Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2011

An empirical study of challenges in managing the security in cloud computing

Bupesh Mansukhani
Charles Sturt University

Tanveer A. Zia
Charles Sturt University

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/124

AN EMPIRICAL STUDY OF CHALLENGES IN MANAGING THE SECURITY IN CLOUD COMPUTING

Bupesh Mansukhani1 and Tanveer A Zia[2]
School of Computing and Mathematics, Charles Sturt University, NSW, Australia
[1]bhupeshmansukhani@yahoo.com, [2]tzia@csu.edu.au

Abstract

Cloud computing is being heralded as an important trend in information technology throughout the world. Benefits for business and IT include reducing costs and increasing productivity. The downside is that many organizations are moving swiftly to the cloud without making sure that the information they put in the cloud is secure. The purpose of this paper is to learn from IT and IT security practitioners in the Indian Continent the current state of cloud computing security in their organizations and the most significant changes anticipated by respondents as computing resources migrate from on-premise to the cloud. As organizations grapple with how to create a secure cloud computing environment, we believe the findings from this study can provide guidance on how to address business and technology risks exacerbated by cloud computing. Specifically, in this paper cloud computing users evaluate security technologies and control practices they believe are best deployed either on-premise or in the cloud. Survey results are presented where we have asked cloud-computing users to rate the types of sensitive or confidential information too risky to be moved to the cloud. Alongside this paper also discusses the need of having SSL in the cloud to provide definitive way of securing the cloud.

Keywords
Security, Cloud Computing, Cloud Computing Security, VPN, SSL, Security in the cloud, Challenges, Cloud risks, Cloud Burst Security, Encryption, Authentication

INTRODUCTION

Cloud computing is a model for delivering information services that provides flexible use of servers, scalability and management services. In terms of its essential features cloud computing is a unique combination of capabilities which include:

- Scalable and dynamic infrastructure
- Global/Remote access
- Précised usage controls and pricing
- Standard Platform
- Support Services – IT and Management

The aforesaid capabilities enable a number of variations in cloud computing services, for instance one will provide database infrastructure services, and the other one will provide a fully functional CRM (Customer Relationship Management) model (Appistry, 2010). Since cloud computing is way of delivering services over a networked environment sometimes in virtual data-centres hence it involves a greater risk of security. In this paper we cover these aspects of security with respect to various technologies and risks that revolve around cloud computing.

SECURITY CHALLENGES IN CLOUD COMPUTING

Conventional infrastructure security controls designed for dedicated hardware do not always map well to the cloud environment. Cloud architectures must have well-defined security policies and procedures in place. Realizing full interoperability with existing dedicated security controls is unlikely; there has to be some degree of compatibility between the newer security protections specifically designed for cloud environments and traditional security controls.

Integrated Cloud Security

Traditional environments segment physical servers with Virtual Local Area Networks (VLANs). Cloud environments should take the same approach and segment virtual machines by VLANs through Port Group configurations. Since these are physical servers, traffic flows are visible to traditional network-based security protection devices, such as network-based intrusion prevention systems (IPSs). The concern in cloud environments is that IPS's provide limited visibility to inter-virtual machine traffic flows (Rittinghouse, 2009).

Cloud Burst Security

One of the primary advantages of cloud computing is that enterprises can move applications that consist of several virtual machines to the cloud provider when the physical environment requires additional processor or compute resources. These bursting virtual machines need security policies and baseline histories to move with them. When a virtual machines moves, if the security policy does not accompany it, those virtual machines become vulnerable (Binning, 2009).

Defense In-Depth

Strategies for ensuring perimeter security have evolved significantly over the last few years. Today, most enterprises have deployed layered defense strategies, but server virtualization can complicate matters. In an attempt to consolidate servers, many organizations have left themselves vulnerable to the inter-virtual machine communications that exist, because if one virtual machine is compromised (Brown, 2011), then all the other virtual machines that are part of the virtual network can be compromised without anyone detecting it (Schultz, 2011).

SSL CERTIFICATES - KEY TO SECURE CLOUD COMPUTING

SSL is a security protocol used by web browsers and web servers to help users protect their data during transfer. SSL is the standard for establishing trusted exchanges of information over the Internet. Without the ubiquity of SSL, any trust over the Internet simply would not be possible. SSL comes into play anytime data changes location. If an enterprise keeps its data in the cloud, secure network access to it is important. Furthermore, that data is likely to move around between servers in the cloud when the service provider performs routine management functions (Forouzan, 2009). In the following section various methods by which SSL can secure cloud computing are highlighted.

