The 2018 Global Cloud Data Security Study

Independently conducted by Ponemon Institute LLC
Publication Date: January 2018
## Contents Page

<table>
<thead>
<tr>
<th>Part</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1. Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Part 2. Key Findings</td>
<td>6</td>
</tr>
<tr>
<td>Part 3. Demographics</td>
<td>36</td>
</tr>
<tr>
<td>Part 4. Caveats to the Study</td>
<td>39</td>
</tr>
</tbody>
</table>
Executive Summary

PART 1

The following are important trends in cloud data security:

IT security may be losing its relevance in determining cloud security strategies for several reasons shown in the research findings.

First, more corporate data is stored in the cloud but the IT department has less control over it. Second, security practitioners are often not the decision maker when it comes to the use of cloud resources. Third, IT is losing control of corporate IT spending.

Companies anticipate significant growth in the use of cloud services.

Today cloud computing applications and platform solutions are considered critical to their organizations’ operations, according to 79 percent of respondents and 87 percent of respondents say the cloud will increase in importance in the next two years. In two years an average of 51 percent of all IT and data processing requirements will be in the cloud, an increase from today’s average of 39 percent. On average, companies are using 27 cloud applications. Cloud infrastructure applications, such as online backup, virtual desktop and email texting and other communication tools have increased significantly in use since 2015.
Regulated data such as payment and customer information continue to be most at risk.

Because of the sensitivity of the data and the need to comply with privacy and data protection regulations, companies worry most about payment and customer information. This has been consistent over the past three years.

Compliance with GDPR will require changes in cloud governance.

Any company outside of the EU that is targeting consumers in the EU will be subject to the GDPR. Eighty-eight percent of respondents anticipate the GDPR will require changes in cloud governance.

More companies are selecting cloud providers because they will improve security.

While cost and faster deployment time are the most important criteria for selecting a cloud provider, security has increased from 12 percent of respondents in 2015 to 26 percent in 2017.

Confidence in knowing all cloud computing services in use is increasing.

As an example of companies making progress in securing data in the cloud, 54 percent of respondents are either very confident (24 percent) or confident (30 percent) that the IT organization knows all cloud computing applications, platform or infrastructure services in use today. This is an increase from 45 percent of respondents in the previous study, as shown in Figure 16.

Encryption in the cloud is increasing in use and importance.

Seventy-seven percent of respondents say the ability to encrypt or tokenize sensitive or confidential data is important and 91 percent say it will become more important over the next two years, an increase from 86 percent of respondents. Currently, an average of 40 percent of data in the cloud is secured with encryption and key management.

The storage of keys is shifting from software to hardware.

Most encryption keys are still stored in software (38 percent vs. 45 percent in 2015). However, the storage of keys in hardware increased from 27 percent of respondents in the previous study to 35 percent of respondents.

Security risks caused by the use of social identities to regulate access have increased.

Sixty-seven percent of respondents say the management of user identities is more difficult in the cloud than the on-premises environment. The use of social identities in regulating access to cloud resources increases security risk.
Key Findings

In this section we provide an analysis of the key findings. The report is organized according to the following topics:

- The cloud’s growing importance demands a greater commitment to security
- Control of cloud security practices and budget is shifting away from IT
- Trends in cloud security practices
- Encryption, tokenization or other cryptologic solutions increase in use and importance
- Identity and access management in the cloud
- Country differences

The cloud’s growing importance demands a greater commitment to security

Companies anticipate significant growth in the use of cloud services.

Cloud computing applications and platform solutions are considered very important or important to their organizations’ operations, according to 79 percent of respondents. Eighty-seven percent of respondents say cloud solutions will become very important or important over the next two years. The use of cloud computing resources for total IT and data processing requirements is expected to increase from an average of 39 percent to an average of 51 percent in the next two years.

Does the growth and importance of the cloud mean there is an increase in policies and procedures to safeguard data? Despite the finding that 67 percent of respondents say their organizations are committed to protecting confidential or sensitive information in the cloud, Figure 2 reveals that 53 percent of respondents (100 minus 47 percent) do not agree their organizations have a proactive approach to managing compliance with privacy and data protection regulations in the cloud environment. Fifty-seven percent of respondents (100 minus 43 percent) do not agree that their organization is careful about sharing sensitive information with third parties such as business partners, contractors and providers in cloud environments.

