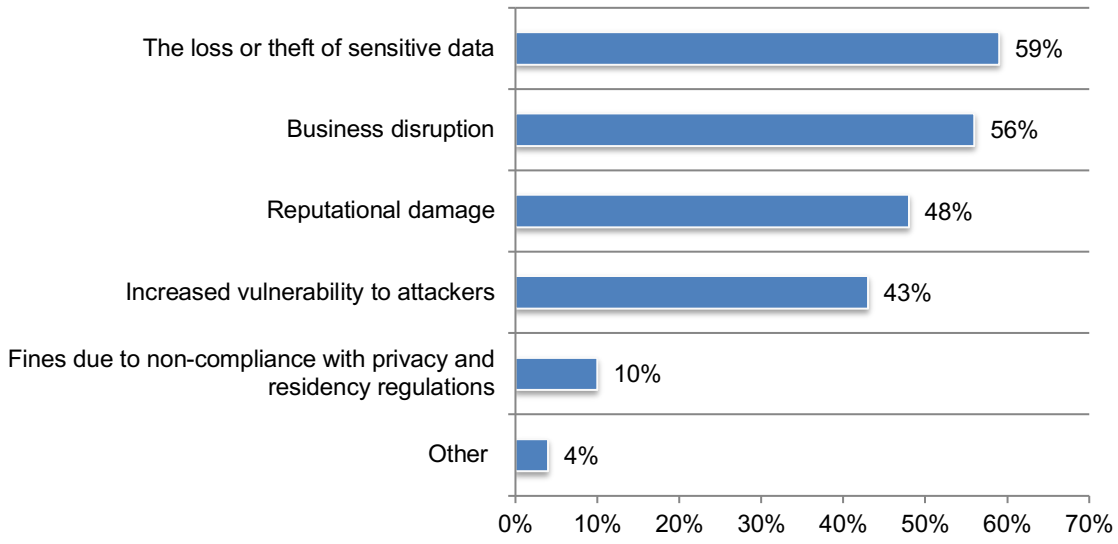
Figure 15. What best describes your organization's approach to user access and identity management in the cloud environment?



Compromises in the cloud and the end-user risk

Highly sensitive data is at risk in the cloud. Sixty-seven percent of respondents say their organizations experienced an account compromise that exposed sensitive data. According to Figure 16, the top three consequences are the loss or theft of sensitive data (59 percent of respondents), business disruption (56 percent of respondents) and reputational damage (48 percent of respondents). In the past 12 months, organizations represented in this research had an average of 19 cloud-based compromises.

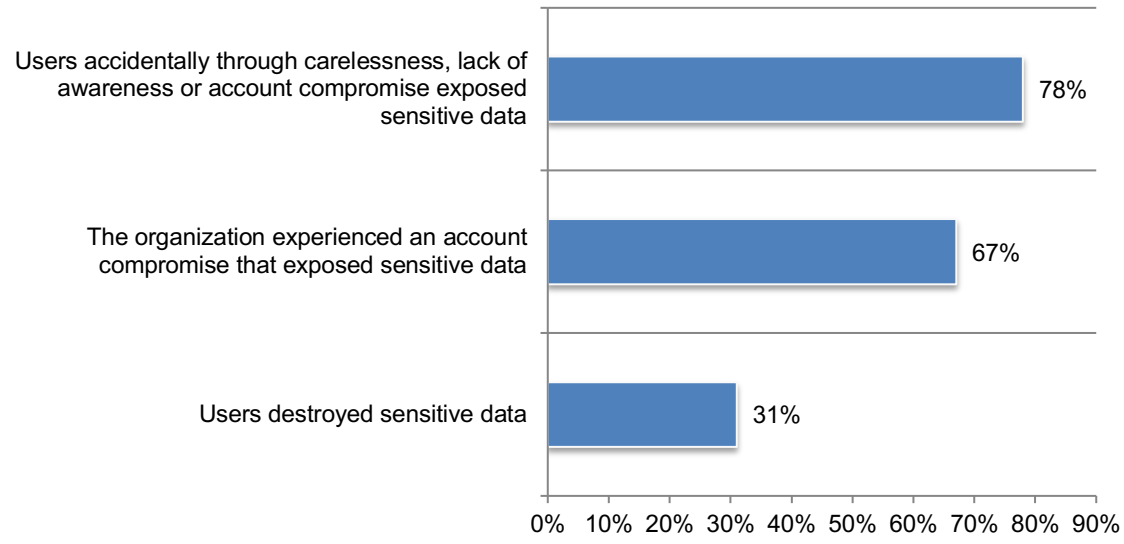
Figure 16. What were the consequences of an account compromise that exposed sensitive data?
More than one response permitted



The following are three examples of end-user compromises.