HOW SSL CAN SAFEGUARD THE CLOUD

Segregating Data And Securing Access To Cloud Services

Data segregation risks are ever-present in cloud storage. With traditional onsite storage, the business owner controls both exactly where the data is located and exactly who can access it. In a cloud environment, that scenario is fundamentally changed: the cloud service provider controls where the servers and the data are located. However, a proper implementation of SSL can secure sensitive data as it is being transmitted from place to place in the cloud, and between cloud provider servers and end users on browsers.

- Encryption

  Businesses should require their cloud provider to use a combination of SSL and servers that support, at minimum, 128-bit session encryption (or, preferably, the stronger 256-bit encryption) (Forouzan, 2009). This way their data is secured with industry-standard levels of encryption or better as it moves between servers or between server and browser, preventing unauthorized interception of their data from being able to read it.

- Authentication

  Businesses also should demand that server ownership be authenticated before even one bit of data transfers between servers. Self-signed SSL certificates provide no authentication. Only independent, third party SSL certificates (Verisign, 2009) can legitimately deliver ownership authentication. Requiring a commercially issued SSL certificate from a third-party certificate authority that has authenticated the server makes it virtually impossible to establish a rogue server that can infiltrate the cloud provider's environment.

- Certificate Validity

  Once a server and domain are authenticated, the SSL certificate issued to that device will be valid for a defined length of time. In the rare case that an SSL certificate has been compromised in some way, there is a fail-safe check to verify that the certificate has not been revoked in the time since it was originally issued.

  Every time an SSL session handshake is initiated, the SSL certificate is checked against a current database of revoked certificates. There are currently two standards used for this validity check, Online Certificates Status Protocol (OCSP) and Certificate Revocation List (CRL) (Forouzan, 2009). With OCSP a query is

sent to the certificate authority asking if this certificate has been revoked; the certificate authority answers yes or no. If the answer is no, the handshake may commence.

Monitoring Data Provenance

SSL addresses the third area of risk, data location, in the same manner. Public clouds are like black boxes: while they enable ubiquitous access to data, they also obfuscate the physical location of the servers and the data. But if a cloud provider uses SSL to encrypt data as it changes places, an enterprise can be assured that its data will be secured as it moves around the cloud (Community, 2011).

Using SSL Certificates To Establish Trust In The Cloud

Using a cloud service provider requires a high level of trust and confidence. Business critical applications cannot rely on trial and error. Businesses must insist for critical reliability equation to establish trust, and SSL certificates provide a highly visible and immediately recognizable way to accomplish that. Alternately, missing or broken SSL can destroy trust instantly. For example: suppose an enterprise chooses a cloud provider to host their e-commerce web site, but the host has a problem with the site's SSL certificate (Owens, 2010).

Cloud providers should be using SSL from an established, reliable and secure independent certificate authority. Its SSL should deliver at minimum 128- bit session encryption and optimally 256-bit encryption (Owens, 2010). And it should require a rigorous authentication process. Additionally, some providers may use servers with Debian-based operating systems to generate their SSL keys. SSL certificates can be issued for validity lengths of up to six years, so it is possible that SSL with this flaw is still being used (Beaver, 2009).

Conclusion On SSL Certificates

When selecting a cloud service provider, enterprises must also be very clear with their cloud partners regarding handling and mitigation of risk factors not addressable by SSL. Enterprises should consider the seven categories suggested by Gartner (Brodkin, 2008) when evaluating (and contracting with) cloud-computing solutions. Cloud providers should be using SSL from an established, reliable and secure independent certificate authority. Its SSL should deliver at minimum 128-bit encryption and optimally 256-bit encryption based on the new 2048-bit global root. And it should require a rigorous authentication process. The SSL issuing authority should maintain military-grade data centers and disaster recovery sites optimized for data protection and availability.

THE SURVEY - ANALYSIS AND DISCUSSIONS ON CLOUD SECURITY

Methodology

Applied research was used to conduct the survey and targeted the following personnel in selected IT organizations in India, we surveyed over 167 people from different IT ogranisations within India that are running, deploying or using cloud computing as part of their migration programs.