Figure 2. Perceptions about governance practices in the cloud

(Strongly agree and agree responses combined)

<table>
<thead>
<tr>
<th>Perception</th>
<th>FY 2015</th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed to protecting confidential or sensitive information in the cloud</td>
<td>43%</td>
<td>44%</td>
<td>47%</td>
</tr>
<tr>
<td>Proactive in managing compliance with privacy and data protection regulations in the cloud environment</td>
<td>43%</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Careful about sharing confidential or sensitive information with third parties such as business partners, contractors, and providers in the cloud environment</td>
<td>43%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The type of corporate data stored in the cloud is also the data most at risk.

As shown in Figure 3, customer information, emails, consumer data, employee records and payment information are most often stored in the cloud. Since 2015, the storage of customer information has maintained a significant share of more than half of the respondents.

**Figure 3. The primary types of data stored in the cloud**
More than one response permitted
Regulated data such as payment and customer information continue to be most at risk.

Because of the sensitivity of the data and the need to comply with privacy and data protection regulations, companies worry most about payment information and customer information. This has been consistent over the past three years, as shown in Figure 4.

Compliance with GDPR will require changes in cloud governance.

Specifically, any company outside of the EU that is targeting consumers in the EU will be subject to the GDPR. Sixty percent of respondents believe they are not ready to comply with the GDPR. 88 percent of respondents [37 percent + 34 percent + 16 percent] anticipate the GDPR will require nominal to significant changes in cloud governance.
Control of cloud security practices and budget is shifting away from IT security

**IT is losing control of its budget and corporate data stored in the cloud.**

The average percent of total corporate IT spending controlled by the IT department has declined from 53 percent in 2016 to 40 percent in 2017.

Functions outside of IT are deploying an average of 58 percent of cloud services. The percent of cloud services deployed by departments other than corporate IT has increased significantly since 2016. More corporate data is stored in the cloud and the IT department has less control of corporate data in the cloud. Both the percent of corporate data stored in the cloud environment has grown significantly and the average percent of corporate data stored in the cloud environment is not managed or controlled by the IT department has also grown from 44 percent to 53 percent.

However, on a positive note, confidence in knowing all cloud computing services in use is increasing. According to Figure 5, 56 percent of respondents are either very confident (25 percent) or confident (31 percent) that the IT organization knows all cloud computing applications, platform or infrastructure services in use today. This is an increase from 45 percent of respondents in the 2015 study.

**Figure 5. How confident are you that IT knows all cloud computing services in use today?**

- **Very confident:**
  - FY 2015: 19%
  - FY 2016: 24%
  - FY 2017: 25%

- **Confident:**
  - FY 2015: 30%
  - FY 2016: 26%
  - FY 2017: 31%

- **Not confident:**
  - FY 2015: 46%
  - FY 2016: 43%
  - FY 2017: 55%
Trends in cloud security practices

Difficulty in protecting confidential or sensitive information when using cloud services decreases.

The difficulty in protecting confidential or sensitive information when using cloud services decreases. In the previous study, 54 percent of respondents, a decrease from the previous year of 60 percent, said it is more difficult to protect confidential or sensitive information when using cloud services. This year, the percentage has decreased to less than half of the percent of respondents (49 percent).

However, organizations still face challenges in the protection of confidential information when using cloud services. Figure 6 reveals that the difficulty in controlling or restricting end-user access has decreased slightly from 53 percent of respondents in the previous study to 51 percent of respondents. Other reasons why cloud security is a challenge is the difficulty in applying conventional information security in the cloud computing environment (71 percent) and the inability to directly inspect cloud providers for security compliance (67 percent).

Figure 6. Why cloud security is still difficult to achieve

More than one response permitted

- It is more difficult to apply conventional information security in the cloud computing environment: 71%, 70%, 71%
- It is more difficult to inspect cloud provider for security compliance directly: 67%, 69%, 70%
- It is more difficult to control or restrict end-user access: 51%, 53%, 48%

Don’t know: 5%, 5%, 5%

Other: 2%, 2%, 2%
Compliance in the cloud is difficult to achieve.