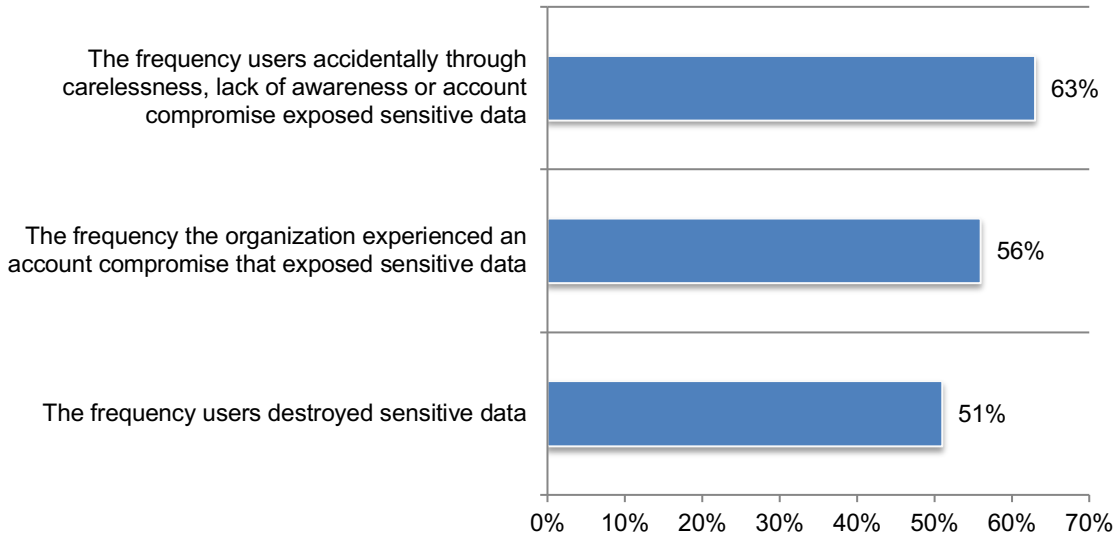
The risk to account compromises. Figure 17 presents three examples of how users have been the source of end-user compromises. Seventy-eight percent of respondents say users in their organizations accidentally through carelessness, lack of awareness or account compromise exposed sensitive data, 67 percent of respondents say the organization experienced an account compromise that exposed sensitive data and 31 percent of respondents say users destroyed sensitive data.

Figure 17. In the past 12 months have users destroyed sensitive data, through carelessness exposed sensitive data or experienced sensitive data?
Yes responses presented



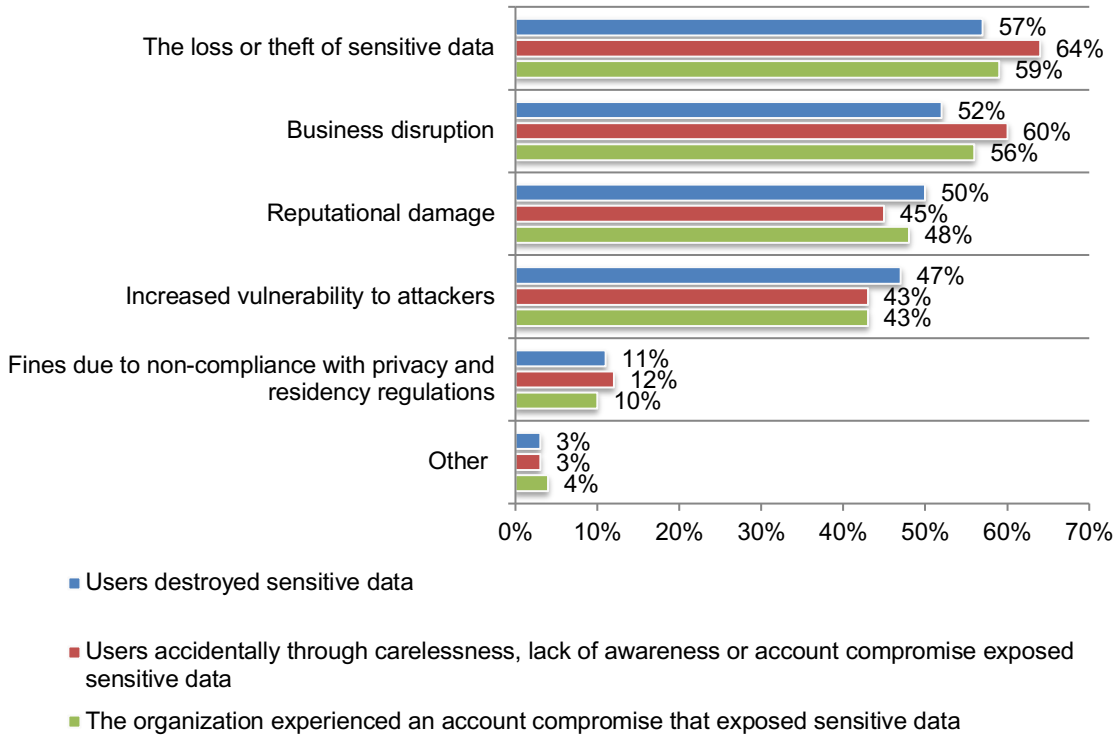
The most frequent end-user compromise is due to negligence. As shown in Figure 18, 63 percent of respondents say users accidentally through carelessness, lack of awareness or account compromise exposed sensitive data very frequently or frequently. Fifty-six percent of respondents say very frequently or frequently organizations experienced an account compromise that exposed sensitive data and 51 percent of respondents say it was very frequently or frequently that users destroyed sensitive data.

Figure 18. How frequently did it happen?
Very frequently and Frequently responses combined



End-user negligence is most responsible for the loss or theft of sensitive data and business disruption, as shown in Figure 19. Sixty-four percent of respondents say the loss o theft of sensitive data was due to carelessness, lack of awareness or account compromise exposed sensitive data followed by 59 percent of respondents who say their organization experienced an account comprise through the exposure of sensitive data. Sixty percent of respondents say negligence caused business disruption.

