The Impact of Cloud Computing on Organizations in Regard to Cost and Security

Mihail Dimitrov
Ibrahim Osman

Department of informatics
IT Management
Master thesis 1-year level, 15 credits
SPM 2014.22

Abstract

Throughout the recent years cloud computing has gained large popularity in the information technology domain. Despite its popularity, there are many organizations that are lacking broader understanding of implementing and utilizing cloud computing for business and operating purpose due to the existing vagueness regarding its cost and security effect associated. It is argued that the main attractiveness of cloud computing for organizations is its cost effectiveness, whilst the major concern relates to the risks for security. Accordingly, more effort has been made in exploring these issues of cloud computing impact. However, little effort has been focused at critically examining the cost risks and security benefits which cloud computing bring to organizations. By using a qualitative method this research examines in detail the essential benefits and risks of cloud computing utilization for organizations in terms of cost and security. Unlike prior studies, it also explores the cost risks and security benefits and shows that they should be taken into consideration by organizations. The findings are based on empirical data collected via interviews with IT professionals. The main cost risk identified is the lack of accurate and sophisticated cost models on the current cloud market. Among the identified security benefits are increased data safety, faster data recovery and transfer, centralization, and improved security software mechanisms and maintenance. Moreover, this research shows several major implications that organizations should keep in mind while utilizing cloud computing and provides some suggestions on how to avoid the cost and security risks identified. At present, reduction of the operational and administrative costs is seen by organizations as the most essential cost benefit. The results show that cloud computing is better for small- and medium-sized organizations and that the hybrid cloud is the most appropriate model for them. Furthermore, the cost and security risks of cloud computing cannot be avoided without resolution of the problem with the lack of accurate cost models, international regulatory frameworks and interoperable security standards on supranational levels.

1. Introduction

Cloud computing is one of the most discussed and promising IT innovations in today's technological market. It is very attractive for organizations thanks to the potential it brings such as increased efficiency and cost savings. It constitutes a fundamental shift in the way organizations are provided with computing resources (Greenwood at al., 2011). The provision is moving from computing as a *product* to computing as a *service* (Greenwood at al., 2011), as this shift is inevitable and irreversible (McAfee, 2011 p. 126). This technology is evolving and growing very fast. According to research firm IDC, the Worldwide revenue from public IT cloud services exceeded $ 21.5 billion in 2010 and will reach $ 72.9 billion in 2015 (IDC, 2013). Many IT players, such as Google, Amazon, Microsoft, etc., are involved in developing and offering cloud services. Cloud computing is at its infant stage of life, but in 10 – 15 years it will look completely different (Velte et al., 2010).

Cloud computing has changed the way organizations use computers and the Internet. This change relates mainly to how the information is stored and the applications are used. In cloud computing they are stored in the "cloud" instead of on desktop computers. The cloud is "*a nebulous assemblage of computers and servers accessed via the Internet*". (Miller, 2009 p. 12) It provides users with access to all of their data, documents and applications when they are connected to the Internet. The users are no longer tied to their desktop computers and it is easier for them to collaborate from different locations (Miller, 2009).

Organizations aim to reduce their computing costs. Many of them start doing so by consolidating their IT operations and implementing virtualization technology, that is optimizing the servers capacity to store and process data by hosting the servers on their own premises. Thanks to cloud computing the organizations are able to reduce additionally the costs by improving utilization, reducing infrastructure and administration costs, and faster deployment cycles. It provides them with high availability, virtualization, and dynamic resource pools (Boss at al., 2007).

The term "Cloud Computing" is used for describing both a platform and type of application. Users` and organizations` data is stored in the cloud on servers that can be physical or virtual machines. Those servers are provided, configured, and reconfigured by the cloud computing platform. The term is also used for applications which are made accessible through Internet. Cloud applications are stored in large data centres on powerful servers which host Web applications and Web services (Boss at al., 2007).

Cloud computing allows organizations to use their hardware and software investments in more efficient ways. This is achieved by overcoming the physical barriers of the isolated systems and automated managing a group of systems as a single unit. This technology is seen as a virtualized system which constitutes a natural evolution of data centres (Boss at al., 2007).