The survey was two page long asking them questions on usage of cloud computing, technologies that can safeguard cloud computing and others (as shown in Findings). Most of the survey questions were based on a likert scale ranging from "Strongly agree" to "Strongly disagree" and some of them were "Yes" or "No" option based.

A total of 167 completed surveys were returned out of which 166 were usable for this paper leaving one as incorrectly filled by the respondent. The following groups were selected for answering our survey, their percentage breakup has been shown on Figure 1.0

- Senior Management (CTO/CIO's)
    - Chief Information Officer
    - Chief Information Security Officer
    - Chief Technology Officer
- Middle Management/Executives
    - Network Engineers
    - Security Risk Auditors
    - Security Operations Engineer

The survey was conducted over the phone and in some cases through in-person scheduled interviews and was completed in August 2011.

Demographics

As part of the survey 167 people were interviewed from the chosen 40 organizations, resulting in an average of 4 - 5 personnel per organization. Almost 50% of the people interviewed were IT security practitioners such as chief information security officers, security risk auditors, IT security consultants and IT security managers, 20% were network engineers and the rest 30% were from other senior management or decision making positions (Figure 1.0).

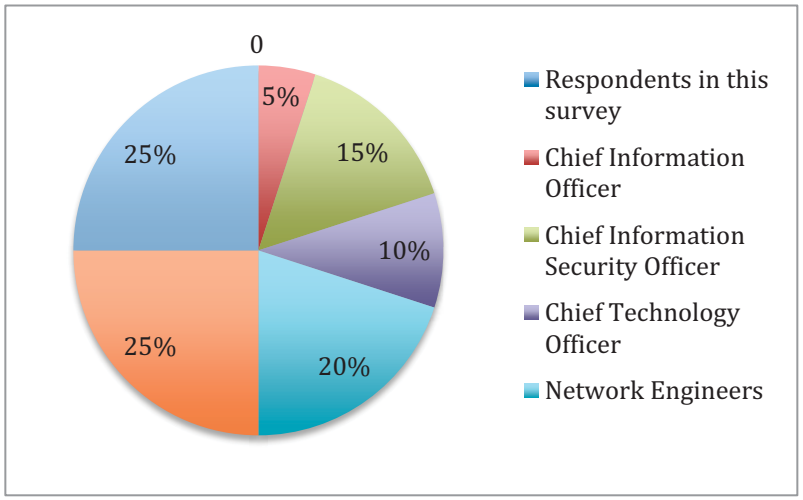

Figure 1.0 Survey Respondents

Key Findings

This section provides most important findings about this survey; all the representations are in graphical (chart) format along with a study discussion. The findings from this study were collected in several stages.

Stage 1: Attributions about cloud computing security (Please note respondents were given 5 point range scale ranging from "Strongly Agree" to "Strongly Disagree" for each statement.)

Figure 1.1 provides a graphical representation of the views for security practitioners, network consultants and senior management. Results clearly show respondents in senior management hold more favorable perceptions about the state of cloud computing security than IT security practioners and network consultants. However IT security practitioners show a concern on various areas of the survey especially with respect to security of the cloud. From Figure 1.1 it is evident that security practitioners believe their organizations' senior management are not engaged in the security aspect of the cloud computing, whereas the response of the senior management says otherwise. In personal view the security practitioners are to be believed since they are the ones working on cloud computing and its security for long.

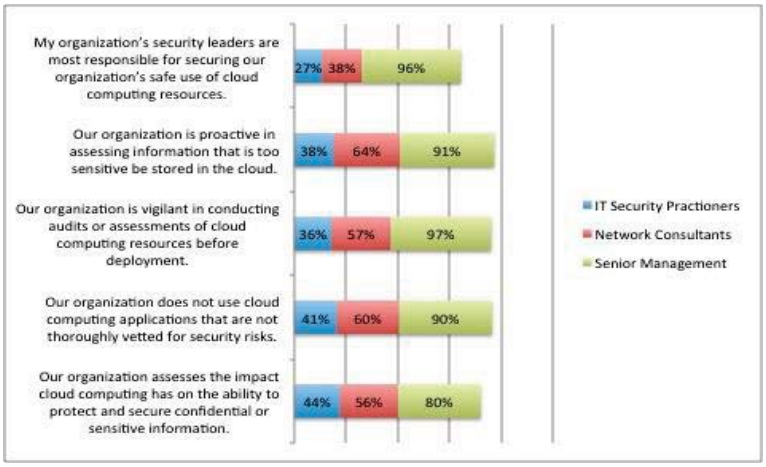

Figure 1.1: Attributions of Cloud Computing Security

Stage 2: Critical Business Applications/Services on the cloud (Please note respondents were given three options to select from "PaaS", "SaaS", "IaaS" for this statement)