Figure 19. What were the consequences of the end-user compromise?
More than one response permitted



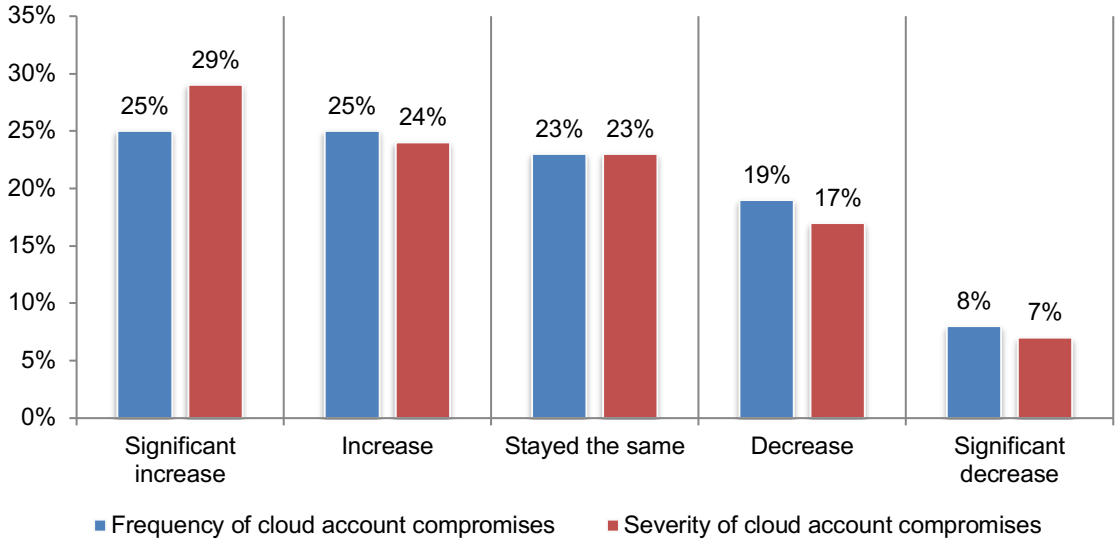
The cost of compromised cloud accounts

Compromised cloud accounts are costly incidents and should drive organizations to invest in technologies, in-house expertise and user training and awareness programs. According to the findings, the average yearly financial loss due to compromised cloud accounts per year for the organizations represented in this research is $6.2 million and in the past 12 months represented an average of 3.5 percent of their total revenues. In a year, organizations experience an average of 138 hours of application downtime.

In addition to the costs that can result from the hours spent by staff responding to the incident (See Table 1), the total average financial losses can include application downtime, business process work arounds, fines, legal fees, consultants/lawyers, MSSPs, notification of individuals and business partners affected by the exposure of their confidential information, loss of customers and business relationships due to reputational damage and more.

The frequency and severity of cloud account compromises increases. Organizations need to address the importance of preventing and quickly detecting cloud compromises because of the growing plethora of such incidents. In fact, 50 percent of respondents say the volume or frequency of cloud account compromises and 53 percent of respondents say the severity of cloud account compromises have significantly increased or increased over the past 12 months.

Figure 20. How has the volume and severity of cloud account compromises changed over the past 12 months?



On average, 16 cloud compromises are detected every three months or an average of 64 compromises per year. The average annual IT budget in the organizations represented in this research is $167 million, of that an average of 22 percent or $36.8 million is allocated to securing cloud-based resources.

A component of the total cost of compromised cloud accounts is time spent on the following activities: Organizing and planning the organization's approaches to the detection and containment of cloud account compromises, analyzing and investigating cloud account compromises, conducting forensic analysis of those accounts that have been compromised, documenting and reporting cloud account compromises in conformance with policies or compliance mandates and containing and remediating cloud account compromises.

An average of six IT security personnel is involved in these activities in their organizations. As shown in Table 1, the IT security team spends an average of 1,182 hours monthly and 14,184 hours annually to deal with cloud account compromises.

Table 1. Average hours spent monthly and annually on five steps to deal with cloud account compromises

Steps to respond to an account compromise	Average hours spent monthly by IT security	Average annual hours spent annually by IT security
Organizing and planning approaches to the detection and containment of cloud account compromises	158	1,896
Analyzing and investing cloud account compromises	290	3,480
Conducting forensic analysis on accounts determined to have been compromised	312	3,744
Documenting and reporting cloud account compromises in conformance with policies or compliance mandates	101	1,212
Containing and remediating cloud account compromises	321	3,852
Total	1,182	14,184