In order to decide whether to adopt and utilize cloud computing, organizations need to consider carefully its benefits and risks (Hosseini et al., 2010). However, an enthusiasm about cloud computing often provokes a certain level of skepticism. While the enthusiasm relates mainly to the cost benefits, the skepticism is provoked by the risks for security. Although there are many studies regarding the cost and security effect of cloud computing on organizations, according to McAfee (2011) their results are contradictory. As a result, there is an uncertainty regarding the possible benefits for organizations (Greenwood at al., 2011). Therefore, for eliminating the existing vagueness regarding the cost and security effect a further and deeper research of these issues is necessary. Furthermore, although the extant research is mainly focused on the cost benefits and security risks of cloud computing for organizations, it is still problematic in that it fails at addressing the cost risks and security benefits. In addition, the extant research is lacking suggestions for avoiding these risks. Recognizing the aforementioned gaps in previous research, this paper aims to answer the following research questions:

1. *What are the cost benefits of cloud computing for organizations and are there any cost risks?*
2. *What are the security risks of cloud computing for organizations and are there any security benefits?*

To address these research questions, this thesis explores in detail the impact of cloud computing on different organizations in cost and security aspect and identifies the benefits and risks they face while utilizing cloud services. Thus, this research aims to provide in-depth and complete understanding of these issues and contribute to the cloud computing research area.

2. Literature review

In order to understand the impact of cloud computing on organizations in terms of cost and security, it is necessary to understand what cloud computing is. This chapter firstly reviews background information about cloud computing based on prior studies, including cloud computing definition, essential characteristics, deployment and delivery models, and security trade-offs (2.1). Then, it reviews extant research related to the cost (2.2) and security (2.3) aspect of cloud computing impact on organizations. Since the extant research fails at addressing the cost risks and security benefits of cloud computing, these sections focus on reviewing the cost benefits and security risks.

2.1 Cloud Computing

Since the emergence of cloud computing many researchers have given definitions trying to define what exactly it is. So far, there is not a universal definition that gives a complete and sufficient understanding of the nature of this phenomenon. A variety of definitions exist because researchers conduct their studies in different research fields – business, education, etc. The most important thing in defining cloud computing is whether the definition explains sufficiently and in a most acceptable manner the cloud computing paradigm. A very well accepted definition is developed by the U. S. National Institute of Standards and Technology (NIST):

> *"Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g. network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell, P., & Grance, T., 2011, p.2)*

This definition explains clearly and simply cloud computing, addressing its main features and aspects and synthesizing most of the developed definitions among many ambiguous descriptions of the phenomenon.

Cloud computing features several distinctive characteristics, deployment and delivery models. A review of these characteristics and models is a must when it comes to understanding of the cloud concept and how cloud computing is organized as a service. The latter relates to the cost and security aspect of the cloud services and the issues that emerge in this field.

The characteristics that make cloud computing appealing to consumers are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (Cloud Security Alliance, 2009). If the consumers need a server time, network storage and applications, they can get them automatically without having to interact with a service provider (Cloud Security Alliance, 2009). As these capabilities are available over the network, they can be accessed from everywhere via different platforms, in-house devices, laptops as well as mobile devices such as smartphones and tablets. We argue that since the mobile devices started getting more power and capabilities, cloud computing has been enabling organizations to enhance their mobility. The next essential characteristic refers to how cloud services are provisioned and managed by cloud providers. Required computing resources such

as storage, memory, processing, virtual machines, and network bandwidth are pooled by the provider in order to serve multiple consumers using a multi-tenant model (Cloud Security Alliance, 2009). These resources are dynamically provided according to the consumers` demand. Besides, they are also delivered elastically, meaning that the supply is not invariable and the consumer gets as much as he needs (Cloud Security Alliance, 2009). Thus, the rapid elasticity of cloud computing allows providers to scale quickly the provision of computing resources. The cloud services are also measured in a sense that the cloud systems optimize, control, monitor and report automatically "*resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service."* (Cloud Security Alliance, 2009). This makes the service transparent and predictive for both providers and consumers. Moreover, we argue that it enables consumers to calculate their long-term need of computing resources through an assessment of the real-time usage.