In Figure 1.2 it is seen that most of the companies and employees are engaged in using cloud computing for critical business applications. As per the survey it was evident that organizations are mainly using SaaS (Software as a service) platform on the cloud to host critical business applications, followed by IaaS (Infrastructure as a service) for hosting infrastructure services on the cloud. It is also seen that most of the organizations are using SaaS or IaaS to hosts their intellectual or running their business critical applications. Hence security on the cloud plays a major concern since most of the organizations are engaged in using cloud for hosting either applications or their infrastructure, compromising security over the cloud will effect these two platforms directly and severely.

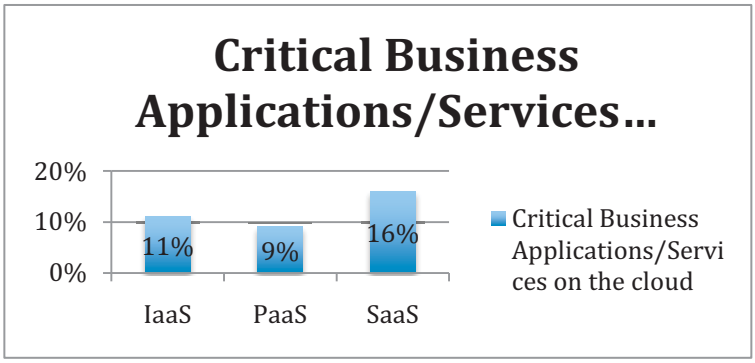

Figure 1.2: Critical business applications/services that run on the cloud

Stage 3: Cloud computing providers are responsible for ensuring security (Please note respondents were given with an option of "Yes" or "No" for this question)

As per Figure 1.3 most respondents believe that cloud computing providers are responsible for ensuring security on the cloud, over 42% of the respondents believe that service providers (in this case cloud computing providers) are responsible for securing SaaS platforms and 34% of them feel that service providers are responsible for securing the IaaS platform. However the results derived from this finding is Organizations are trying to hand over the responsibility of cloud computing security to the service provider irrespective of the platforms. Indeed the service providers are responsible for managing security in the cloud since they are the only ones who are providing us with cloud computing services.

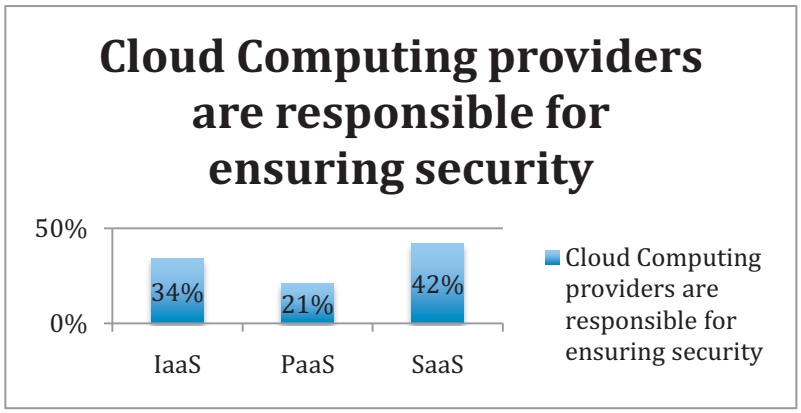

Figure 1.3: Service providers responsible for ensuring cloud safety

Stage 4: Are cloud computing resources evaluated prior deployment? (Please note respondents were given with an option of "Yes" or "No" for each of the statement)

As per Figure 1.4 most of the respondents believe that cloud computing resources are not evaluated for security prior to deployment, mostly security practitioners and network consultants feel that security is not evaluated before deployment over the cloud followed by management in 44% of ratio. Most respondents showed their

discontent within their answers, disapproving of the fact that organizations are not paying any attentions to evaluate computing resources before moving or deploying to the cloud. This negative reaction of the respondents came especially from the middle management; it is therefore a matter of concern for the organizations' decision makers to evaluate computing resources before moving to the cloud.