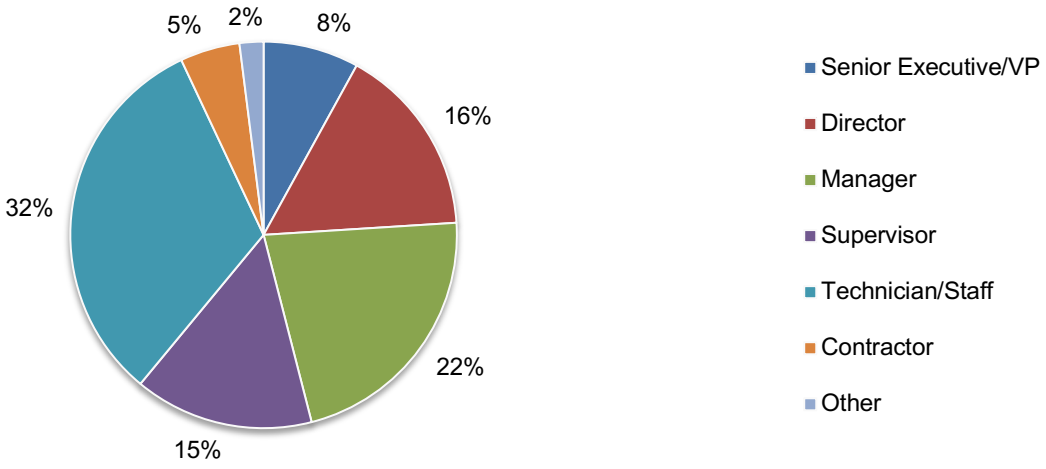
Part 3. Methodology

A sampling frame of 17,005 IT and IT security professionals in the United States were selected as participants to this survey. Table 1 shows 726 total returns. Screening and reliability checks required the removal of 64 surveys. Our final sample consisted of 662 surveys or a 3.9 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	17,005	100.0%
Total returns	726	4.3%
Rejected or screened surveys	64	0.4%
Final sample	662	3.9%

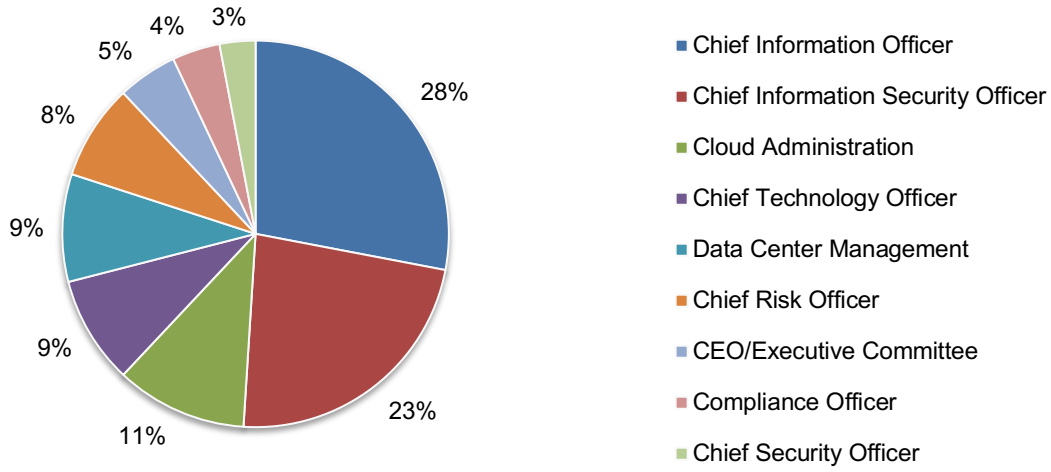
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (61 percent) of respondents are at or above the supervisory levels. The largest category at 32 percent of respondents is technician/staff.

Pie Chart 1. Current position within the organization



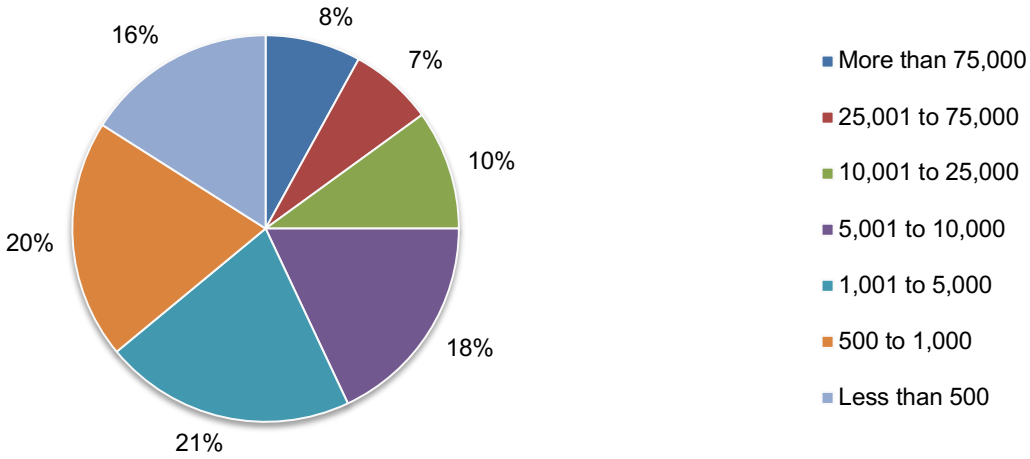
According to Pie Chart 2, 28 percent of respondents report to the chief information officer, 23 percent of respondents report to the chief information security officer, 11 percent of respondents report to cloud administration, 9 percent of respondents report to the chief technology officer and another 9 percent report to data center management.

