Abstract

The thesis investigates, in a qualitative way, the vectors that contribute to cloud computing risks in the areas of security, business, and compliance. The focus of this research is on the identification of risk vectors that affect cloud computing and the creation of a framework that can help IT managers in their cloud adoption process. Economic pressures on businesses are creating a demand for an alternative delivery of the model that can provide flexible payments, dramatic cuts in capital investment, and reductions in operational cost. Cloud computing is positioned to take advantage of these economic pressures with low cost IT services and a flexible payment model, but at what risk to the business? Security concerns about cloud computing are heightened and fueled by misconceptions related to security and compliance risks. Unfortunately, these security concerns are seldom, expressed quantifiably. To bring clarity to cloud computing security, compliance, and business risks, this research focuses on a qualitative analysis of risk vectors drawn from one-on-one interviews with top IT experts selected. The qualitative aspect of this research separates facts from unfounded suspicions, and creates a framework that can help align perceived risks of cloud computing with actual risks. The qualitative research was done through interviews with experts and through the survey to measure risk perceptions about cloud computing using a Likert scale. The decision-making model and the framework created by this research help to rationalize the risk vectors on cloud environments and recommend reducing strategies to bring the IT industry one step closer to a clearer understanding of the risks-tradeoffs implications of cloud computing environments.

Keywords

Cloud computing, CSRF, CBRF, CCRF, Cloud Provider, Cloud assets, Compliance, Expert, IT Professional, Threat, Vulnerability, Attack, Risk.

Abstrakt

Práce zkoumá kvalitativním způsobem vektory, které přispívají k rizikům cloud computingu v oblasti bezpečnostní, obchodní a shody standardů. Zaměření tohoto výzkumu je na identifikaci rizikových vektorů, které mají vliv na cloud computing a vytvoření rámce, který může pomoci IT manažerům v procesu přijetí cloudu. Ekonomické tlaky na podniky vytvářejí poptávku po alternativnívh dodávkách pomocí modelu, který může poskytnout flexibilní platby, dramatické škrty v oblasti kapitálových investic a snížení provozních nákladů. Cloud computing je schopen využít těchto ekonomických tlaků na poskytování nízkonákladových IT služeb a flexibilního platebního modelu, ale s jakým rizikem pro podnikání? Bezpečnostní obavy cloud computingu jsou zvýšeny a podporovány mylnými představami o zabezpečení a riziky spojenými s dodržováním předpisů. Bohužel, tyto obavy o bezpečnost jsou zřídkakdy vyjádřeny kvantifikovatelně. Cílem je vyjasnit cloud computing zabezpečení, dodržování předpisů, a podnikatelská rizika, proto se tento výzkum zaměřuje na kvalitativní analýzy rizikových vektorů čerpané z individuálních rozhovorů se špičkovými IT odborníky ve vybraných společnostech. Kvalitativní aspekt tohoto výzkumu odděluje fakta od nepodložených podezření a vytváří rámec, který může pomoci sladit vnímaná rizika cloud computingu s aktuálními riziky. Kvalitativní výzkum byl proveden prostřednictvím rozhovorů s experty a prostřednictvím průzkumu vnímání rizik ohledně cloud computingu pomocí otázek a odpovědí s využitím Likertovy stupnice. Rozhodovací model a rámec pomáhají racionalizovat rizikové vektory v cloudovém prostředí a doporučit strategie ke snížení rizik tak, aby IT průmysl byl o krok blíž k jasnějšímu pochopení rizik a kompromisů, které vyplývají z důsledků prostředí cloud computingu.

Klíčová slova

Cloud computing, CSRF, CBRF, CCRF, poskytovatel cloudu, cloud aktiva, shoda, expert, IT profesionál, hrozba, zranitelnost, útok, riziko.