Sixty-two percent of respondents say the use of cloud resources increases compliance risk. This can be due to the difficulty in controlling end-user access to sensitive data in the cloud. According to Figure 7, only 28 percent of respondents say the cloud has no effect on the company’s ability to comply with privacy and data protection regulations or legal requirements around the globe.
Security practitioners are not the decision makers when it comes to the use of cloud resources.

According to Figure 8, only 21 percent of respondents say members of the security team are involved in the decision-making process about using certain cloud applications or platforms always (8 percent) or most of the time (13 percent). This is similar to the previous study.

Most organizations still do not have security policies for the cloud. Fifty-four percent of respondents say their organizations do not have a policy that requires the use of security safeguards such as encryption as a condition to using certain cloud computing applications. However, this is a decrease from 60 percent of respondents in the previous study who said there were no policies.

Figure 8. Is the security team involved in cloud decisions?
Responsibility for cloud security is moving to the cloud user.

According to Figure 9, respondents have mixed views on who should be most responsible for protecting sensitive or confidential data in the cloud. Fewer respondents (32 percent of respondents) say it is a shared responsibility. Respondents are evenly divided between responsibility resting with the cloud provider or cloud user (both 34 percent).

Figure 9. Who is responsible for cloud security?
Efficiency and cost are the most important factors for selecting a cloud provider, not security.

The primary reasons for selecting a particular cloud provider are efficiency (42 percent of respondents) or cost (39 percent), as shown in Figure 10. However, more respondents say security is a consideration when selecting a cloud provider (23 percent) than in previous studies.
Evaluation of cloud providers is shifting to the end-user.

Sixty-one percent of respondents say their organizations evaluate the security capabilities prior to engagement or deployment. Only 14 percent of respondents say it is the security function that is most responsible for evaluating the cloud provider’s security capabilities, as shown in Figure 11. More respondents increasingly believe the end-user is responsible for security evaluations (31 percent), and less (22 percent) responsible by corporate IT.

Figure 11. Who evaluates the cloud provider’s security capabilities?

<table>
<thead>
<tr>
<th>Evaluation Role</th>
<th>FY 2015</th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-users</td>
<td>27%</td>
<td>23%</td>
<td>30%</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>27%</td>
<td>25%</td>
<td>31%</td>
</tr>
<tr>
<td>No one person is responsible</td>
<td>20%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>Information security</td>
<td>16%</td>
<td>15%</td>
<td>14%</td>
</tr>
<tr>
<td>Compliance</td>
<td>4%</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>Legal</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Procurement</td>
<td>3%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Internal audit</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
</tr>
</tbody>
</table>
Security evaluations of cloud providers rely increasingly on contractual negotiations and legal reviews.

Figure 12 reveals a significant aspect in the use of contractual negotiation and legal reviews to evaluate cloud providers from 51 percent of respondents in a previous study to 58 percent of respondents. Word-of-mouth or market reputation is used to evaluate the provider by 51 percent of respondents, followed by availability of information security tools (48 percent).

Fewer organizations look at proof of security compliance (42 percent), a self-assessment security questionnaire (34 percent) and an assessment by in-house security team (24 percent). Similar to the previous study, only 18 percent of respondents say their organizations conduct a third-party assessment by security expert or auditor.
The inability to control end-users is resulting in more cloud resources deployed without evaluation.

As shown in Figure 13, it is the loss of control over end-users that results in cloud resources deployed without security scrutiny. Other reasons are not enough resources to conduct an evaluation (58 percent of respondents) and increasingly no one is in-charge (41 percent vs. 35 percent in a previous study).
Protection of data in the cloud is important but not practiced.

More organizations use private data network connectivity to secure data in the cloud. Similar to the previous study, when asked what security solutions are used to protect data in the cloud, 40 percent of respondents say their organizations use encryption, tokenization or other cryptographic tools, as shown in Figure 14. Slightly more respondents (41 percent) say they use private data network connectivity.