Pie Chart 2. Primary person respondents or IT security leader reports to



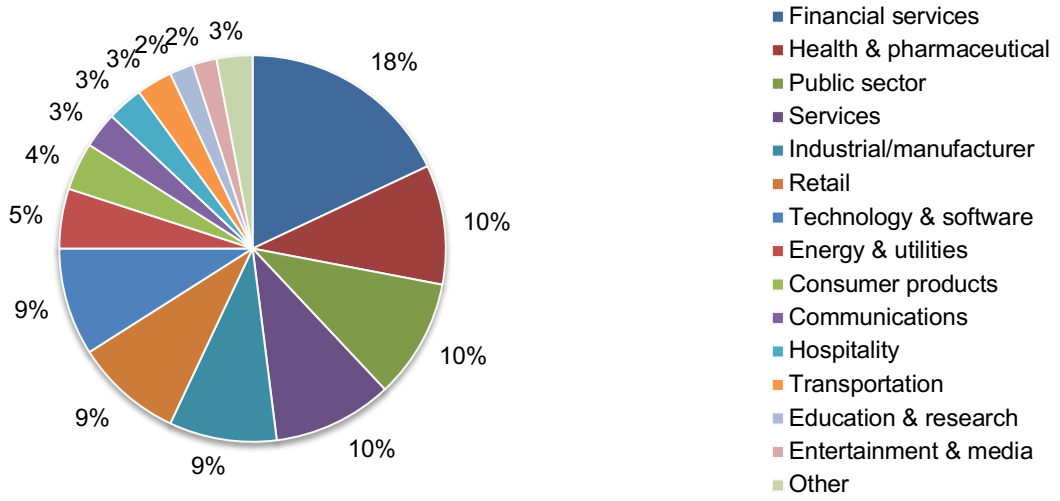
As shown in Pie Chart 3, 64 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 3. Global employee headcount



Pie Chart 4 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by followed by health and pharmaceutical (10 percent of respondents), public sector (10 percent of respondents), and services (10 percent of respondents). Industrial/manufacturer, retail, and technology and software are each at 9 percent of respondents.

Pie Chart 4. Industry focus of respondents' organizations



Part 4. 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.

Part 5. Appendix with the detailed audited findings

The following tables provide the frequency or percentage frequency of responses to al survey questions. All survey responses were captured in December 2020.

Survey response	Freq	Pct%
Total sampling frame	17,005	100.0%
Total returns	726	4.3%
Rejected surveys	64	0.4%
Final sample	662	3.9%

Part 1. Screening

S1. What percent of your organization's IT functions utilize cloud technologies?	Pct%
Less than 10% (stop)	0%
10% to 25%	18%
26% to 50%	28%
51% to 75%	29%
76% to 100%	25%
Total	100%
Extrapolated value	54%

S2. What best defines your familiarity with cloud compromises that have impacted your organization?	Pct%
Very familiar	43%
Familiar	31%
Somewhat familiar	26%
Not familiar (stop)	0%
Total	100%

S3. Did your organization experience one or more cloud compromises over the past 12 months?	Pct%
Yes	100%
No (stop)	0%
Unsure (stop)	0%
Total	100%

Part 2. Attributions about security in the cloud. Strongly Agree and Agree response	Pct%
Q1a. The move to the cloud and a mobile workforce has brought new security and compliance risks to my organization.	72%
Q1b. Cloud account takeovers present a significant security risk for my organization.	68%
Q1c. Cloud-based collaboration or messaging tools for sharing sensitive or confidential files present a significant security risk for my organization.	70%
Q1d. Shadow IT, which refers to the use of cloud apps and services without the explicit approval of IT, presents a significant security risk for my organization.	75%
Q1e. Office 365 and Google G Suite accounts are heavily targeted by brute force and phishing-based cloud attacks because they hold the key to business communications.	57%
Q1f. Phishing is the most frequent method that attackers use to acquire legitimate cloud credentials.	51%
Q1g. Internal phishing results in more compromised accounts.	48%
Q1h. My organization has established clearly defined roles and accountability for safeguarding of confidential or sensitive information stored in the cloud.	44%
Q1i. My organization is careful about sharing confidential or sensitive information with third parties such as business partners, contractors, and providers in the cloud environment.	40%
Q1j. My organization is concerned about oversharing of files via public links.	34%
Q1k. My organization is vigilant in conducting assessments of cloud apps before deployment.	39%
Q1l. My organization has 360 degree visibility of the sensitive or confidential data collected, processed and/or stored in the cloud.	32%
Q1m. Compliance with data protection regulations such as PCI DSS, HIPAA, NIST, GDPR and CCPA is a main driver to my organization's migration to the cloud ecosystem.	36%

Part 3. Cloud experience

Q2. What is your organization's primary cloud service provider? Please select no more than two choices.	Pct%
Microsoft Azure	44%
Amazon AWS	48%
Google	18%
IBM	17%
Oracle	9%
Alibaba	8%
Other (please specify)	0%
Total	144%

Q3a. Does your organization deploy a multicloud architecture or strategy?	Pct%
Yes	68%
No (Please skip to Q4)	31%
Unsure (Please skip to Q4)	1%
Total	100%

Q3b. If yes, how many different clouds does your organization use?	Pct%
One	0%
Two	21%
Three	35%
Four	27%
Five	11%
More than five	6%
Total	100%
Extrapolated value	3.5

Q4. If your organization does not deploy a multicloud architecture, will it deploy it in the future?	Pct%
Yes, within the next 6 months	52%
Yes, within the next 12 months	26%
No plans to deploy	22%
Total	100%