Introduction

The thesis presents an analysis of cloud computing risks associated with security, compliance and business risks. The research focuses on helping IT managers in their ongoing risk trade-off efforts, which must always balance the demands of the business, constant regulatory changes that must be meet and escalating security threats (1). IT managers and CIOs engage in a relentless battle to maintain the confidentiality of dealings and the protection of information, and they spend a lot to money to make sure delicate data is keep protected. Nevertheless, IT security problems accounted for more than 160 major security breaches from January 2010 to April 2011 (2). When the cloud computing becomes more persistent, many organizations are considering moving mission-critical workloads to cloud processing promotions. However, doubt and limitations to adopting continue to persist due to issues about security, conformity, and business threats, as well as the lack of an efficient design to justify and evaluate IT threats in cloud processing services

The research concentrates on a qualitative research of Cloud Computing & IT threats that are motivated by security, conformity, and business issues, and efforts to provide a design to justify these threats. In addition, a structural structure is to provide assistance in the assessment and execution of cloud computing, with minimization techniques to decrease IT threats.

Goal of thesis

The aim of the thesis is to bring clarity and to create a better understanding of the security, business, and compliance risks associated with cloud computing, and to align perceived risks with actual risks. There is much discussion about cloud computing in magazines and blogs across the Internet, but there are very few reliable sources, that document the facts about cloud risks and adoption principles to reduce possible risks. We are in the early stages of cloud computing adoption and cloud providers are competing with each other to establish their offerings. Lack of well-documented cloud standards and cloud certifications are hindering the ability to classify clouds using appropriate measurements or characteristics. IT vendors continue to rely on quality of service (QoS) characteristics to evaluate clouds without appropriate acknowledgment of more important risk factors that plague cloud services.

This analysis research will try to builds a model from the knowledge and insight gathered from interviews with more than sixty cloud and security industry experts and users.

The main goal of this research is to create a model that can guide IT professionals in the understanding of security, compliance, and business risks associated with cloud offerings, and tradeoffs that could reduce these risks.

A model that can help categorize and value cloud-computing risks is a significant contribution to the IT community, and computing science body of knowledge,

These are some of contributions for the IT community, which this research delivers.

1. Provides guidance to rationalize risks associated with cloud computing environments in a way to foster better understanding of cloud services.

2. Provides analogies with common situations and other industries to put into perspective the risks associated with cloud offerings. Unfortunately, news media have exaggerated the levels of perceived cloud risk based on isolated incidents that are very unlikely to affect most users. The net effect is the distortion of perceived risk about cloud environments held by many IT professionals. This research will try to provide a model to evaluate risks and help align perceived risk with actual risk.

3. Provides guidance to minimize the overestimation of cloud capabilities, including elasticity, availability, and performance. In addition, helps estimate the challenges associated with moving workloads to the cloud to obtain horizontal scaling (elasticity) and other cloud features.

4. Creates three cloud frameworks for the evaluation and understanding of security, business, and compliance risks.

5. Identifies risks vectors affecting each of the cloud frameworks and provides reducing strategies to minimize possible exposures to ensure selected workloads perform as expected and at a good price point.

6. Explains the value of cloud computing, which workloads are best to move to the cloud to take advantage of low-cost IT.

7. Identifies the cloud risk perceptions of IT professionals, based on the results of a survey targeted to IT cloud professionals.

Research materials and methods

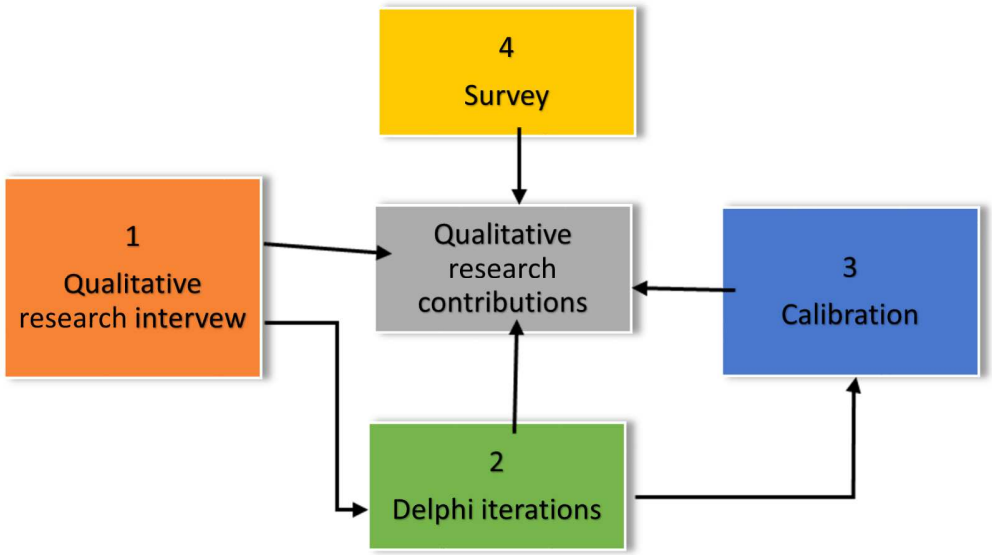
This research analyzes many cloud-computing issues related to security, business, and compliance in an attempt to make sense out of the risks associated with these complex systems. With this qualitative research, we attempt to answer the “what” and “why” of the most important cloud risks. It has left for further research to determine the “how” to best fix cloud problems identified by this research. This research is achieve a simple and coherent way for IT manager to understand and rationalize cloud-computing risks and help them gain some insight on reducing strategies for current cloud risks.

