

---

## State of Cloud Adoption and Security in India

---

**Dr Vanishree Pabalkar<sup>1</sup>,**

Assistant Professor

Symbiosis International University

**Mr Allan Jose<sup>2</sup>**

Research Student

Symbiosis International University

### ABSTRACT

Around the world IT leaders are at a very fast pace coming up with innovations and working together which revolves around cloud computing. At a world where data and storing has been a major issue and hackers are challenging them every day, the Chief Information Officers (CIO) are integrating data and analytics in the cloud and securing them safely. Now-a-days social platforms are being key elements and used for organizational benefits, these are often based in Platform-as-a-service (PaaS) and API technologies. Companies are leveraging various cloud platforms including public and private, sometime a mix of both, SaaS, PaaS, IaaS. These advantage and benefits welcomes more and more concerns related to security.

In India most of the Small and Medium Business (SMBs) have a huge potential to implement and adopt cloud security but due to negligence and lack of awareness about the potential problems that could occur most of them has not yet adopted it yet. For example, most enterprises have adopted BYOD initiatives in the workplace but what they do not realize is that if a mobile device with cloud access is compromised, the cloud itself can be compromised. Another important factor is that a lot of jobs can be generated in this cloud arena and immense innovation can take place producing millions of dollars as revenue.

Businesses are hesitant about the cloud mainly because of data security issues like security policies and control and access at provider sites, financial viability, compliance requirements, lack of recruiting appropriate staff etc.

**KEY WORDS:** Cloud computing, Data Security, PaaS, SaaS, IaaS, Bring your own device (BYOD), Chief Information Officer (CIO).

## INTRODUCTION

Cloud-based IT, particularly public cloud services, diminishes the upfront expenditures associated with hardware and software purchases and application.

According to a report published by Cisco, there is a 30% rise in the public cloud services when comparing to last year. Infrastructure as Service (IaaS) is the most growing segment in the market. Software-as-a-Service (SaaS) is the largest which account to about 34% of the total market (CAGR). It has been predicted by Gartner that by 2017 about 1676 million USD would be spent on the entire cloud market, out of which about 514 million would be for SaaS.

As seen below in the graph, it is predicted that Software-as-a-Service would have a share of 59%, Infrastructure-as-a-Service (IaaS) would grow to 28% and Platform-as-a-Service (PaaS) to 11% by 2019.



Source of the graph: Cisco Global Cloud Index, 2014-2019

## Current Scenario & Factors affecting Public Cloud Adoption in India

A lot of global players in cloud are looking up the Indian market for cloud related services and even setting up local data centers like IBM, Microsoft and Amazon. These efforts made by them are to increase the performance and make a request to its

customers to go ahead who face a regulatory restriction on data location.

Like all other emerging markets in the world, one of the encounters for public cloud computing is lack of infrastructure. Another challenge would be that of the public disparity between rural and urban residents. Their education levels come to play, educated and uneducated, those who access

### **Technology and those who don't.**

Now-a-days most of the SMBs adopt cloud computing because of the scale of adaptability and reduce costs, but still too many security and information leakage remains a paramount challenge to trust with the cloud security vendors. Nevertheless, many companies have adopted and showcased results. This is mainly due to the presence of existing IT department, hence becomes very easy to adopt and enjoy all the functionalities it delivers. They can transfer anything in to the cloud and access it anywhere.

A haunting problem with our country is that we not only lack the required infrastructure but also inconsistency of power supply in many parts of the country. India is ranked 113 out of 142 by the World Economic Forum for the availability of internet bandwidth, which tells us about the amount of internet traffic exchanged between different nations.

Fortunately, the government of India has figured out the problems and challenges. The governments very ambitious Digital India programs has come across and helped address some of the issues but it still need meaningful developments.

### **OBJECTIVES**

The main objective of the study is as following:

1. Survey - To research and analyze the perception of the cloud adoption as well as the security of the cloud in India. Instasafe wanted to know more on the understanding where India stands among other nations when it comes to the cloud domain.
2. Email Campaign – To find potential customers who would want Instasafe's service. Hence work with Lead Squared, a B2C marketing automation software where clear trigger based emails can be set up according to timeline. It helped the company to generate leads.
3. Social Media Campaign – To help the company to increase exposure, expand net traffic, engagement, develop business partnership and improve sales.

4.

## METHODOLOGY

**Primary Data:** All the data collected for the purpose of the survey was primary data. The structured questionnaire was prepared and sent to all the respondents through mail. Few of the CIOs were contacted through telephone and some through WhatsApp messenger as few of them were travelling or not available. The respondents were spread across India spanning SMBs to MNCs.

The questionnaire was the same for everyone, for those who were interviewed telephonically, their answers were recorded and filled.

**Sampling Technique and Size:** The sampling technique used was Stratified random sampling. The target customer base was the CIOs, which is a very niche segment. The survey was open to any sector of the business and the survey was administered pan India. The survey was administered to about 150 CIOs

## ANALYSIS OF DATA

All data collected and analyzed had been presented in the form of table and charts/graphs.

## DATA INTERPRETATION AND ANALYSIS



Figure 1

Most of the organizations that took part in the survey was from the Technology industry (27%) which is quite good because of the nature of the survey.

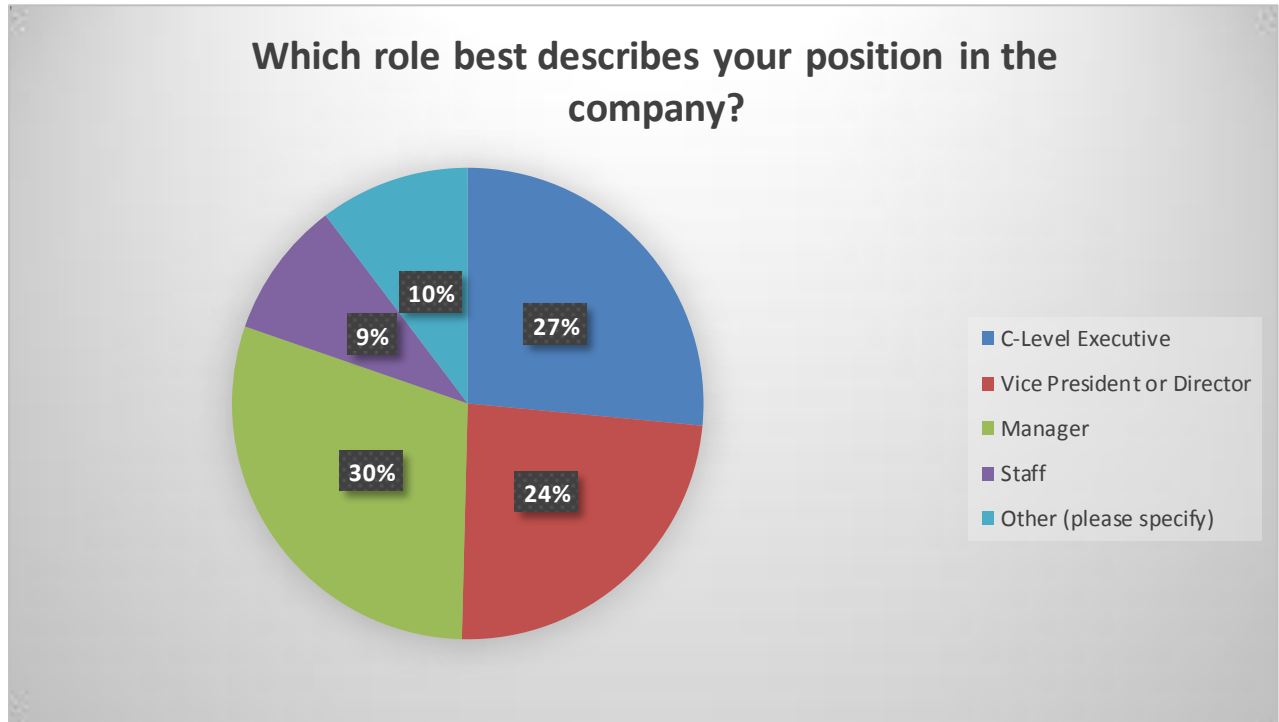


Figure 2

Most of the respondents who participated in the survey were of Managerial level or above, about 26% of them were C-Level Executives.