Q5. What are the primary reasons cloud resources are used within your organization? Please select only two choices.	Pct%
Reduce cost	45%
Increase efficiency	46%
Improve security	29%
Faster deployment time	23%
Increase flexibility and choice	25%
Improve customer service	15%
Comply with contractual agreements or policies	15%
Other (please specify)	2%
Total	200%

Q6. Who in your organization is most responsible for evaluating the cloud provider's security capabilities?	Pct%
End users	19%
Corporate IT	21%
Compliance	5%
Legal	7%
Procurement	4%
Internal audit	3%
Information security	23%
Physical security	6%
Other (please specify)	0%
No one person is responsible	12%
Total	100%

Q7. What percent of corporate data is stored in the cloud environment?	Pct%
Less than 5%	2%
Between 5 to 10%	6%
Between 11 to 20%	7%
Between 21 to 30%	15%
Between 31 to 40%	17%
Between 41 to 50%	21%
Between 51 to 60%	15%
Between 61 to 70%	7%
Between 71 to 80%	5%
Between 81 to 90%	2%
More than 90%	3%
Total	100%
Extrapolated value	42%

Q8. What percent of corporate data stored in the cloud environment is controlled by IT?	Pct%
Less than 5%	8%
Between 5 to 10%	11%
Between 11 to 20%	25%
Between 21 to 30%	15%
Between 31 to 40%	20%
Between 41 to 50%	8%
Between 51 to 60%	6%
Between 61 to 70%	6%
Between 71 to 80%	1%
Between 81 to 90%	0%
More than 90%	0%
Total	100%
Extrapolated value	27%

Q9. What percent of cloud services are deployed by departments other than corporate IT (e.g. shadow IT)?	Pct%
Less than 5%	0%
Between 5 to 10%	2%
Between 11 to 20%	5%
Between 21 to 30%	3%
Between 31 to 40%	5%
Between 41 to 50%	11%
Between 51 to 60%	11%
Between 61 to 70%	10%
Between 71 to 80%	14%
Between 81 to 90%	19%
More than 90%	20%
Total	100%
Extrapolated value	67%

Part 4. The threat to highly sensitive data in the cloud

Q10. How many times have attackers compromised cloud-based user accounts within your organization over the past 12 months?	Pct%
Once	4%
2 to 5	9%
6 to 10	11%
11 to 15	24%
16 to 20	27%
21 to 25	10%
26 to 50	9%
More than 50	6%
Total	100%
Extrapolated value	18.54

Q11. What were the consequences of the cloud compromises experienced by your organization over the past 12 months? Please select all that apply.	Pct%
Data theft	56%
Data breach	49%
Reputation damage	34%
Remediation costs	31%
Litigation costs	23%
Regulatory fines and penalties	9%
System downtime	53%
Leakage of intellectual property	39%
Fraudulent wire transfer	17%
Other (please specify)	5%
Total	316%

Q12a. Does your organization use SaaS resources from cloud service providers?	Pct%
Yes, heavy use	40%
Yes, moderate use	23%
Yes, light use	16%
No (skip to Q19a)	21%
Total	100%

Q12b. If yes, what percent of your organization's business-critical applications utilizes SaaS versus on-premises software applications?	Pct%
Less than 10%	6%
Between 11 to 20%	17%
Between 21 to 30%	25%
Between 31 to 40%	21%
Between 40 to 50%	14%
Between 50 to 75%	9%
Between 76 to 90%	5%
More than 90%	3%
Total	100%
Extrapolated value	36%

Q13. In your opinion, who is most responsible for ensuring the security of SaaS applications used within your organization?	Pct%
My company's end-users (e.g., LOB) are most responsible	30%
My company's IT function is most responsible	10%
My company's IT security function is most responsible	20%
The cloud service provider is most responsible	16%
Responsibility is shared between my company and the cloud service provider	24%
Total	100%

Q14. How important is the use of SaaS in meeting your organization's IT and data processing objectives?	
Q14a.Today	Pct%
Essential	29%
Very important	31%
Important	20%
Not important	12%
Irrelevant	8%
Total	100%

Q14b. Over the next two years	Pct%
Essential	38%
Very important	35%
Important	18%
Not important	9%
Irrelevant	0%
Total	100%

Q15. How confident are you that SaaS applications used within your organization are secure?	Pct%
Very confident	29%
Confident	30%
Not confident	41%
Total	100%

Q16. How confident are you that users are using approved SaaS apps for file sharing, social media collaboration and web conferencing (e.g. shadow IT)?	Pct%
Very confident	24%
Confident	30%
Not confident	46%
Total	100%

Q17. How confident are you that your IT organization knows all cloud computing applications, platforms or infrastructure services in use today?	Pct%
Very confident	19%
Confident	21%
Not confident	60%
Total	100%

Q18. Are SaaS applications evaluated for security prior to deployment within your organization?	Pct%
Yes	22%
No	58%
Don't know	20%
Total	100%

Part 5. Compromises in the cloud

Q19a. In the past 12 months, have your organization's users destroyed sensitive data?	Pct%
Yes	31%
No	49%
Unsure	20%
Total	100%

Q19b. If yes, how frequently did it happen in the past 12 months?	Pct%
Very frequently	24%
Frequently	27%
Somewhat frequently	21%
Not frequently	23%
Not at all	5%
Total	100%