This research used several instruments to research and evaluate risk vectors associated with current cloud computing offerings, and then compared those risks to traditional IT. In the context of this research, as we discussed in Chapter 2, Traditional IT refers to an IT environment that not virtualized, not multitenant, hosted on premise, and with minimum automation. Traditional IT is a well-understood model and that is why is select as the frame of reference to compare with new emerging cloud services risks.

The method employed by this investigation used multiple techniques to collect data, test with a control group, and refine questions as more knowledge gained on the subject.

This research using a modified Delphi process that consisted of Online Questions form and interviews, Delphi iterations to build consensus, and a quantitative analysis that was built using a calibration spreadsheet. These three steps depicted as boxes 1, 2, and 3 in Figure 1. In addition, this research conducted a survey with IT professionals to gain additional support regarding cloud risks perceptions. This research step is illustrated in Figure 1 as box number 4. The final research deliverables listed in the last box in Figure 1.

Figure 1 Steps followed by qualitative research



Research hypotheses

Hypotheses 1- There are differences in risk perceptions between cloud security experts and other IT professionals who are not subject matter experts.

Hypotheses 2- Deep knowledge of cloud security can have a conservative effect

Conclusion

This research has expanded the collective knowledge about cloud computing risks and reducing strategies associated with cloud security, business and compliance risks vectors. By discussions with experts, all cloud risks and reducing methods introduced in the thesis help to rationalize cloud risks and guide IT professionals in what to look for when considering the adoption of cloud computing in the enterprise. Finally, the research goals listed were:

1. The research has created three frameworks:
    I. The Cloud Security Risks Framework (CSRF).
    II. The Cloud Business Risks Framework (CBRF).
    III. The Cloud Compliance Risks Framework (CCRF).

2. In addition, this research illustrated the way financial benefits of the cloud can fluctuate depending on the kind of workloads.
3. The potential financial aids of cloud could be significant, in the meantime substantial reduction in IT cost can be achieved by utilizing the lowest possible configuration and dynamic provisioning of VMs to support demand peaks.
4. Extensive interviews with security and cloud experts provided insights on cloud security, business, and compliance risks. Analysis on the data provided by the experts and consensus-driven Delphi method with the control group helped to rationalize cloud risks and compare these risks with those found in traditional IT.
5. With the intention to guide, IT professionals on their cloud adoption plans, a series of reducing recommendations were provide for each of the risk vectors identified by this research.
6. However, it was not the intention of this research to provide a comprehensive list of reducing alternatives, but instead to offer sufficient reducing options to assist IT professionals with their cloud risks evaluations, and tradeoff decisions between business benefits and security and compliance risks.

    The frameworks of this research created based on the large amounts of data, offered by the experts, are expected to be used by IT managers as a way to rationalize many risks.

Association with cloud computing will ~~to~~ help to understand cloud computing risk vectors, and to prove that cloud risks are a combination of new risks, as well as prior risks already existing in traditional IT.