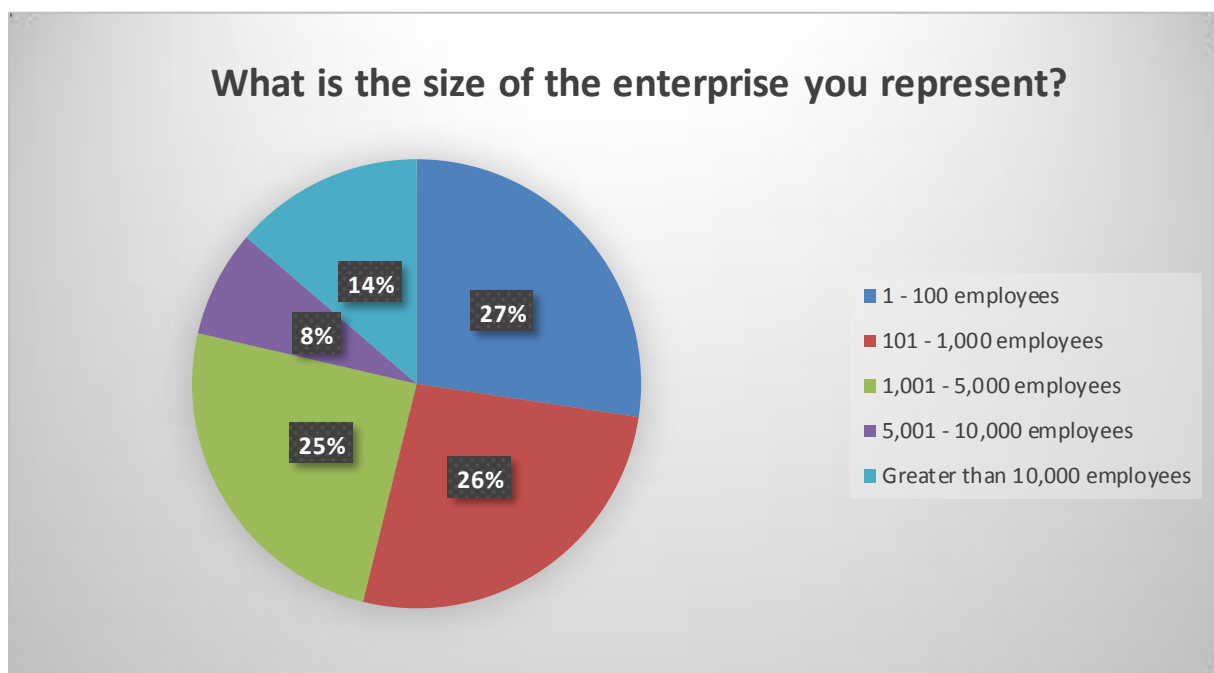


Figure 3

**The Indian Cloud Market is expected to grow more than 70% this year with Enterprise & SMB organizations adopting Cloud Offerings to leverage the efficiency that it provides. What is your organization’s Cloud Adoption Strategy in moving your applications and data to the Cloud?**

| Answer Options  | Response Percent |
|---|------------------|
| Active User: We already have some of our apps and data in the Cloud             | 62.6%            |
| Evaluation: We are in the phase of evaluating multiple vendors prior to a Trial | 26.1%            |
| No Plan: We have no plans of moving our apps and data to the Cloud              | 11.3%            |

Table 1

27% of the organizations have 1-100 employees out of which 53% are active users of cloud and 37% are evaluating multiple vendors prior to a trial

26% of the organizations have 101-1000 employees out of which 56% are active users of cloud and 37% are evaluating multiple vendors prior to a trial

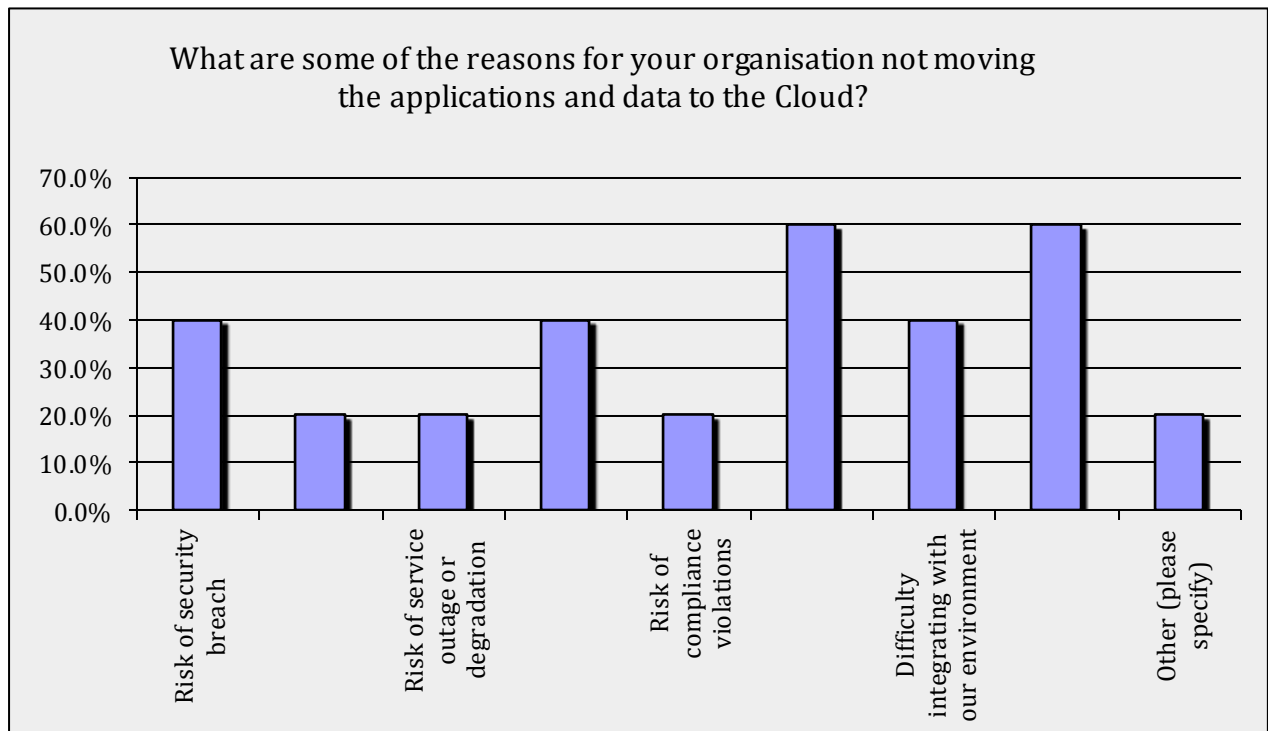


Figure 4

- Not cost-effective
- Lack of industry standards

These were the main reasons because of which organizations were reluctant to move the applications and data to the cloud.