Q19c. If yes, what were the consequences? Please check all that apply.	Pct%
The loss or theft of sensitive data	57%
Fines due to non-compliance with privacy and residency regulations	11%
Reputational damage	50%
Increased vulnerability to attackers	47%
Business disruption	52%
Other (please specify)	3%
Total	220%

Q20a. In the past 12 months, have users accidentally through carelessness, lack of awareness or account compromise exposed sensitive data?	Pct%
Yes	78%
No	12%
Unsure	10%
Total	100%

Q20b. If yes, how frequently did it happen in the past 12 months?	Pct%
Very frequently	33%
Frequently	30%
Somewhat frequently	17%
Not frequently	15%
Not at all	5%
Total	100%

Q20c. If yes, what were the consequences?	Pct%
The loss or theft of sensitive data	64%
Fines due to non-compliance with privacy and residency regulations	12%
Reputational damage	45%
Increased vulnerability to attackers	43%
Business disruption	60%
Other (please specify)	3%
Total	227%

Q21a. In the past 12 months, has your organization experienced an account compromise that exposed sensitive data?	Pct%
Yes	67%
No	30%
Unsure	3%
Total	100%

Q21b. If yes, how frequently did it happen in the past 12 months?	Pct%
Very frequently	35%
Frequently	21%
Somewhat frequently	17%
Not frequently	16%
Not at all	9%
Unsure	2%
Total	100%

Q21c. If yes, what were the consequences?	Pct%
The loss or theft of sensitive data	59%
Fines due to non-compliance with privacy and residency regulations	10%
Reputational damage	48%
Increased vulnerability to attackers	43%
Business disruption	56%
Other (please specify)	4%
Total	220%

Q22. How frequently does the theft of sensitive data occur when employees leave your organization?	Pct%
Very frequently	30%
Frequently	32%
Somewhat frequently	19%
Not frequently	12%
Not at all	6%
Unsure	1%
Total	100%

Q23a. How frequently have your organization's users installed unapproved cloud applications or used unsanctioned cloud services?	Pct%
Yes, very frequently	23%
Yes, frequently	32%
Yes, somewhat frequently	14%
Not frequently	24%
Not at all	7%
Unsure	0%
Total	100%

Q23b. If yes, what were the consequences?	Pct%
The loss or theft of sensitive data	25%
Fines due to non-compliance with privacy and residency regulations	16%
Reputational damage	40%
Increased vulnerability to attackers	37%
Business disruption	40%
Other (please specify)	3%
Total	161%

Part 6. Securing the cloud

Q24. What type of corporate data presents the greatest security risk to your organization when stored in the cloud? Please select only three choices.	Pct%
Email messages	51%
Consumer data	33%
Customer information	20%
Payment information	16%
Employee records	49%
Health information	27%
Financial business information	41%
Intellectual property such as source code, design plans, tech renderings	43%
Research data	20%
Other (please specify)	0%
Total	300%

Q25. How does your organization protect confidential or sensitive information in the cloud? Please select all that apply.	Pct%
We use private data network connectivity	42%
We use premium security services provided by the cloud provider	39%
We use encryption, tokenization or other cryptographic tools to protect data in the cloud	59%
We use a Cloud Access Security Broker (CASB)	56%
Don't know	5%
Other (please specify)	3%
Total	204%

Q26. What best describes your organization's approach to user access and identity management in the cloud environment? Please select all that apply.	Pct%
Separate identity management interfaces for the cloud and on-premise environment	45%
Unified identity management interface for both the cloud and on-premise environment	39%
Deployment of single sign-on (SSO)	18%
Hybrid combination of the above choices	42%
Don't know	5%
Total	149%

Q27. How important are each of the following features to your organization's ability to control and secure access to cloud resources? Essential and Very Important response combined.	Pct%
Q27a. Support multiple identity federation standards including SAML	73%
Q27b. Control strong authentication prior to accessing data and applications in the cloud	70%
Q27c. Utilize adaptive access controls to protect the users most at risk without reducing the productivity of other users	61%
Q27d. Expand or contract usage based on the organization's current needs/demands	54%
Q27e. Deploy short cycles and the ability to add new identity management services quickly	55%
Q27f. Accelerate on-boarding process for new users	70%
Q27g. Ensure consistently high availability of IT resources	75%

Part 7. Estimating the cost of compromised cloud accounts

Q28. Please estimate the financial lost due to compromised cloud accounts per year.	Pct%
Less than $10,000	0%
$10,000 to $50,000	0%
$51,000 to $100,000	3%
$100,001 to $500,000	11%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	15%
$5,000,001 to $10,000,000	30%
More than $10,000,000	28%
Total	100%
Extrapolated value	$ 6,192,750

Q29. In the past 12-month period, what percentage of your company's total revenues (gross sales) were lost due cloud compromises? Your best guess is welcome.	Pct%
None	6%
Less than 1%	25%
1 to 2%	21%
3 to 4%	21%
5 to 6%	9%
7 to 8%	6%
9 to 10%	7%
More than 10%	5%
Total	100%
Extrapolated value	3.5%

Q30. In the past 12-month period, what percentage of cloud compromises were enabled by account takeover? Your best guess is welcome.	Pct%
None	2%
Less than 1%	3%
1 to 2%	9%
3 to 4%	12%
5 to 6%	8%
7 to 8%	10%
9 to 10%	30%
More than 10%	26%
Total	100%
Extrapolated value	7.7%

