**Dissertation Research Proposal**

**For a**

**MBA in I.T Management**

Student name

Institution

Date

**Proposed Title**

*Cloud Computing: Managing the Security Risks in Small and Medium Enterprises in the United Arab Emirates*

**Summary**

Cloud computing, in its present form, is a fairly new and evolving paradigm and as an industry it is showing huge growth potential. This is due mainly to the sheer attractiveness of providing very expensive server computing technology to smaller businesses that find it completely impractical to invest in this type of infrastructure when their needs are, for the most part, sporadic with usage requirements that are difficult to forecast. It is also useful for the larger companies that have their own servers for day to day operations, but require increased computing power for relatively short periods of time in their business cycles (Chee & Franklin 2010). The ability to pay for the services as required without the costly infrastructure expenses is a good business model.

The relative newness of this type of service, while highly beneficial, has the potential for huge risks for the customers including security risks. This paradigm is a network in which the primary users have minimal control of the structure, shared users, and overall security, particularly in relation to data that is processed or stored in the external servers.

This mixed method study will discover and examine the issues that arise from the risks identified and discussed in the literature, particularly in relation to security for the small and medium business owners in the United Arab Emirates who access cloud computing technology to support their internet-based businesses. Data will be collected, from a convenience sample of information technology mangers in small and medium enterprises that conduct some or all of their business using the internet in the United Arab Emirates, using an on-line survey instrument that will be designed to collect both quantitative and qualitative data about their cloud computing experiences and issues.

The risks will always exist, but this researcher intends to discern which risks are the most problematic for end users in this country. The researcher will determine what mitigations are already being employed by information technology professionals that are supporting these internet-based businesses and how effective they are in minimizing security issues. And finally, the researcher will determine what issues persist and the types and levels of risk these issues bring to business owners and operators in the United Arab Emirates. Discovering the nature and severity of these risks will enable the information technology industry, the support organizations for small and medium enterprises, and perhaps even government to develop technology or policy to secure the cloud for end users in this country.

The potential for business growth will only increase as more small and medium enterprises access cloud-computing services and technology and this research will contribute to the ability of small and medium enterprises in the United Arab Emirates to minimize their risks associated with conducting business using this type of technology.

**Literature Review**

**Cloud Computing: A Definition**

The services offered by providers that deliver either hardware or software over the internet are referred to as cloud computing (Armbrust et al., 2010). Cloud computing provides business access to off-site resources that are efficient and agile (what is needed, when it is needed).

Marstona et al. (2011) define cloud computing as:

An information technology service model where computing services (both hardware and software) are delivered on-demand to customers over a network in a self-service fashion, independent of device and location. The resources required to provide the requisite quality-of-service levels are shared, dynamically scalable, rapidly provisioned, virtualized and released with minimal service provider interaction. Users pay for the service as an operating expense without incurring any significant initial capital expenditure, with the cloud services employing a metering system that divides the computing resource in appropriate blocks.

Mell & Gance (2011) of National Institute of Standards and Technology in the United States drafted a lengthy definition of cloud computing, including this first line:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**Deployment Models**

Ogigău-Neamţiu (2012) describes four deployment models for cloud computing. The private cloud is infrastructure designed and operated for only one business user. It can be hosted externally and managed by a third party, but in effect is a company's private server. This model does not have any of the benefits outlined in the next section. The *public cloud* is infrastructure made available to subscribers or pay-per-use customers by a third party cloud service provider. The *community cloud* is infrastructure purchased and managed by a consortium of users. It is similar to the private cloud, but the costs are shared by all the members of the consortium. The hybrid cloud is a combination of two or more of the other models and users have both on-site and off-site infrastructure to support their computing requirements.

**Advantages of Cloud Computing**

Armbrust et al. (2010) explain how a 'pay as you go' utilization of accessing an external server for utility computing makes more economic sense than tying up capital resources in a server that will be under-utilized much of the time. Cloud computing now permits a business to purchase server hours on demand and as needed, such as for peak load times or when the organization needs additional server time to perform batch analytics. Additionally, when a business is unable to determine how much server time/capacity they may require (e.g., during a new Web startup), cloud computing does not require up-front commitments and will support spikes and the business will not be penalized (at least not from the public cloud) when there is a reduction in demand.