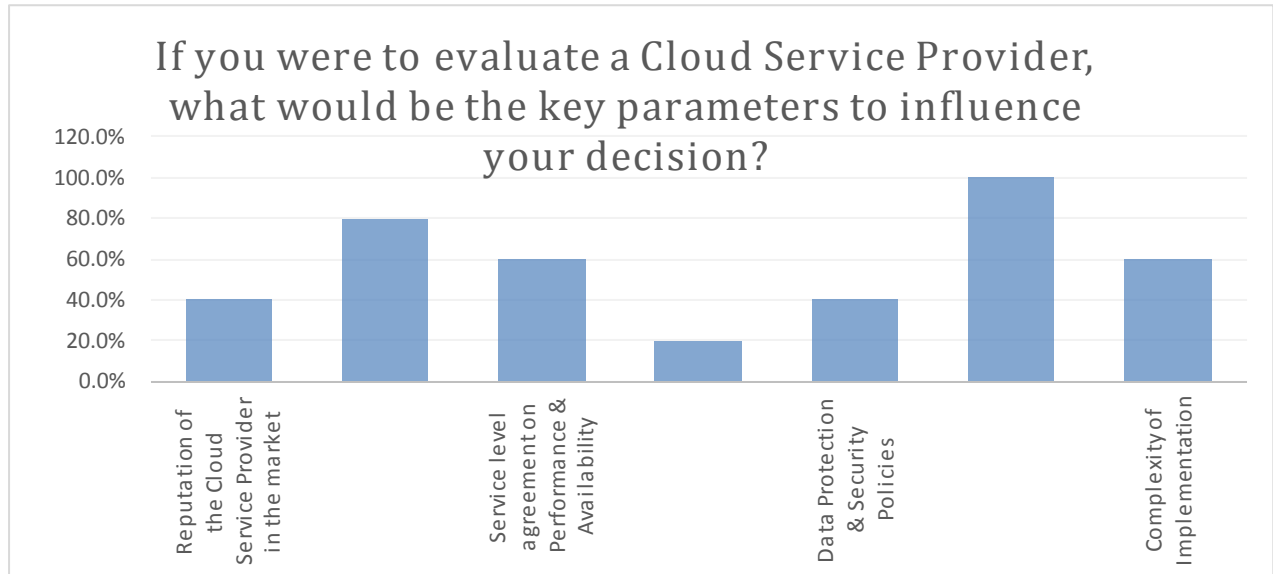


Figure 5

According to the survey results, organizations evaluate a Cloud Service Provider on the following top key parameters:

- Customer Support
- Cost/Billing options that they have to offer
- SLA on Performance and availability
- Complexity of Implementation

The results also showed that the least significant parameter is the presence of a local datacenter.

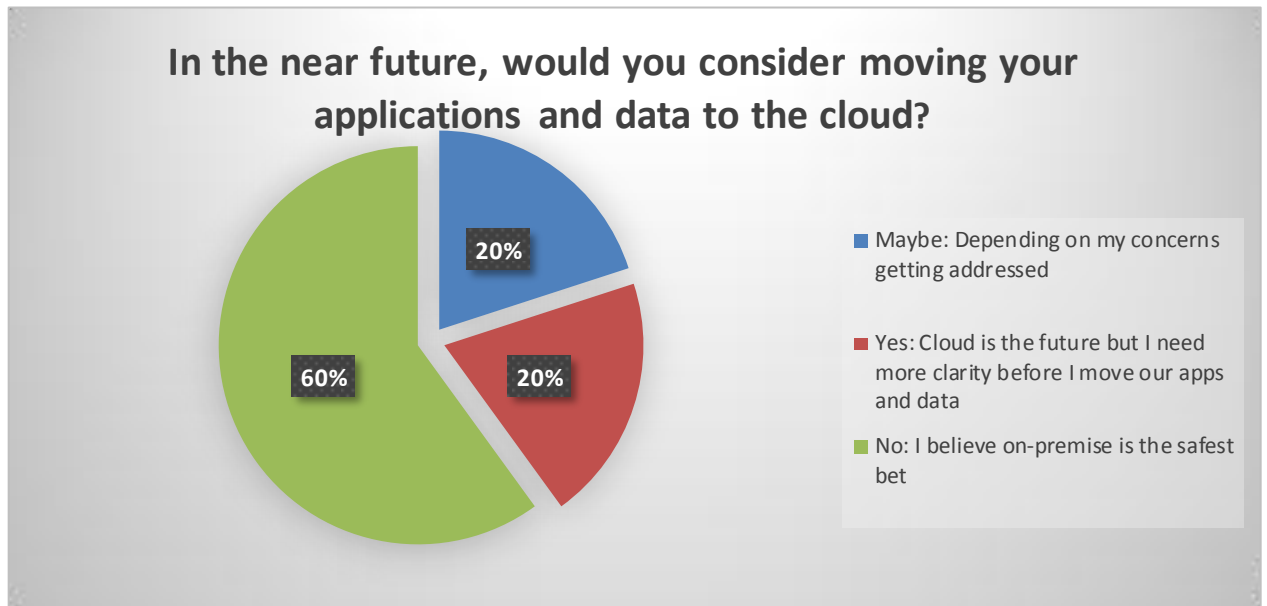
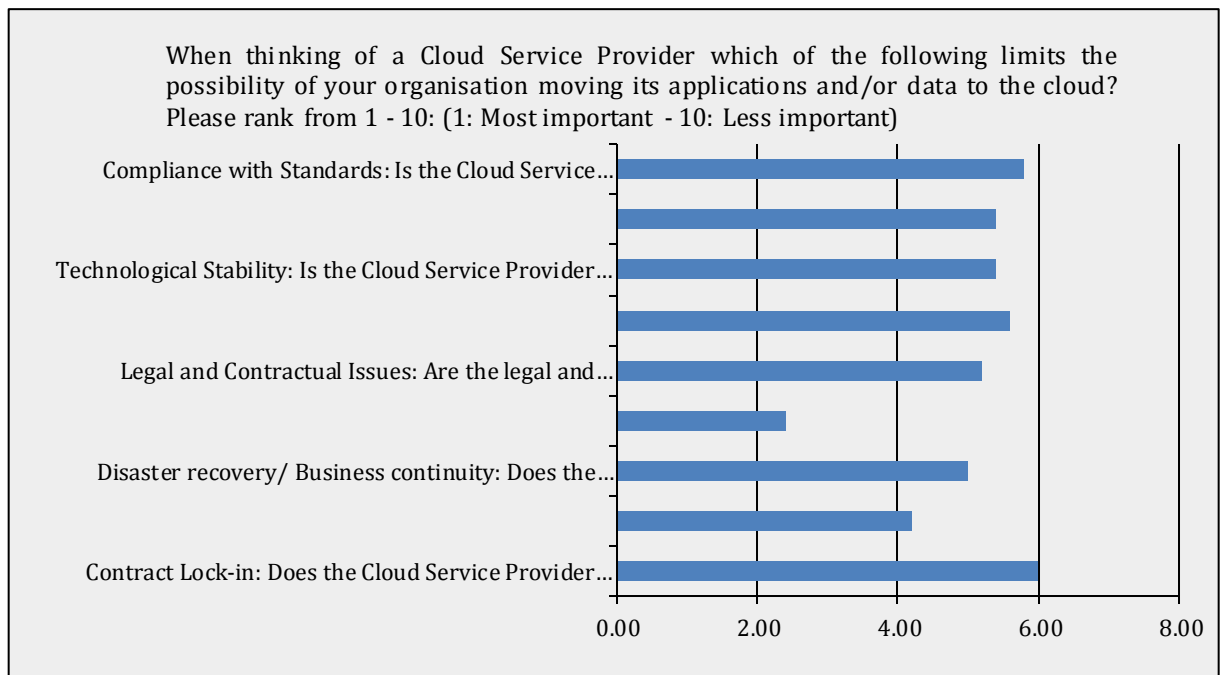