Thirty-five percent of respondents say they don’t know what security solutions they use. A possible explanation is that business units and corporate IT are making investments in security without input from IT security.
Encryption, tokenization or other cryptologic solutions increase in use and importance

Seventy-seven percent of respondents say the ability to encrypt or tokenize sensitive or confidential data is important and 91 percent say it will become more important over the next two years, an increase from 86 percent of respondents. According to Figure 15, more respondents than in the previous study say their organizations use encryption, tokenization or other cryptographic solutions to secure sensitive or confidential information at rest, up from 36 percent of respondents in 2015.

Figure 15. Use of encryption, tokenization or other cryptographic solution to secure data at rest in the cloud

More respondents say encryption is used when it is sent and received by the cloud provider (58 percent). Encryption or tokenization of sensitive or confidential data directly within cloud applications such as SaaS has increased from 28 percent to 34 percent to 36 percent of respondents.

Encryption is used when it is sent and received by the cloud provider

Encryption or tokenization of data directly within cloud applications
Encryption to sensitive or confidential information is most often made unreadable before it is sent to the cloud.

If data at rest is encrypted, as shown in Figure 16, 43 percent say the data is made unreadable before it is sent to the cloud. The remaining respondents say it is made unreadable in the cloud using tools supplied by their organization or the cloud provider (27 percent of respondents and 28 percent of respondents, respectively). These results are consistent to the previous study.
There is a lack of encryption of cloud applications (SaaS).

According to the study, Software as a Service (SaaS) is used more frequently than Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Only 16 percent of respondents say they don’t use SaaS, a large drop from previous studies holding at 54 percent. Seventy-three percent of respondents say they use business applications such as document sharing tools and 78 percent of respondents say they use online backup. However, only 36 percent of respondents say their organization encrypts or tokenizes sensitive or confidential data directly within these applications.

According to Figure 17, an average of 12.7 applications requires encryption. This is a continuing increase from 11.9 in the previous study.

Figure 17. How many applications require encryption?
Extrapolated value 12.7

<table>
<thead>
<tr>
<th>Applications</th>
<th>Less than 5</th>
<th>5 to 10</th>
<th>11 to 20</th>
<th>More than 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>17%</td>
<td>19%</td>
<td>33%</td>
<td>38%</td>
</tr>
<tr>
<td>2016</td>
<td>17%</td>
<td>28%</td>
<td>35%</td>
<td>35%</td>
</tr>
<tr>
<td>2017</td>
<td>17%</td>
<td>28%</td>
<td>35%</td>
<td>35%</td>
</tr>
</tbody>
</table>
How prevalent is the use of key management systems?

Figure 18 reveals that on average organizations have 8.9 key management systems or encryption platforms, an increase from 7.5 in the previous study.

Fifty-two percent of respondents say their organizations control the encryption keys when data is encrypted in the cloud. Twenty-one percent say it is the cloud provider and 16 percent say a third party controls the encryption keys (neither the organization nor cloud provider).

Figure 18. How many key management systems or encryption platforms does your organization have?

Extrapolated value 8.9

<table>
<thead>
<tr>
<th>Less than 5</th>
<th>5 to 10</th>
<th>11 to 20</th>
<th>More than 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>28%</td>
<td>16%</td>
<td>4%</td>
</tr>
<tr>
<td>42%</td>
<td>41%</td>
<td>13%</td>
<td>1%</td>
</tr>
<tr>
<td>43%</td>
<td>43%</td>
<td></td>
<td>1%</td>
</tr>
</tbody>
</table>

Average number of key management systems:

- 7.2 in 2015
- 7.5 in 2016
- 8.9 in 2017

Organization that control their own encryption keys for data in the cloud:

- 52% in 2017
- 55% in 2016
- 54% in 2015
The storage of keys is shifting from software to hardware.

As shown in Figure 19, most encryption keys are still stored in software (38 percent overall). However, the storage of keys in hardware increased from 27 percent of respondents in a previous study to 35 percent of respondents.
Identity and access management in the cloud

Strong authentication measures continue to be important.

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

The most important features of controlling and securing access to cloud resources are shown in Figure 20. The ability to control strong authentication prior to accessing data and applications in the cloud has increased from 73 percent of respondents to 81 percent of respondents over the past few studies. A record of consistently high availability is important, according to 70 percent of respondents.