Q31. On average, how many account compromises are detected by your organization per quarter? Your best guess is welcome.	Pct%
None	0%
1 to 2	6%
3 to 5	13%
6 to 10	21%
11 to 20	20%
21 to 25	25%
25 to 30	10%
More than 30	5%
Total	100%
Extrapolated value	15.89

Q32. Within your organization, how many IT security personnel are involved in the detection and containment of cloud account compromises?	Pct%
None	4%
1 to 2	32%
3 to 5	35%
6 to 10	13%
11 to 15	7%
16 to 20	5%
21 to 25	3%
More than 25	1%
Total	100%
Extrapolated value	5.72

Q33. In your opinion, how has the volume or frequency of cloud account compromises changed over the past 12 months?	Pct%
Significant increase	25%
Increase	25%
Stayed the same	23%
Decrease	19%
Significant decrease	8%
Total	100%

Q34. In your opinion, how has the severity of cloud account compromises changed over the past 12 months?	Pct%
Significant increase	29%
Increase	24%
Stayed the same	23%
Decrease	17%
Significant decrease	7%
Total	100%

Q35. Approximately, how many hours each week are spent organizing and planning the organization's approaches to the detection and containment of cloud account compromises? Please estimate the aggregate hours of the IT and IT security team.	Pct%
Less than 5	0%
5 to 10	3%
11 to 25	5%
26 to 50	16%
51 to 100	31%
101 to 250	26%
251 to 500	14%
More than 500	5%
Total	100%
Extrapolated value	158.21

Q36. Approximately, how many hours each week are spent analyzing and investigating cloud account compromises? Please estimate the aggregate hours of the IT security team.	Pct%
Less than 5	0%
5 to 10	0%
11 to 25	3%
26 to 50	8%
51 to 100	12%
101 to 250	27%
251 to 500	31%
More than 500	19%
Total	100%
Extrapolated value	289.93

Q37. Approximately, how many hours each week are spent conducting forensic analysis for those accounts, believed to have been compromised cloud account compromises? Please estimate the aggregate hours of the IT security team.	Pct%
Less than 5	0%
5 to 10	3%
11 to 25	11%
26 to 50	9%
51 to 100	7%
101 to 250	14%
251 to 500	26%
More than 500	30%
Total	100%
Extrapolated value	312.33

Q38. Approximately, how many hours each week are spent documenting and/or reporting upon cloud account compromises in conformance with policies or compliance mandates? Please estimate the aggregate hours of the IT security team.	Pct%
Less than 5	7%
5 to 10	12%
11 to 25	14%
26 to 50	19%
51 to 100	24%
101 to 250	14%
251 to 500	5%
More than 500	5%
Total	100%
Extrapolated value	101.37

Q39. Approximately, how many hours each week are spent containing and remediating cloud account compromises? Please estimate the aggregate hours of the IT and IT security team.	Pct%
Less than 5	0%
5 to 10	0%
11 to 25	2%
26 to 50	12%
51 to 100	16%
101 to 250	14%
251 to 500	25%
More than 500	31%
Total	100%
Extrapolated value	321.07

Q40. In an average month, how much application downtime resulting from account compromises do you experience?	Pct%
None	8%
Less than 1 hour	9%
1 to 2 hours	11%
3 to 5 hours	16%
6 to 10	17%
11 to 24 hours	19%
24 hours+	20%
Total	100%
Extrapolated value	11.54

Part 8. Budget

Q41a. What range best describes your organization's annual IT budget in the current fiscal year?	Pct%
Less than $1 million	2%
$1 to $10 million	6%
$11 to $25 million	10%
$26 to $50 million	21%
$51 to $100 million	18%
$101 to $250 million	20%
$251 to $500 million	13%
More than $500 million	10%
Total	100%
Extrapolated value	$ 167.29

Q41b. If yes, what percentage of your company's annual IT budget is dedicated to securing cloud-based resources?	Pct%	
None	2%	
Less than 5%	7%	
5% to 10%	9%	
11% to 15%	18%	
16% to 20%	25%	
21% to 30%	18%	
31% to 50%	14%	
More than 50%	7%	
Total	100%	
Extrapolated value	22%	$ 36.78

Part 9. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive/VP	8%
Director	16%
Manager	22%
Supervisor	15%
Technician/Staff	32%
Contractor	5%
Other (please specify)	2%
Total	100%

D2. Check the primary person you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	5%
Chief Information Officer	28%
Chief Information Security Officer	23%
Chief Risk Officer	8%
Chief Security Officer	3%
Chief Technology Officer	9%
Compliance Officer	4%
Data Center Management	9%
Cloud Administration	11%
Other (please specify)	0%
Total	100%

D3. What is the worldwide headcount of your organization?	Pct%
Less than 500	16%
500 to 1,000	20%
1,001 to 5,000	21%
5,001 to 10,000	18%
10,001 to 25,000	10%
25,001 to 75,000	7%
More than 75,000	8%
Total	100%
Extrapolated value	13,820.00

D4. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	4%
Defense & aerospace	0%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	10%
Hospitality	3%
Industrial/manufacturer	9%
Public sector	10%
Retail	9%
Services	10%
Technology & software	9%
Transportation	3%
Other (please specify)	2%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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 **Insights Association,** 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.