Figure 6

60% of the respondents said No to move their applications and data on cloud because of the primary reason of safety. They choose to opt on premise options over cloud. However, 20% organizations said yes to cloud being the future but are still not 100% convinced and need more clarity. This leaves great scope for cloud solution/security companies likes Instasafe to educate clients on cloud security.





**Figure 7**

The key reasons for limiting organizations to move its applications and/or data on cloud are found as the following (in order of importance):

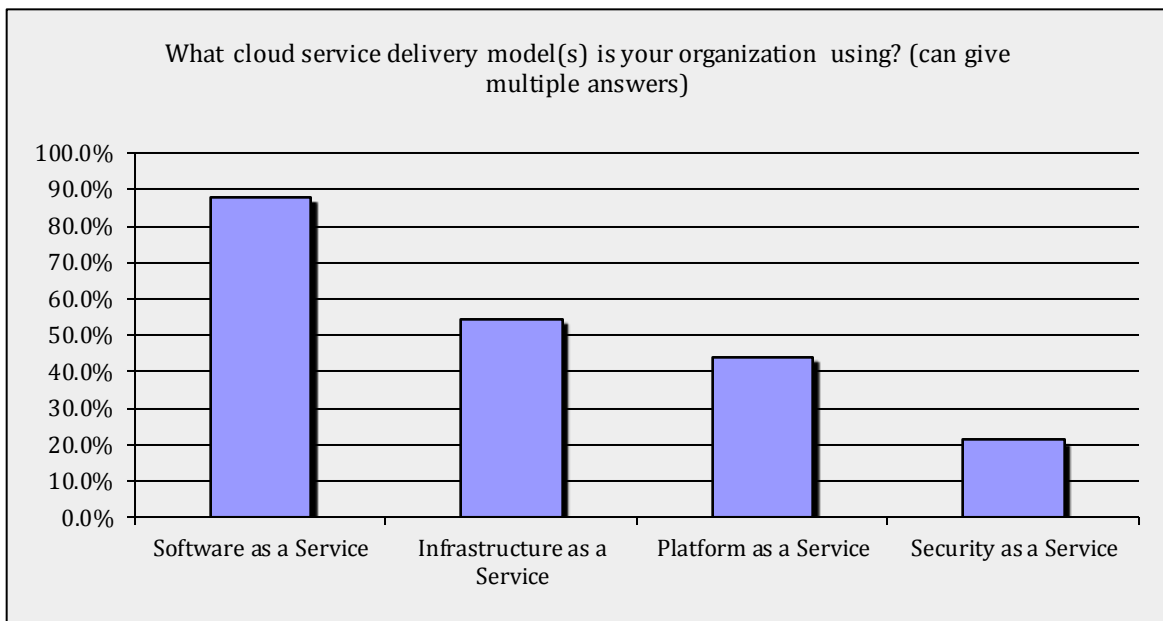
- Contract Lock-in
- Compliance with standards
- Geographical Issues

Surprisingly the least important reason ranked by the organizations was Information Security.

| What services and workloads is your organization hosting on the Cloud? (can give multiple answers) |                  |
|--|------------------|
| Answer Options   | Response Percent |
| Storage  | 63.2%            |
| Computing  | 47.4%            |
| Business Application   | 87.7%            |
| Networking   | 10.5%            |
| Virtualization   | 33.3%            |
| Other (please specify)   | 8.8%             |

**Table 2**

Only 7% of respondents have cloud hosted services in all of the above fields while majority of respondents have Business Applications and storage related services hosted on cloud (87% and 63% respectively).



**Figure 8**

As can be seen the cloud service delivery model that is most widely used across various organizations is Software as a Service model (SaaS) which is used by 87% of respondents. Next most used service delivery model is Infrastructure as a Service which is used by 54% of the organizations. Only 12% of organizations are involved in all of the above mentioned 4 service delivery models.

**Which cloud delivered security tools are currently deployed in your organization?**

| Answer Options   | Response Percent |
|--|------------------|
| Web security as a service: Ensuring users are compliant with the corporate web browsing policies and are being protected from accessing malicious websites                         | 56.1%            |
| Cloud Application Policy Control: Ensuring users have a safe and secure access to the applications that they need and are able to upload and download data from the cloud securely | 38.6%            |
| Identity and access management: Ensuring the right people get access to the right applications   | 52.6%            |
| VPN/Remote access: Secure access to cloud infrastructure (data-in-transit encryption) from any device over any network from any location.  | 54.4%            |

**Table 3**

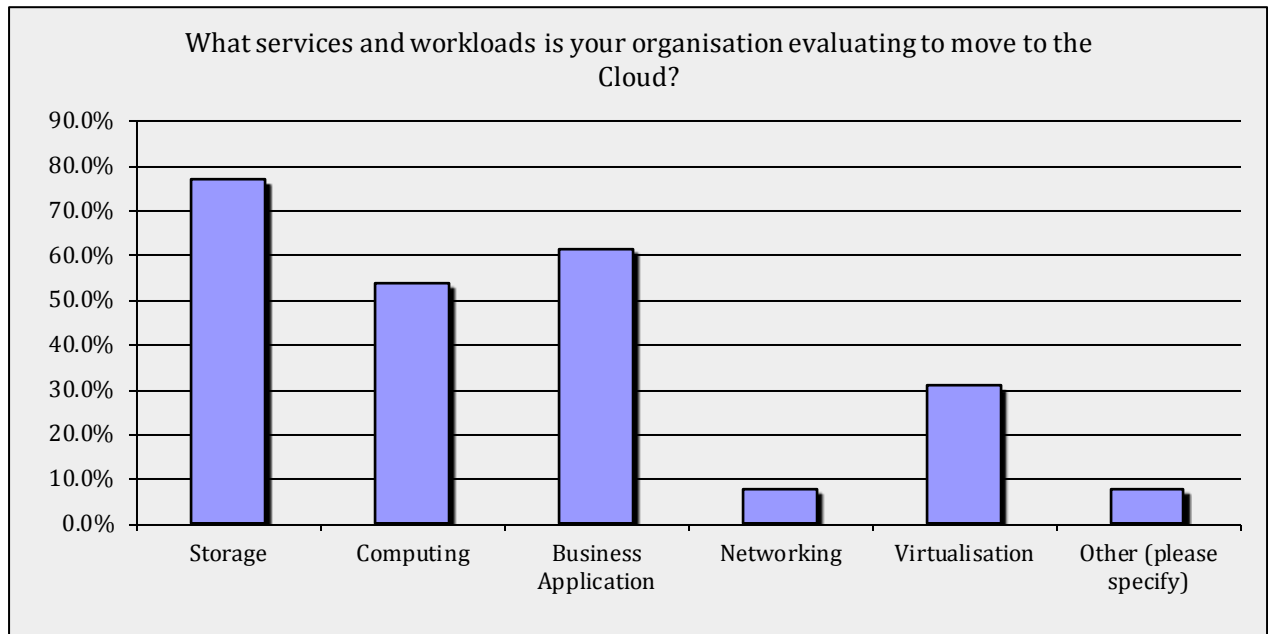


Figure 9

Even in the evaluating phase, the top most preferred service delivery model is related to storage services (77%). The next most service model is of Business Application with 61% organizations evaluating the same. Networking services are being evaluated the least for now.