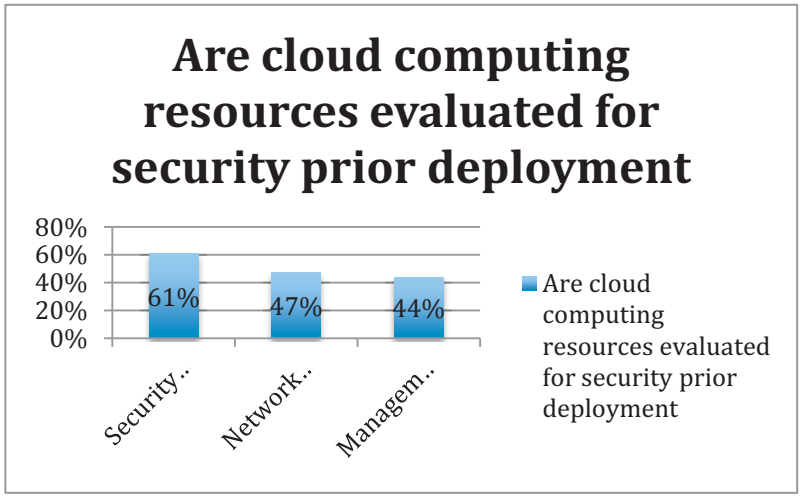

Figure 1.4: Evaluation of cloud computing resources prior deployment

Stage 5: How confident are you about the usage of all cloud computing resources? (Please note respondents were given with an option of "Likely", "Very Likely" and "Not likely" for each of the statement)

Figure 1.5 depicts that most of the security resources are still under the radar from the respondents' views and knowledge. Especially the management is hardly aware of the new or existing security resources that can be used within the cloud with respect to cloud security such as VPN and virtual networks or private clouds. The security practitioners are still aware of the aforesaid technologies and other security resources of cloud computing, however the numbers still depict that more knowledge is needed by the respondents on the application of security resources of cloud computing.

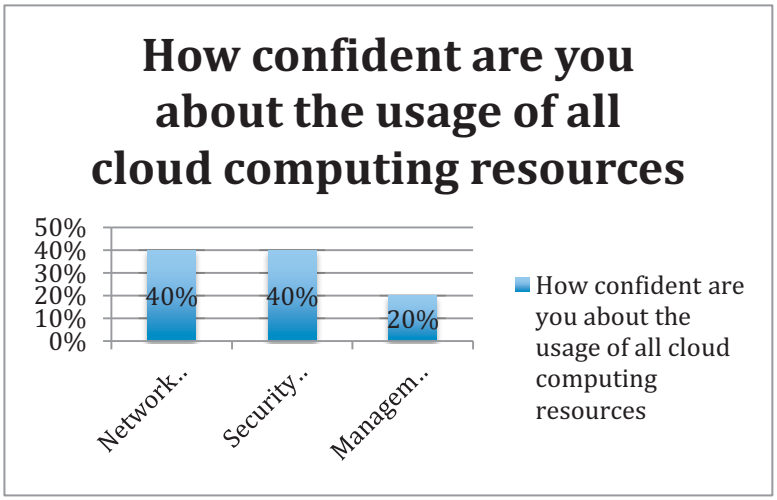

Figure 1.5: Usage of cloud computing

Stage 6: Security features with respect to on-premise or in-the cloud? (Please note respondents were given 5-point range scale ranging from "Strongly Agree" to "Strongly Disagree" for each statement.)

Figure 1.6 illustrates various security countermeasures that can be applied within the organizations to safeguard

cloud computing and the data over the cloud. The major chunk of "on-premise" methods includes "Limiting physical access to Data Centers/IT Infrastructure" with over 84% of agreement, followed by "Conducting Security Audits" with over 70% agreement. However with respect to security countermeasures "In-Cloud" almost 67% of the respondents are in agreement with "Tighten Security Policies" at the service provider end, followed by 55% for "Conducting Security Audits" at the service provider end, in the end major portion agrees to "Limiting access to the Data Center/IT infrastructure" for safeguarding the cloud data.