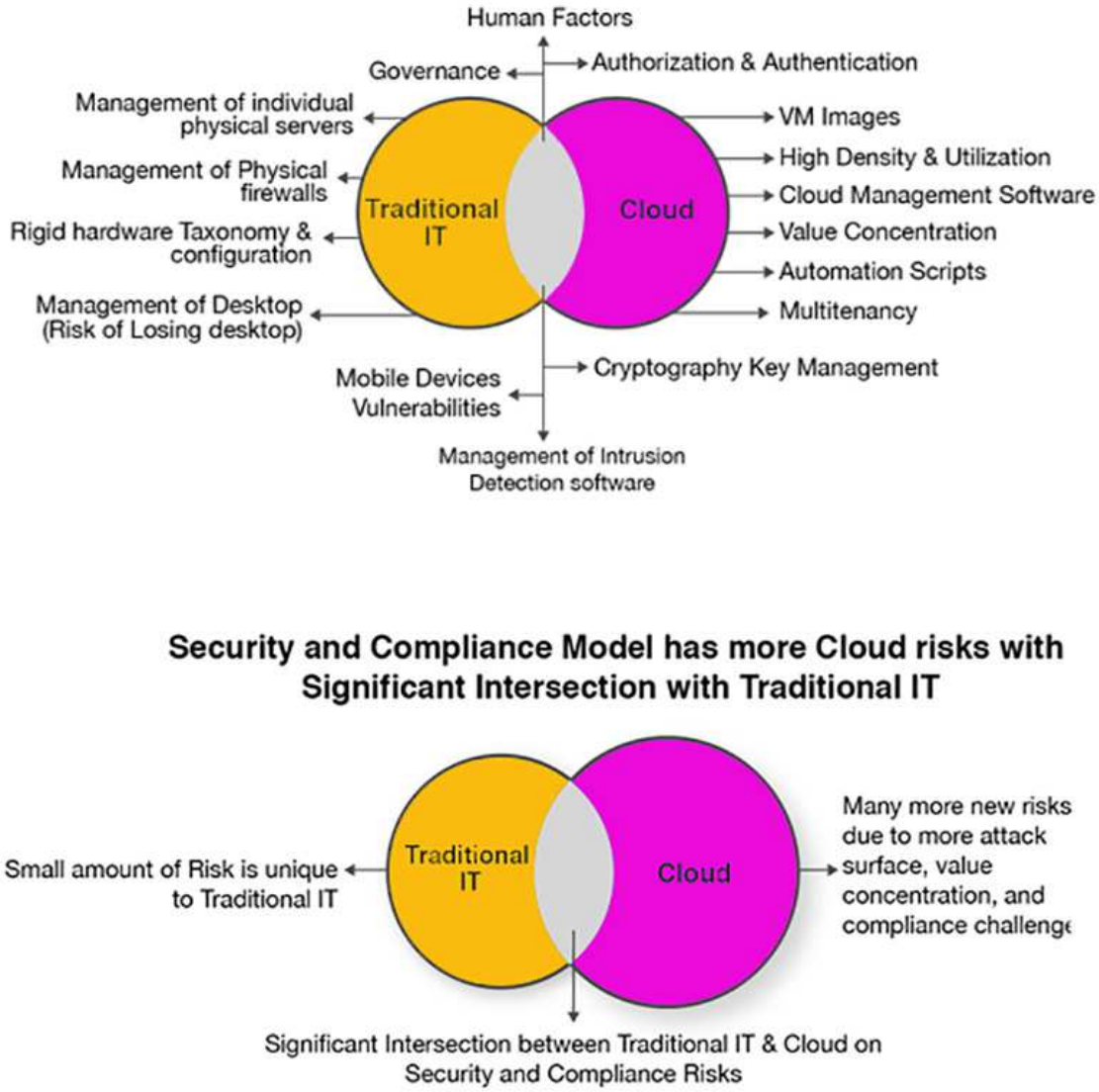
In the literature review, many of the current risks prevalent on clouds as well as traditional IT, and under the Cloud Security Risk Framework, the new cloud-specific security risks, such as multitenancy and automation risks were discussed.

New cloud compliance risks related to cyber forensics, data segmentation, and data remnants are a few of the many new risks associated with clouds, and described under the Cloud Compliance Risks Framework.