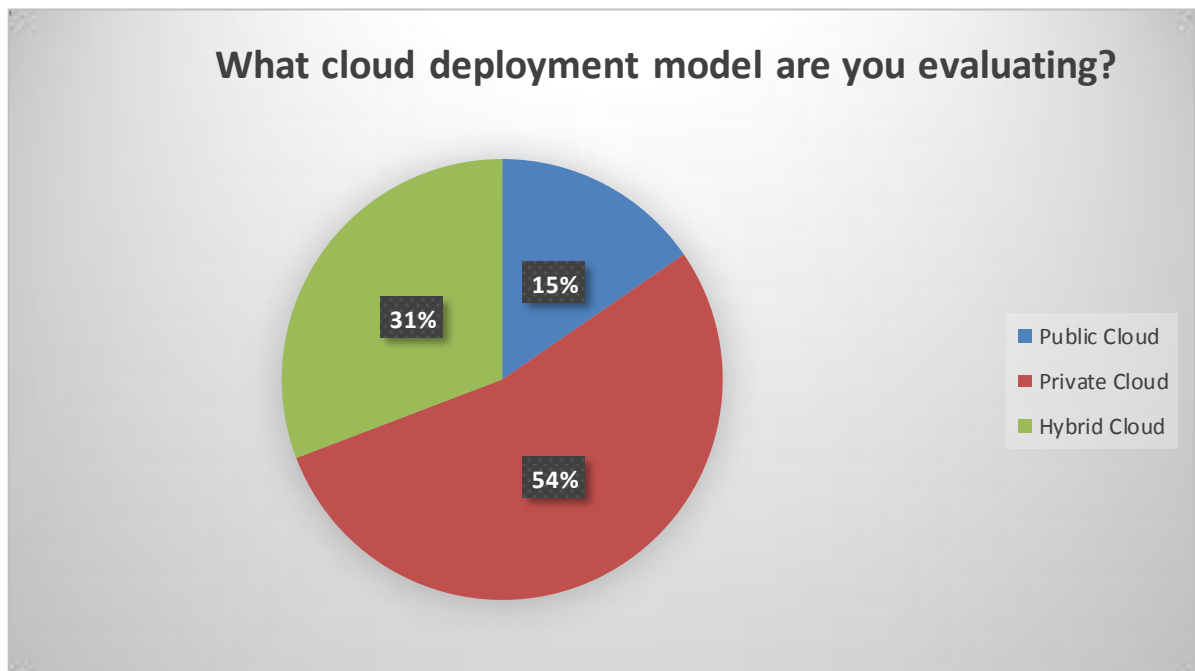


Figure 10

More than half the respondents (54%) are deploying their services on private cloud at present. 31% are on hybrid cloud whereas only 15% are on public cloud.

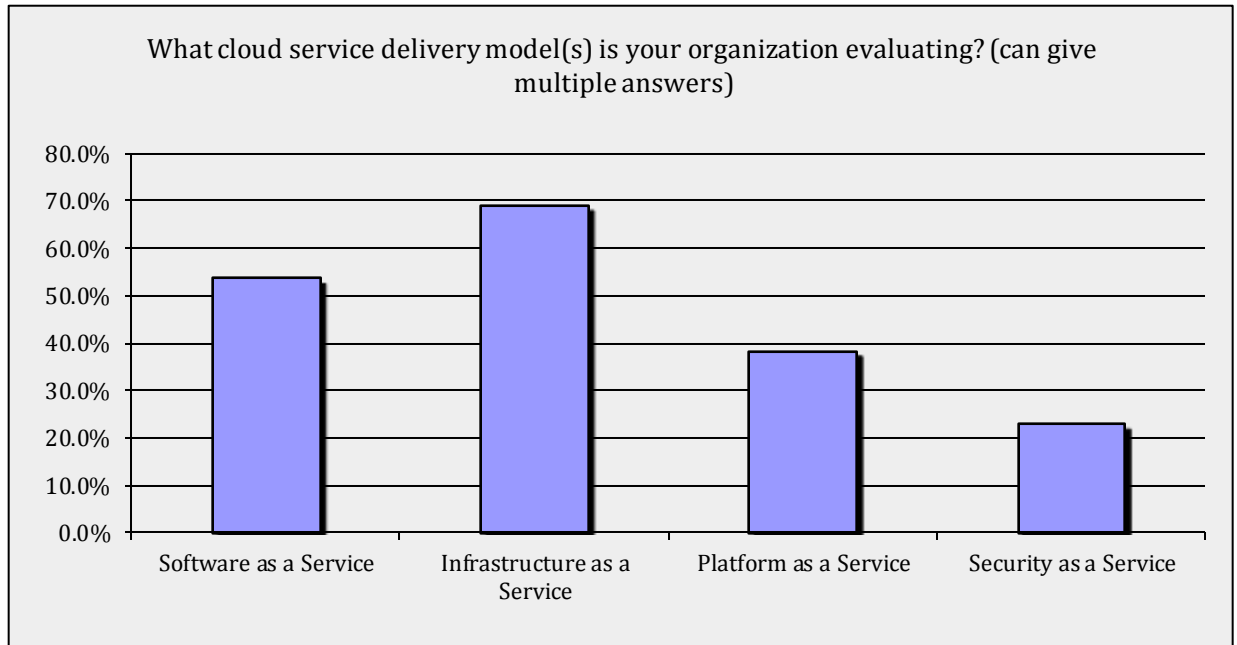


Figure 11

All the organizations who are using Private Cloud, about 87.5% of them are evaluating SaaS as their Cloud delivery model.

69% of the organizations are evaluating IaaS as their cloud service delivery model, only 23% are evaluating Security as a Service.