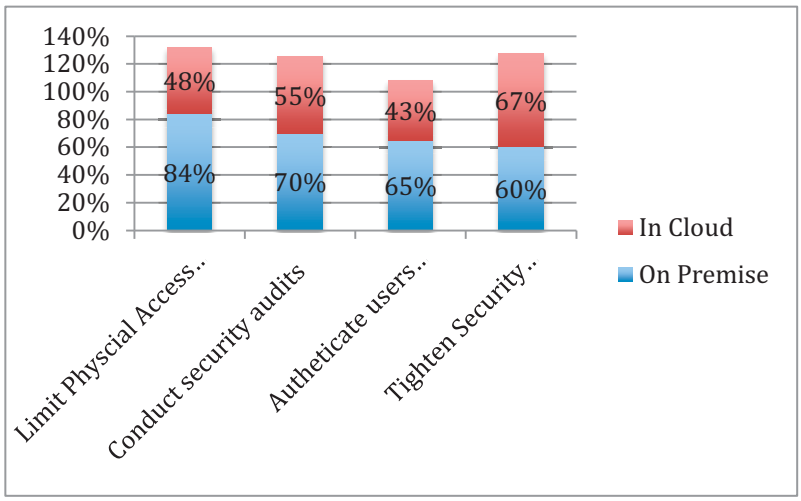

Figure 1.6: Security Measures on Cloud Computing

Stage 7: Technologies that can safeguard cloud computing? (Please note respondents were given 5-point range scale ranging from "Strongly Agree" to "Strongly Disagree" for each statement.)

In this stage various technologies were listed out to the respondents and their individual responses were recorded on each of the technology to illustrate a combined response. Almost 70% of the respondents feel SSL certifications and Network Intelligence are best bet for safeguarding cloud computing, followed by VPN and Log Management (63% and 64% respectively) at the second place. This paper also emphasizes SSL certification as a first choice of safeguarding cloud computing and same view is shared by the respondents in this survey.

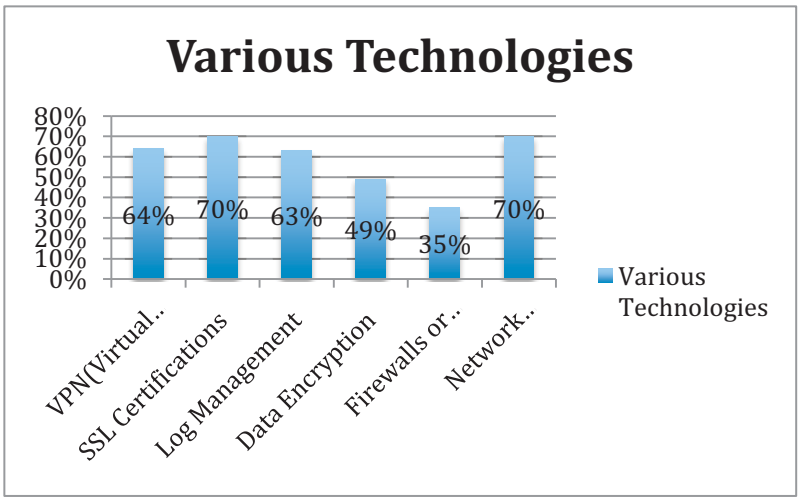

Figure 1.7: Various technologies to safeguard cloud

Stage 8: Identified risks of cloud computing by respondents. (Please note respondents were given 5-point range scale ranging from "Strongly Agree" to "Strongly Disagree" for each statement.)

In Figure 1.8, the risks were divided in two sections "On-Premise" and "In the cloud", most of the respondents benchmarked "illegal activity" as primary risk to cloud computing, needless to say "illegal activity" refers to hacking, breaking or stealing or all of them with respect to the context of this survey. Followed by security of data assets at second place, this involved the security of data assets at the data centers or IT infrastructure security. As the answers clearly represent the current risks to focus on cloud computing are "Security of Data

Assets" and "Illegal Activities" as these are the only risks that are high "On-Premise" and "In-the-Cloud". Hence organizations and Service providers should focus on these two security risks of cloud computing.