Associated with clouds, and described under the CCRF. In addition, we discussed some of the risks that remain exclusively on traditional IT, such as high upfront capital investment for new IT services, and the ever increasing operational cost of proprietary configuration of traditional IT. Based on the substantial data collected by this research, and the analysis of the three frameworks offered by this investigation we can conclude that:

1. Many cloud computing risks are distinctly different from traditional IT risks, that traditional IT still has unique risks that differ from cloud computing,
2. In addition, that there are some of risks that are shared across both environments, creating what we can consider an intersection of risks between cloud and traditional IT.
3. We can conclude that the vectors from the business and compliance cloud models have aggregate total risks higher than traditional IT. From the data obtained by this research, the Cloud Security Risk Framework, and the Cloud Compliance Framework, We have sufficient evidence to conclude that clouds have substantially higher risks than traditional IT in the areas of security and compliance Figure 2.

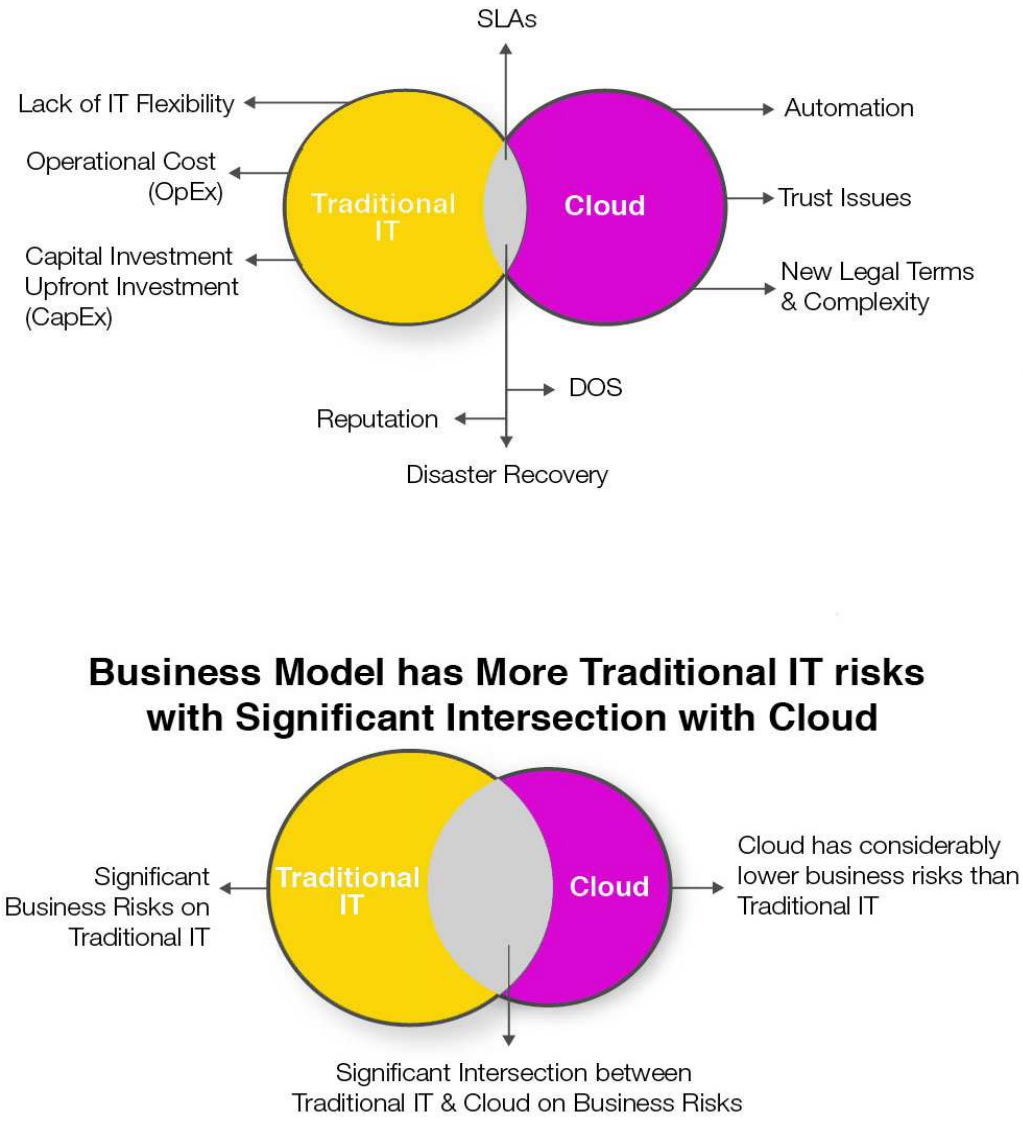
Figure 2 Cloud Security and Compliance Risks Model



Source Author

Following the same logic on the business side, what is shown to us that the CBRF tends to have vectors with aggregate risks lower than traditional IT, Some of the vectors driving higher business risks on Traditional IT are presented in Figure 3.