<table>
<thead>
<tr>
<th>Feature</th>
<th>FY 2015</th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of user identities is more difficult in the cloud than the on-premises environment</td>
<td>67%</td>
<td>69%</td>
<td>70%</td>
</tr>
<tr>
<td>The ability to control strong authentication prior to accessing data and applications in the cloud</td>
<td>73%</td>
<td>78%</td>
<td>81%</td>
</tr>
<tr>
<td>A record of consistently high availability</td>
<td>67%</td>
<td>69%</td>
<td>70%</td>
</tr>
<tr>
<td>The ability to support multiple identity federation standards including SAML</td>
<td>56%</td>
<td>65%</td>
<td>67%</td>
</tr>
<tr>
<td>The existence of short deployment cycles and the ability to add new identity management services quickly</td>
<td>58%</td>
<td>60%</td>
<td>63%</td>
</tr>
<tr>
<td>The ability to utilize social identities provided from trusted third parties</td>
<td>58%</td>
<td>59%</td>
<td>61%</td>
</tr>
<tr>
<td>The existence of an accelerated on-boarding process for new users</td>
<td>58%</td>
<td>56%</td>
<td>54%</td>
</tr>
<tr>
<td>The ability to expand or contract usage based on the organization’s current needs</td>
<td>57%</td>
<td>55%</td>
<td>55%</td>
</tr>
</tbody>
</table>

Figure 20. Most important identity and access management features

Essential and very important responses combined
Most organizations permit third-party users to access data in the cloud.

Sixty-three percent of respondents say their organizations have third-party users accessing their data and information in the cloud. As shown in Figure 21, more than half of respondents (53 percent of respondents) say their organization uses multi-factor authentication to secure access to data in the cloud environment.

Just under that percentage of respondents (47 percent) say their organizations use multi-factor authentication for employees’ access to the cloud. When asked the percent of cloud applications that have user-enabled access controls, the average is only 19 percent.

Figure 21. Use of multi-factor authentication for third-party access

- Employ multi-factor authentication to secure access to data in the cloud environment
- Deploy multi-factor authentication for internal employees’ access to data in the cloud environment
Country differences

In this section, we analyze the differences among the following countries included in this research: United States (US), United Kingdom (UK), Australia (AU), Germany (DE), France (FR), Japan (JP), India (IN) and Brazil (BZ). German organizations seem to be the most proactive in securing sensitive and confidential information in the cloud, managing the complexity of privacy and data protection regulations in the cloud environment, and ensuring security polices for the cloud are in place.

Third party data sharing practices are most strict, according to respondents in German organizations.

As shown in Figure 22, 61 percent of German respondents agree that their organizations are careful when sharing sensitive and confidential information with third parties. Contrastly, only 34 percent of respondents in Brazil and 31 percent of Japanese respondents agree their organizations are careful when sharing sensitive information.

---

**Figure 22. My organization is careful about sharing confidential or sensitive information with third parties such as business partners, contractors and providers in the cloud environment**

Strongly agree and agree responses combined
German organizations are most proactive in managing compliance with regulations.

Sixty-nine percent of respondents in Germany agree their organizations are most proactive in managing compliance with privacy and data protection regulations in the cloud environment. Only 35 percent of Australia respondents say their organizations are proactive in making sure the handling of sensitive and confidential information is in compliance, as shown in Figure 23.

**Figure 23. My organization is proactive in managing compliance with privacy and data protection regulations in the cloud environment**
Strongly agree and agree responses combined
Most global respondents believe it is a challenge to manage privacy and data protection regulations in the cloud.

According to Figure 24, respondents in France, the US and India (97 percent, 87 percent and 83 percent, respectively) believe it is more complicated to manage privacy and data protection regulations in a cloud environment than in on-premises networks.
Germany and France are most likely to evaluate the security capabilities of cloud providers.

As shown in Figure 25, 73 percent of German respondents and 69 percent of UK respondents say their organizations evaluate the security capabilities of cloud providers. Only 54 percent of Australia respondents and 41 percent of Brazilian respondents say their organizations evaluate cloud providers prior to deployment or engagement.
How confident are respondents that they know all cloud computing applications, platform or infrastructure services in use in their organizations?