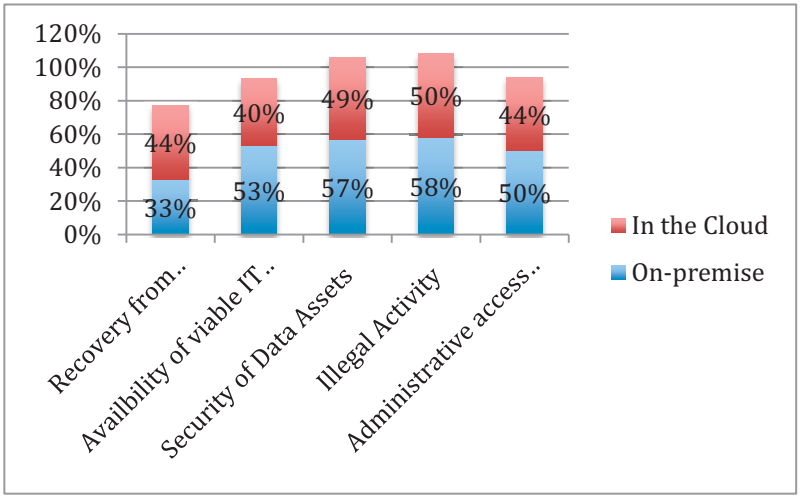

Figure 1.8: Identified risks of cloud computing

Stage 9: Type of Information that can be risky over the cloud. (Please note respondents were given 5-point range scale ranging from "Strongly Agree" to "Strongly Disagree" for each statement.)

In Figure 1.9 respondents marked out various information categories that can be risky if kept in the cloud, almost 70% people responded with risk of putting intellectual property over the cloud, followed by financial data at 62% and other categories of data were at an average of 40 – 55%, which included credit card information, non-commercial information and employee data. It is evident from the response of the surveyors that "Intellectual Property" followed by "Financial Data" are the two of the major categories of information that are at high risks in the cloud computing space.

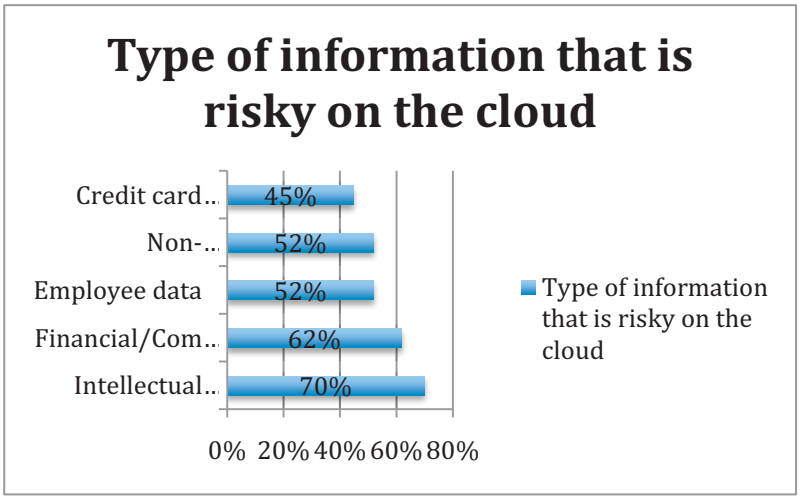

Figure 1.9: Information that can be risky on the cloud

CAVEATS

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 phone-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We asked 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.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

SURVEY SUMMARY

Following is a summary of some salient findings from this survey.

- IT practitioners (respondents) lack confidence in their organizations' ability to secure data and applications deployed in cloud computing environments (especially public clouds).
- IT practitioners hold views on the reasons for using cloud computing resources as well as a plethora of security issues caused by rapid migration from on-premise to cloud computing environments.
- IT practitioners believe the security risks most difficult to curtail in the cloud computing environment include securing the physical location of data assets and restricting privileged user access to sensitive data.
- IT practitioners believe critical areas of focus as their organizations migrate from on-premise to cloud computing environments concern access governance, identity and access management, business continuity and disaster recovery planning.

CONCLUSION

The findings of this study suggest that users of cloud computing may be putting their organizations' information and interests at stake as a consequence of inadequate security knowledge present at the higher management level. As noted in the paper cloud computing security decisions are left on higher management (being the decision makers) who may not have adequate knowledge on the deployment of cloud computing or expertise to properly evaluate the security parameters of cloud and its arena.