Figure 3 Cloud Business Risks Model



Source: Author

For each of the threat vectors, the analysis offered some stage of suggestions to reduce the risk. In accordance with the many minimization techniques provided, the fast speed with which cloud computing technological innovation is improving, and the significant economic advantages of

the cloud business, we can conservatively predict that many of the cloud risks uncovered by this research will diminish over time, and clouds will become a much safer place to outsource company IT services.

This research found several areas that could benefit from additional research. For example, there is a wealth of additional research that should be done on how to improve cyber forensics tools and methodology in cloud environments.

The dynamic aspects of clouds have created many challenges for cyber forensics practitioners, and there are not too many mitigation strategies to contain this risk vector. In addition, this research did not investigate the claims from some of the experts on possible correlation between best practices and the cost to transform the business to adhere to new regulatory compliance rules, but this could be interesting future research.

Since the pace of technology is very fast in the area of cloud computing, it would be

It would be interesting to do an evaluation of cloud risks in several years to show how risk vectors, identified by this research, have changed with new technologies. We suggest that many current risk vectors are very likely to have lower risk levels in the future, but new vectors will appear and others, like the human factor, will remain the same.

References

1. P.Hochmuth. *cloud security survey.* s.l. : IDC, 2011.

2. IDC. *Data center and cloud computing survey.* s.l. : IDC, 2010.

3. Roman T, Lamas,William Stofega. *Worldwide smartphone 2013-2017 forcast and analysis* . s.l. : IDC, 2013.

4. IDC. *data center and cloud computing survey* . s.l. : IDC, 2010.

5. Peter Mell, Timothy Grance. The NIST Definition of Cloud. *National Institute of Standards and Technology.* [Online] September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. 800-145.

6. Lydia Leo, Neil MacDonald. *Cloud IaaS: Security Considerations.* G00210095 : Gartner, March,2011. http://www.chinacloud.cn/upload/2011-11/11113019588314.pdf.

7.M, Azua,. *The Social Factor : Innovate, Ignite, and Win through mass collaboration and social networking.* s.l. : IBM press, 2009.

8. TeleGeography's. *GLOBAL BANDWIDTH RESEARCH SERVICE EXECUTIVE SUMMARY.* s.l. : TeleGeography's, 2013. http://www.telegeography.com/page_attachments/products/website/research-services/global-bandwidth-research-service/0003/8368/gb13-exec-sum.pdf.

9. M. Weilage. Mary's Shoebox2",. *techrepublic.* [Online] April 5, 2010. [Cited: march 5, 2013.] http://www.techrepublic.com/photos/marys-shoebox2/280735?seq=108&tag=content;siu-container#photopaging.

10. (GENERIC) (GENERIC) C. Wolf. Apples, Oranges, and Hypervisor Price Comparisons Chris. Apples, Oranges, and Hypervisor Price Comparisons Chris Wolf's Virtualization Tips and Ramblings,. *C. Wolf.* [Online] april 2008. [Cited: December 15, 2012.] http://www.chriswolf.com.

11. *Cloud Computing Vs. Grid Computing.* Seyyed Mohsen Hashemi, Amid Khatibi Bardsiri. Tehran, IRAN : ARPN Journal of Systems and Software , 5,may,2012. 2222-9833 .

12. google. google trends. [Online] 2013.

13. *World Community Grid.* [Online] http://www.worldcommunitygrid.org/..

14. N. G. Carr. IT Doesn't Matter. *http://utminers.utep.edu.* [Online] may 1, 2003. [Cited: January 2, 2013.] http://utminers.utep.edu/kbagchi/itdoesntmatter.pdf.

15. JeffreyDeanand, SanjayGhemawat. MapReduce: Simplified Data Processing on Large Clusters. [Online] 2008. [Cited: december 25, 2012.] http://static.usenix.org/event/osdi04/tech/full_papers/dean/dean.pdf.