Marstona et al. (2011) reported that six corporate data centres who participated in a survey conducted by Gartner Research showed they were using only 10-30% of their available computing power. The businesses were responsible for 100% of the maintenance and service costs, however and this has been shown to be up to two-thirds of an 'average corporate IT staffing budget.' The cloud permits smaller businesses to benefit from "computational exercises [that] typically involve large amounts of computing power for relatively short amounts of time" without having to invest in high-cost server resources. In fact purchasing cloud computing services can provide a business "immediate access to hardware resources with no upfront capital investment" as well as to innovative applications (Antonopoulos & Gillam 2010).

The opportunity for cost reduction while still enjoying optimal, efficient, and fully scalable computing resources that can be provisioned immediately and on demand, implemented according to business needs, decommissioned when no longer required, scaled up when business requirements peak, and scaled down when requirements wane is very attractive indeed. However, this burgeoning newer method of sharing technological resources had brought a plethora of privacy, security, reliability, access, and regulation issues (Rittinghouse & Ransome 2010).

**Security Issues in the Cloud**

While the benefits of cloud computing delivering business-supporting technology are vast, there are a number of issues and security challenges that must be acknowledged and addressed. Marstona et al. (2011) insist there is an "urgent need for understanding the business related issues surrounding cloud computing."

The Cloud Security Alliance (2013) and Samson (2013) identify and discuss nine top threats to security as a result of cloud security The 'Top Threats Working Group' conducted a survey of industry experts and compiled a list of nine critical threats to cloud security (ranked in order of severity):

1. Data Breaches

2. Data Loss

3. Account Hijacking

4. Insecure APIs

5. Denial of Service

6. Malicious Insiders

7. Abuse of Cloud Services

8. Insufficient Due Diligence

9. Shared Technology Issues

**Objective**

This project seeks to discover the experience of managers providing information technology services to small and medium enterprises that serve their customers using the internet. Specifically, this research will gather feedback from information technology managers on their utilization of cloud computing services, the specific issues they have encountered, the mitigation activity resulting from encountered issues, the efforts they have undertaken to ensure security of their cloud enabled business interests and data storage, and their perceptions on the value of cloud computing to their respective businesses.

**Project Outcomes**

The purpose of this mixed methods study is to evaluate the current state of cloud computing in the United Arab Emirates. The researcher will gather quantitative and qualitative data from identified stakeholders in order to determine the specific risk factors, and associated mitigation in relation to security, associated with utilizing cloud computing technology and services to support internet-based businesses in this country in 2013. By examining the experiences of businesses currently engaged in this practice, this study hopes to discover commonalities in the issues experienced by the selected stakeholders.

The results will permit the researcher to make recommendations for specific solution opportunities for information technology practitioners in the UAE.

**Value of this Research**

Ample literature exists explaining the benefits, risks, and mitigations associated with cloud computing, but few are from the perspective of the users who incorporate the cloud into their business operations. In fact, Marstona et al. (2011) claim that the majority of literature concerning cloud computing is from a computer science perspective and it is 'imperative' for IS researchers to "bring forth a holistic perspective that has often been lacking in many technology discussions" on the business issues related to technology. The stories that will be collected in this study will add to the body of knowledge by providing a perspective of cloud computing from the end users point of view and begin to understand the prevalence, severity, and business costs of the issues arising from the risks associated with cloud computing. Ideally this knowledge will provide opportunities for this researcher and others to engage in activities that will support the specific needs of business owners in the United Arab Emirates with regards to the standardization of privacy, security, reliability, access, and regulation within this newer service industry.

**Research Questions**

What are the major risks associated with cloud computing in small and medium enterprises (SME), in the United Arab Emirates, which conduct business using the Internet?

What solutions exist to mitigate each of these risk factors?

What internal factors (i.e., policy, training, etc.) must also be addressed to implement an appropriate security system to protect data and business interests?

What security measures are SMEs, that are utilizing the cloud, employing?

What commonalities exist in the issues experienced by SMEs in the UAE?

**Research Methods**

**Data Collection: Survey Research**

A survey instrument will be designed to collect both quantitative and qualitative data on cloud computing experiences from a convenience sample of information technology mangers in small and medium enterprises that conduct some or all of their business using the internet in the United Arab Emirates.

Quantitative Data

Check box response: Type of cloud usage/access (list of uses and types of access will be provided)

Scaled response: Frequency of cloud usage/access

Scaled response: Level of comfort (satisfaction) with cloud usage/access

Check box response: Types of issues encountered (list generated from current literature plus an option for adding issues not listed)

Scaled response: Level of impact on business due to issues

Check box response: Current security measures (both technology and policy) employed (list generated from current literature plus an option for adding issues not listed)

Scaled response: Level of internal resource requirements to implement security measures (description line added for respondent to define the internal resource e.g., financial costs, training, policy development, etc.)