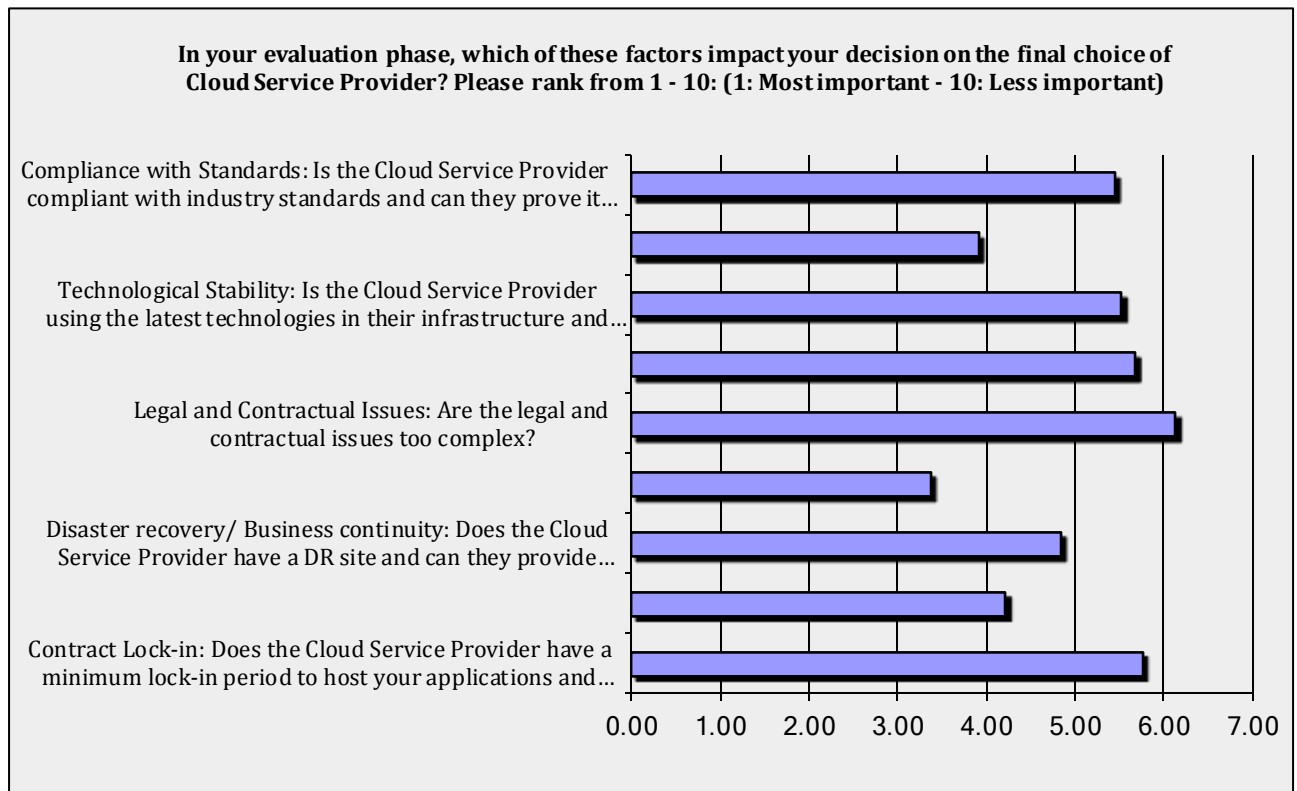


Figure 12

**What are your major concerns about policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing (Cloud security)?**

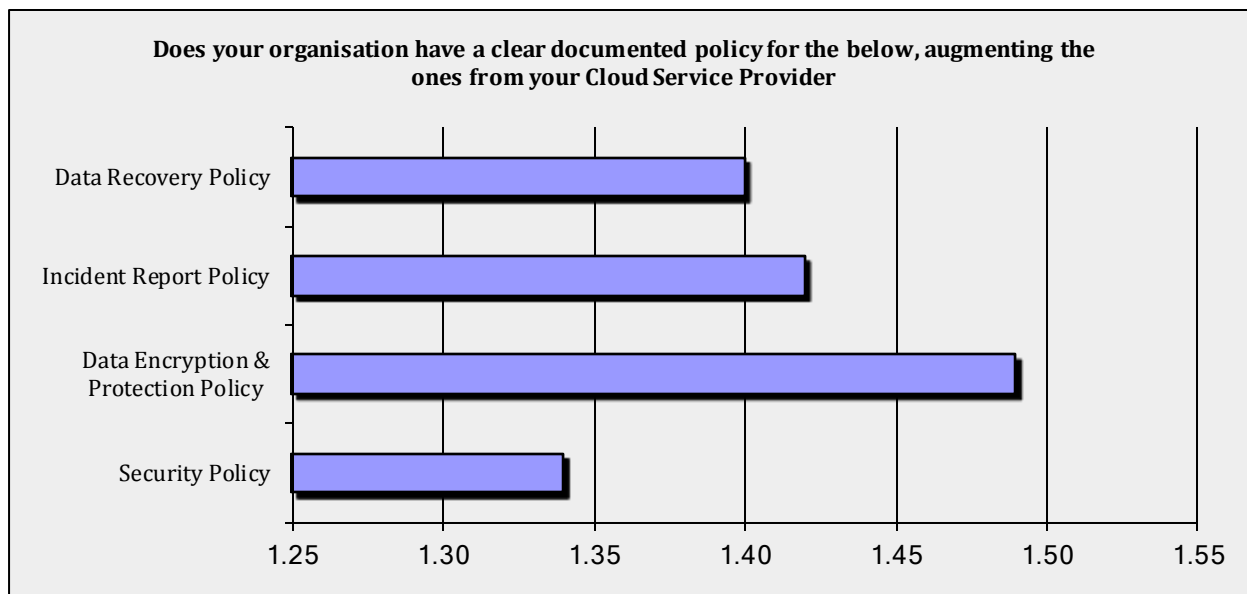
| Answer Options   | Response Percent |
|--|------------------|
| Data Breach: Data accessed by unauthorized personnel   | 77.5%            |
| Data-in-transit hacking: Data hacked and stolen while in transit from end point to the cloud (MITM Attacks)    | 43.7%            |
| Hijack of accounts: Accounts stolen through hacking  | 49.3%            |
| Insider Threat: Internal employee abusing cloud access to steal data and information                           | 57.7%            |
| Malware injection: Malicious code injected into cloud services compromising integrity of sensitive information | 52.1%            |

|  |       |
|--|-------|
| Denial of Service attacks: Make your servers and website unavailable to legitimate users                             | 46.5% |
| Insufficient due diligence: Lack of clear policies and procedures within the cloud service provider's infrastructure | 49.3% |
| Data Loss: Risk of losing data on the cloud due to factors like malicious attacks, natural disasters, data wipe etc  | 71.8% |

**Table 4**

Only 43% are concerned about MITM attacks, an assumption for this is probably because many of them are unaware of the potential threat.

77% are very much concerned about unauthorized personnel accessing their data



**Figure 13**

Most companies seem to understand the need for having proper data encryption & protection policy, and over half of the companies surveyed have a good understanding or have implemented data encryption.

Incident management is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. 70% of the organizations have established incident report policy in their organization.

77% of the organization have Security Policy established and running (rating average of 1.34)



Figure 14

75% of the organization conduct regular security audit and certification.