Sixty-one percent of respondents in Australia are not confident that their organizations have visibility into the use of cloud computing applications, platform or infrastructure services. France is the most confident (only 25 percent of respondents say they are not confident), as revealed in Figure 26.

Figure 26. Are you confident your IT organization knows all cloud computing applications, platform or infrastructure services in use today?
Not confident responses
Cloud services are considered to make the protection of confidential or sensitive information difficult.

As shown in Figure 27, 57 percent of respondents in Australia believe it is more difficult to protect confidential or sensitive information. Respondents in France and Germany are least likely to think it is difficult.
Security policies are most likely to exist in Germany and France.

Sixty-five percent of German respondents say their organizations have a policy that requires the use of security safeguards such as encryption as a condition to using certain cloud computing applications, according to Figure 28. In contrast, only 33 percent of respondents in the India and 26 percent of respondents in Brazil say their organizations have such policies in place.

Figure 28. Does your organization have a policy that requires the use of security safeguards as a condition to using certain cloud computing applications?
Yes responses
Strong authentication measures are important globally.

India and the US are most likely to believe the ability to support federations including SAML are essential or very important (78 percent and 77 percent of respondents, respectively). The least likely to think this ability is important are Brazil and Japan (45 percent and 52 percent of respondents, respectively).
Controlling authentication prior to cloud access is important.

As shown in Figure 30, respondents in Australia and India (92 percent and 85 percent of respondents, respectively) believe the ability to control strong authentication prior to accessing data and applications in the cloud is essential or very important. Seventy-four percent of respondents in the UK are least likely to believe that such an ability is critical.
Consensus says managing user identities in the cloud is challenging.

Respondents in France, the US and India (82 percent, 73 percent and 73 percent of respondents, respectively) are more likely to agree that the management of user identities is more difficult in the cloud than the on-premises environment.
A sampling frame of 94,577 experienced IT and IT security practitioners located in the United States, United Kingdom, Australia, Germany, France, Japan, India and Brazil who are familiar and involved in their company’s use of both public and private cloud resources were selected as participants in the research. Table 1 shows 3,621 total returns. Screening and reliability checks required the removal of 336 surveys. Our final sample consisted of 3,285 surveys or a 3.5 percent response.

Table 1.

<table>
<thead>
<tr>
<th>Sample response</th>
<th>US</th>
<th>UK</th>
<th>AU</th>
<th>DE</th>
<th>FR</th>
<th>JP</th>
<th>IN</th>
<th>BZ</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>16,063</td>
<td>11,240</td>
<td>6,455</td>
<td>12,320</td>
<td>11,700</td>
<td>11,842</td>
<td>12,867</td>
<td>12,090</td>
<td>94,577</td>
</tr>
<tr>
<td>Total returns</td>
<td>645</td>
<td>439</td>
<td>267</td>
<td>521</td>
<td>338</td>
<td>460</td>
<td>549</td>
<td>402</td>
<td>3,621</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>70</td>
<td>34</td>
<td>23</td>
<td>29</td>
<td>45</td>
<td>36</td>
<td>52</td>
<td>47</td>
<td>336</td>
</tr>
<tr>
<td>Final sample</td>
<td>575</td>
<td>405</td>
<td>244</td>
<td>492</td>
<td>293</td>
<td>424</td>
<td>497</td>
<td>355</td>
<td>3,285</td>
</tr>
</tbody>
</table>
Pie Chart 1 reports the respondent’s organizational level within participating organizations. By design, 56 percent of respondents are at or above the supervisory levels.

As shown in Pie Chart 2, 60 percent of respondents reported their functional area as IT operations, 20 percent reported security and 14 percent report lines of business (LOB).
Pie Chart 3 reports the industry classification of respondents’ organizations. This chart identifies financial services (15 percent) as the largest segment, followed by public sector (14 percent) and industrial organizations (11 percent).

As shown in Pie Chart 4, 65 percent of respondents are from organizations with a global headcount of more than 1,000 employees.
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.
Visit the website for more information: www2.gemalto.com/cloud-security-research

Learn more about Gemalto’s Cloud Data Security solutions at: safenet.gemalto.com/cloud-data-security

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

©Gemalto 2018. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. (EN)-Feb.15.2018 - Design: GH