Demographics: Type of business, number of employees, number of employees engaged in IT

Qualitative Data

Narrative response: Description of the most serious issues relating to cloud security facing the business, the best security solutions employed by the business, and the solutions that the business wished were available or more affordable.

**Data Analysis: Descriptive Statistics**

Check box responses will be processed to generate percentages of businesses associated with each check box category. Data will be reported using frequency charts and broken down by business type (based on data collected in the demographics section)

Scaled responses will be processed to generate mean scores for satisfaction, impact, and level of resource requirements.

Narrative responses will be processed and analyzed for themes and observed constructs will be reported in frequency tables or charts.

The discussion section of the dissertation will review the overall discoveries and the data will be supported by quotations from the stakeholder narratives.

**Data Sources**

A search of the Internet will be conducted to generate a list of at least fifty small to medium enterprises in the United Arab Emirates that conduct business over the Internet, including the names and contact information of their information technology or network manager.

An emailed invitation will be sent to the manager of each company inviting them to complete an on-line survey. We will encourage their participation by offering to share our final outcomes. We will contact each potential respondent with a telephone call in order to ensure maximum participation from as many respondents as possible.

**Proposed Outline of Dissertation**

I Introduction

Background

Statement of the Problem

Objectives of the Study

Significance of the Study

Scope and Limitations

Key Terms

II Literature Review

Definition of Cloud Computing

Benefits of Cloud Computing

Risks of Cloud Computing

Security Issues in the Cloud

Mitigation of Cloud Risks

III Methodology

Research Design

Sources of Data

Methods of Data Collection

Methods of Analysis

IV Results

V Summary

Summary

Conclusion

Recommendations

VI References

VII Appendices

VIII Approval Sheet

**Research Plan**

Review of academic journals for scholarly literature using key words: cloud computing definition, cloud computing benefits, cloud computing risks, cloud computing security. Generate a comprehensive collection of literature to conduct a meta-analysis of cloud computing - risks, benefits, and security measures.

Development of a survey instrument to collect feedback from information technology managers in small and medium enterprises (who conduct business on the Internet) about utilization of cloud, benefits, risks, issues experienced, and security measures undertaken.

Draft an invitation to recruit information technology managers to complete the electronic survey.

Internet search for at least fifty small and medium enterprises that conduct business on the Internet, in the UAE, including names and contact information on their information technology manager.

Administration of survey to selected population.

Follow up telephone calls to engage respondents, to assure a maximum response rate from this convenience sample.

Quantitative (descriptive statistics) and qualitative (themes) analysis of survey responses.

Draft recommendations based on findings.

**References**

Antonopoulos, N & Gillam L. (2010). *Cloud computing: Principles, systems and applications*. London: Springer-Verlag London Limited.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Ion Stoica, A., & Zaharia, M (2010). *A view of cloud computing. Communications of the ACM.* Retrieved from http://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext

Chee B. & Franklin J. (2010). *Cloud computing: Technologies and strategies of the ubiquitous data center.* New York, NY: CRC Press.

Cloud Security Alliance (2008). *The notorious nine: Cloud computing top threats in 2013. Cloud Security Alliance*. Retrieved from http://www.cloudsecurityalliance.org/topthreats

Marstona, S., Lia, Z., Subhajyoti Bandyopadhyaya,S, Zhanga, J., & Ghalsasib, A (2012). *Cloud computing — The business perspective. Decision Support Systems*. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167923610002393

Mell, P. & Grance, T (2011). *The NIST definition of cloud computing (draft): Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD: U.S. Department of Commerce.* Retrieved from http://pre-developer.att.com/home/learn/enablingtechnologies/The\_NIST\_Definition\_of\_Cloud\_Computing.pdf

Ogigău-Neamţiu, F (2011). *Cloud computing security issues. Journal of Defense Resources Management.* Retrieved from http://journal.dresmara.ro/issues/volume3\_issue2/13\_ogigau.pdf

Rittinghouse J. W. & Ransome J. F. (2010). *Cloud computing: Implementation, management, and security*. New York, NY: CRC Press.

Samson, T (2008). *9 top threats to cloud computing security. InfoWorld [blog] 25 February.* Retrieved from http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428