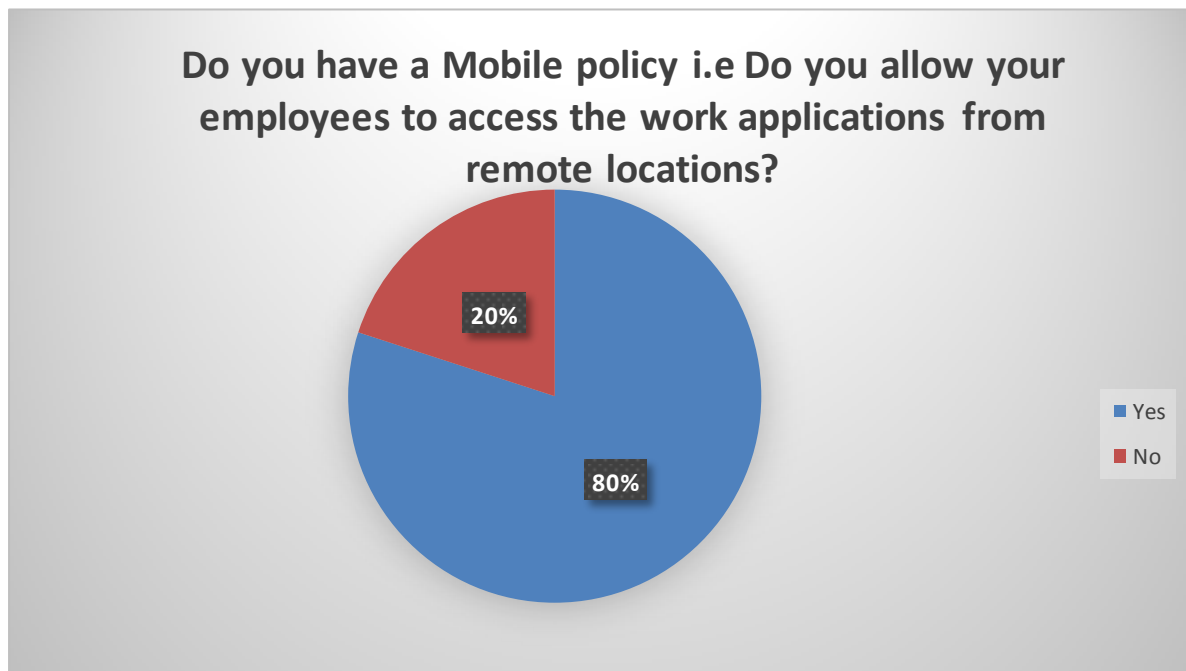


Figure 15

80% of the organization allow employees to work from remote locations. Out of these 10% of the organization have 76-90% of their workforce working from Remote locations or from Home.

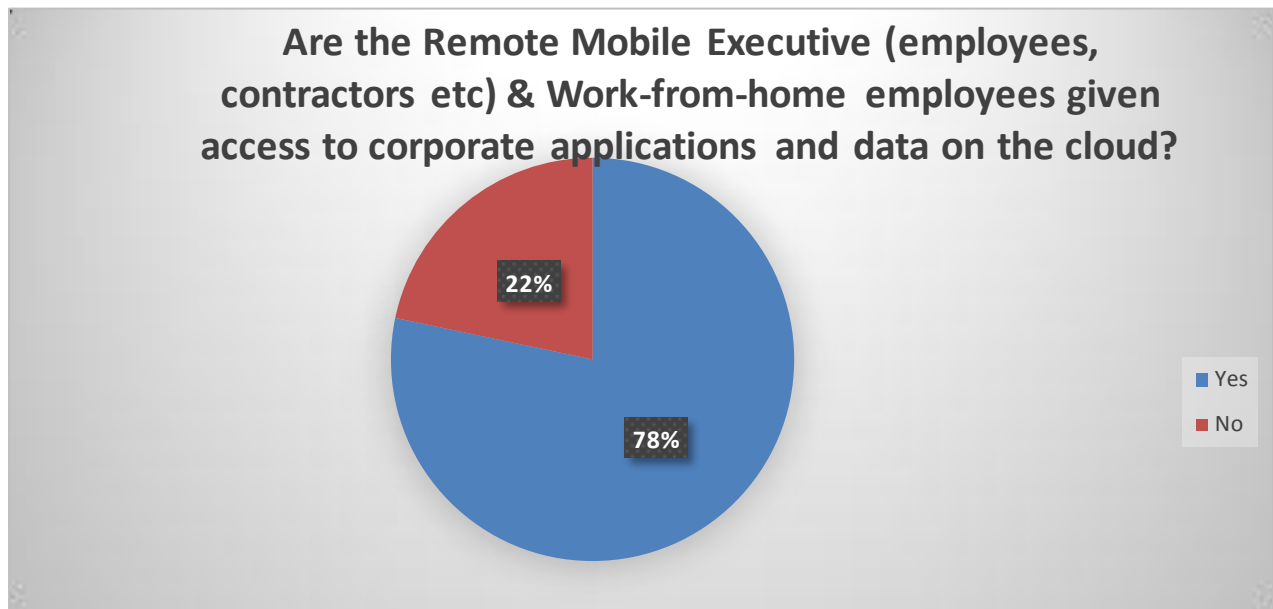


Figure 16

Only 6% of the organizations that have a BYOD policy do not give access to corporate applications and data on cloud to their Remote Mobile Executive (employees, contractors etc) & Work-from-home employees.

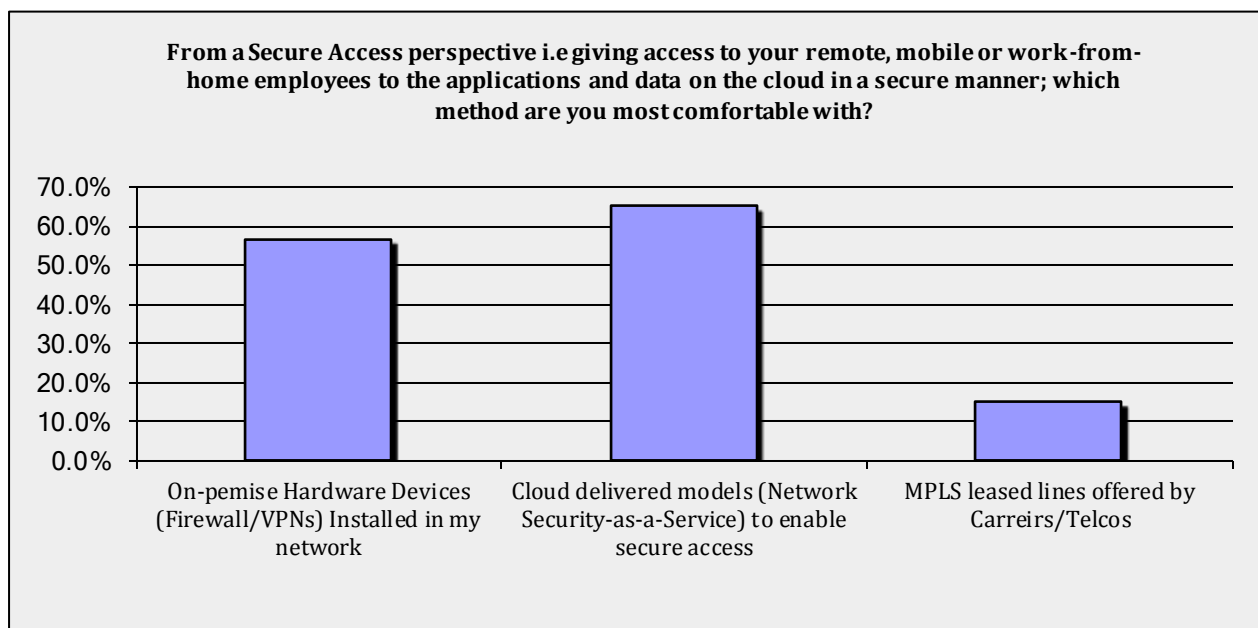


Figure 17



65% of the organizations are more comfortable using Cloud delivered models (Network Security as a Service) to enable secure access. This shows that security as a service is in demand and is being implemented by many organizations.