Indeed the benefits of cloud computing are many as compared to the traditional computing but the cost of implementation of various technologies to safeguard the cloud play a vital role in selecting the right service provider.

As the result of this study, we conclude that the usage of cloud computing should be first mitigated with the following:

- Asset and inventory management of new or existing assets are imperative before moving to cloud, organizations should spend time in assessing the security risk involved in moving the assets to cloud, as this study will help whether to choose cloud computing or not;
- Data that will be moved to the cloud should be assessed with respect to security risk matrix; doing so would help the organizations in choosing the right security and service provider for the organization;
- Security policies and procedures should be drafted out in accordance with the security practitioners to enable the organizations to select the right service provider for various cloud computing solutions.

In conclusion, cloud computing does provide us with tangible benefits but today we still have no definite answers on a proper security platform for cloud computing, only suggestions and theories are being formed but we are yet to see a practical security measure for cloud computing to be a safer platform for organizations and individuals. The paper suggests the use of SSL to secure Cloud computing however this technology is still under the radar for practical usage and may serve as a security checkpoint for cloud computing security issues as of this moment, but cannot be used a sole tool to safeguard cloud computing, as the time progresses different technologies shall be discovered to safeguard cloud computing in the future.

REFERENCES

Appistry. (2010). Why cloud computing. Retrieved 01 02, 2011, from Appistry: http://www.appistry.com/cloud-info-center

Beaver, K. (2009, n.d.). Firewall Best Practices. Retrieved May 05, 2011, from http://www.principlelogic.com/docs/Firewall_Best_Practices.pdf

Binning, D. (2009). Top Five Cloud Computing Security Issues. Retrieved 06 15, 2011, from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

Brodkin, J. (2008). Gatrner: Seven Cloud computing security risks. Retrieved 06 07, 2011, from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

Brown, T. (2011, October 06). House Homeland Security - Cybersecurity, Infrastructure Protection, and Security Technologies Hearing - "Cloud Computing: What are the Security Implications?". (CONGDP, Ed.) Congressional Documents and Publications.

Center, E. P. (2009). USA Patriot Act. Retrieved 07 18, 2011, from E.P.I.C. Patriout Acts: http://epic.org/privacy/terrorism/usapatriot/

Community, A. T. (2011). Microsoft Windows Azure Platform Technical Analysis. Retrieved 07 17, 2011, from http://unknownerror.net/2011-07/37617-microsoft-windows-azure-platform-technical-analysis.html

Forouzan, B. A. (2009). Cryptography & Network Security (2nd Edition). New York, USA: Tata McGraw-Hill.

Forouzan, B. A. (2010). TCP/IP Protocol Suite (3rd Edition). New York, USA: Tata McGraw-Hill.

Liddle, J. (2009). Cloud Computing Best Practices. Retrieved 07 17, 2011, from http://websphere.sys-con.com/node/1103814

Microsoft. (2003). What is TSL/SSL? Retrieved 06 17, 2011, from Microsoft Technet: http://technet.microsoft.com/en-us/library/cc784450%28WS.10%29.aspx

Owens, D. (2010, June). Securing elasticity in the cloud. Communications of the ACM , 46.

Perilli, W. (2009). The benefits of virtualization and cloud computing. Retrieved 07 17, 2011, from http://virtualization.sys-con.com/node/870217

Rittinghouse, J. W. (2009). Cloud Computing : Implementation, Management, and Security. CRC Press.

Schultz, B. (2011). Public v/s private cloud: why not both? Retrieved 05 02, 2011, from http://www.networkworld.com/supp/2011/enterprise2/040411-ecs-cloud.html

Subramanian, K. (2009). Public v/s Private Cloud computing. Retrieved 04 02, 2011, from http://www.cloudave.com/1670/public-vs-private-cloud-brouhaha-my-take/

VeriSign. (2009). SGC: True 128 Bit SSL Encryption. Retrieved 06 18, 2011, from SSL Certification: http://www.verisign.com/ssl/ssl-information-center/strongest-ssl-encryption/index.html

Winkler, V. (. (2011). Securing the Cloud - Cloud Computing Security Techniques and Tactics (1st Edition ed.). Oxford: Syngress.