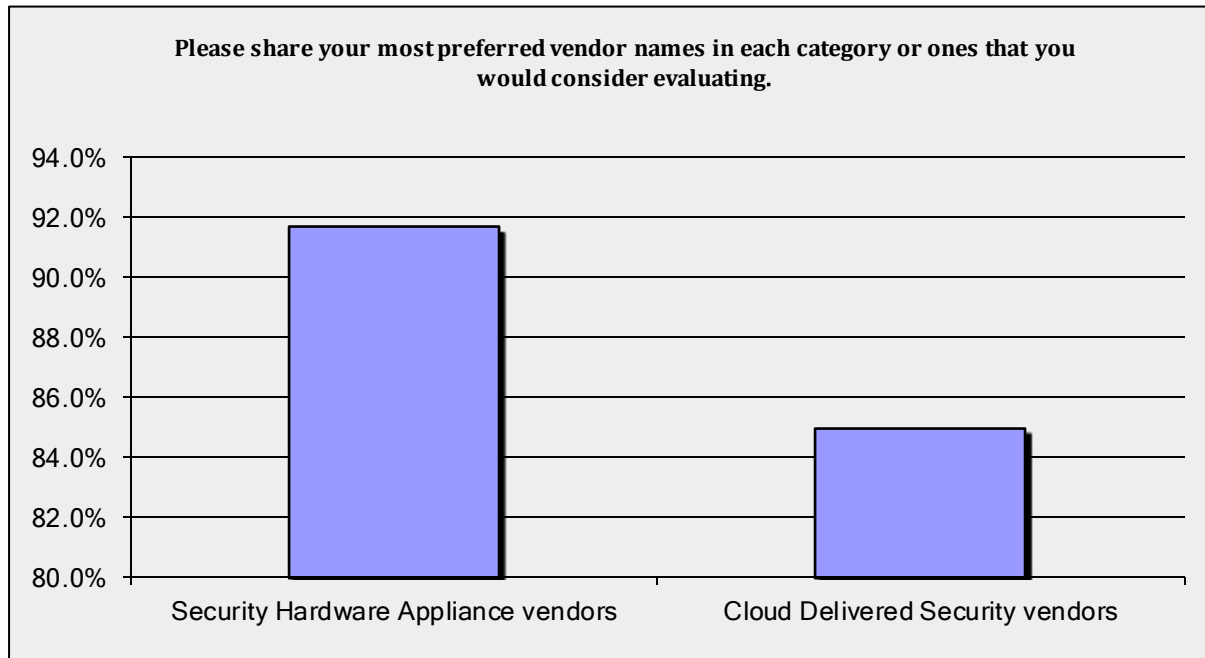


Figure 18

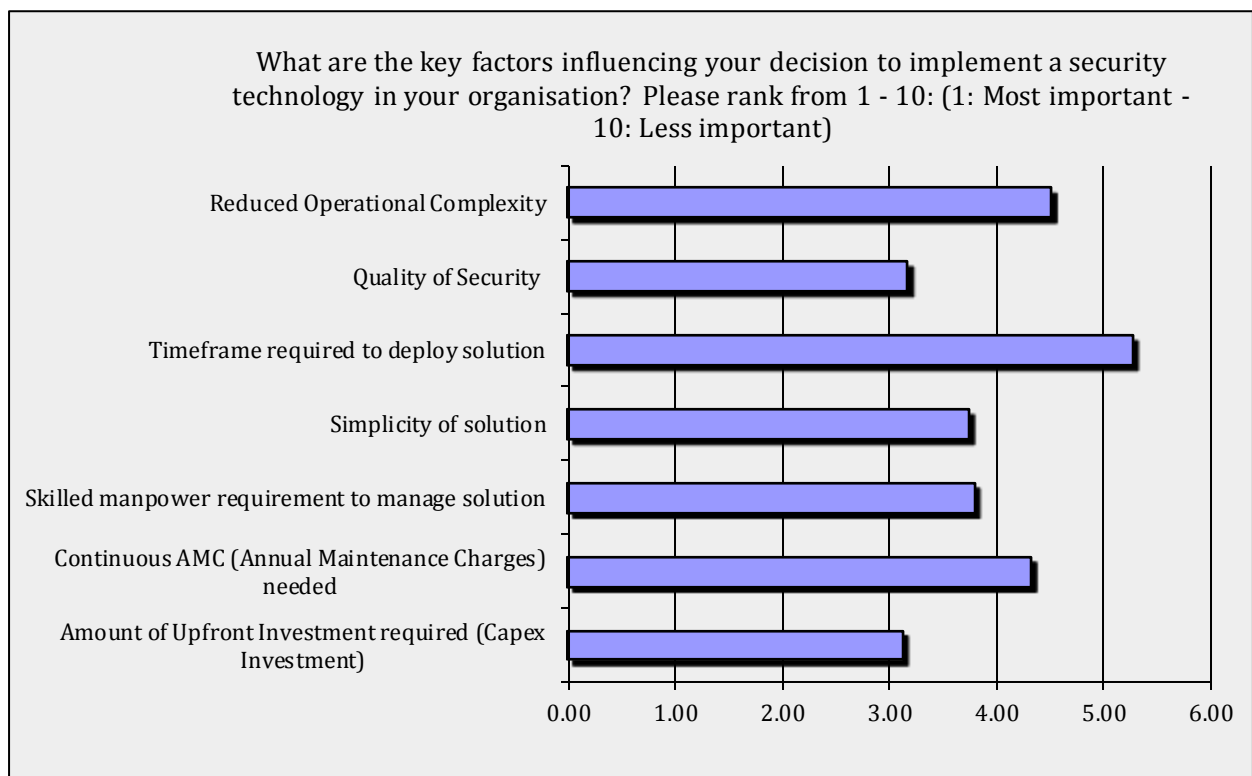


Figure 19

The key factor influencing an organizations decision to implement a security technology are

1. Time frame required to deploy solution
2. Reduced operational complexity

### **Discussion**

- Insatasafe has a good image in the current market hence they should recruit more employees on tech support also in the marketing team as the company is growing bigger and bigger.
- As the scope for Cloud based security is increasing and more SMBs are adopting cloud, more strategies should be focused on different types of marketing.
- More focus and campaigns should be built on the social campaigns to create a general awareness about the brand.
- Another major challenge for the company was the tech support needed at odd hours when the client required, hence the tech team to work in time shift basis as the team expands gradually.
- Software as a Service model (SaaS) which is used by 87% of respondents is good scope for Instasafe. Therefore, they should come up with more strategies to tap the potential business.

### **CONCLUSION**

- Instasafe has a good image in the current market which is quite evident form the existing customer base it has.
- 
- The scope for gaining more market share is much more than anticipated with large organizations still evaluating a plan to move towards cloud.
- There is an unparalleled need for a strong social campaign throughout the industry for more dominant position for Instasafe. They should be hiring more staff for the same with digital marketing scopes.

- Organizations evaluate a Cloud Service Provider primarily on Customer Support which the firm does well and is known for it.
- It is very clear that the Cloud service delivery model that is most widely used across various organizations is Software as a Service model (SaaS) which is used by 87% of respondents which is good scope for Instasafe.
- All the organizations who are using Private Cloud, about 87.5% of them are evaluating SaaS as their Cloud delivery model.
- 75% of the organization conduct regular security audit and certification

## REFERENCES

[www.insatsafe.com](http://www.insatsafe.com)

[www.leadssquared.com](http://www.leadssquared.com)

<https://cloudsecurityalliance.org>

<https://cloudsecurityalliance.org/group/top-threats/>

<http://www.crowdresearchpartners.com/wp-content/uploads/2016/05/Cloud-Security-Report-2016.pdf>