Cloud Computing has four deployment models; public, private, community and hybrid (Cloud Security Alliance, 2009). Their differentiation is based on the cloud infrastructure`s location and how and by whom it is managed and owned. This implies a different user`s control over the data and its security. Public cloud is a model where the cloud infrastructure is owned by the organization that sells cloud services and is available to the general public (Cloud Security Alliance, 2009). It is the most open model and is appropriate in cases when a high level of data confidentiality is not required. The most closed model is the private cloud, where the infrastructure existing on-premises or off-premises is used only by a single organization and managed by the organization itself or a third party (Cloud Security Alliance, 2009). Organizations employing this model have the fullest control over their data and its security as the cloud is not shared with other organizations (Velte et al., 2010). For organizations willing to share cloud resources a community cloud exists. Its infrastructure is used by several organizations that have shared concerns, e.g. mission, policy, security requirements, or compliance considerations (Cloud Security Alliance, 2009). It may also be on-premises or off-premises and is managed by these organizations or a third party (Cloud Security Alliance, 2009). The fourth deployment cloud model is hybrid cloud, which is composed by two or more cloud infrastructures (private, community, or public) that are linked by standardized technology allowing data and application portability (Cloud Security Alliance, 2009). We argue that this model enables organizations to combine and use the best from the previous models according to their needs.

There are three delivery models of cloud computing; Software (SaaS), Platform (PaaS) and Infrastructure as a Service (IaaS). They differ in terms of the levels of consumer`s control over cloud resources and security. According to the delivery model chosen, this directly reflects on how an organization deals with emerging security issues. SaaS allows consumers to use only applications running on the provider`s cloud infrastructure (Cloud Security Alliance, 2009), meaning that they cannot control and manage the underlying cloud infrastructure including network, servers, storage, and operating systems. This also concerns the individual application capabilities, although there is a possible exception in terms of limited user-specific application configuration settings (Cloud Security Alliance, 2009). The level of integrated security is relatively high and provider is entirely responsible for security (Cloud Security Alliance, 2009). Therefore, in this model the consumer gets least control over

security. With PaaS the consumer can deploy on the cloud infrastructure customer-created or acquired applications (Cloud Security Alliance, 2009). He still cannot control and manage the underlying cloud infrastructure, but can control the deployed applications. The integrated security is less than in SaaS and the consumer has an option to add security himself (Cloud Security Alliance, 2009). IaaS provides the consumer with the greatest control over cloud resources and security. He is able to use and control the main computing resources such as storage, networks, processing, operating systems as well as deployed applications (Cloud Security Alliance, 2009). This model has the least integrated security capabilities among the three as the provider protects only the infrastructure (Cloud Security Alliance, 2009), meaning that the consumer has a full responsibility for the security of the operating systems, applications and data.

As shown in this section, the characteristics of cloud computing illustrate why organizations are tempted to utilize it. Both the deployment and delivery models determine different levels of consumer`s control over cloud resources, data and security. This relates to how an organization deals with emerging security issues. Therefore, for organizations aiming to move into cloud computing, an understanding of the cloud models and the security trade-offs between them is a must. Organizations also have to be aware of the benefits and risks of cloud computing in cost and security aspect, a topic that will be addressed in the following section.

2.2 Cost benefits

The enthusiasm among organizations regarding cloud computing comes mainly from the advantages it brings in terms of cost. Due to that reason, researchers usually focus on the cost benefits while researching the cost impact of cloud computing on organizations. Therefore, the cost benefits of cloud computing and their different facets are reviewed in this section. Nevertheless, as cloud computing is a relatively new technology, despite all the developments in this field there are many untried scenarios that carry a fundamental question of cost risks for relying or even outsourcing some activity using the cloud computing services. However, the extant research is still problematic in that it fails at addressing the cost risks for organizations. For this purpose, this research explores the potential cost risks, which are shown in the conclusions chapter.

First of all, cloud computing enables organizations to reduce their hardware costs (Miller, 2009). When using cloud services, organizations no longer need high-powered and high-priced computers to run applications within the cloud. This comes from the decreased needs for a processing power and storage space (Miller, 2009). Unlike traditional software, for running cloud applications computers need less memory. They also can be with smaller hard disks because there is not installation software. Thus, organizations can reduce costs by purchasing lower-priced computers. Since employing cloud computing, organizations do not have to do high investments in IT infrastructure. This especially concerns the larger organizations (Miller, 2009). Instead of investing a huge amount of money in a large number of powerful servers, the IT departments of those organizations can use the cloud` computing power to replace or improve the internal computing resources. Miller (2009) states, as Armbrust at al. (2009), that organizations do not have to handle with the peaks and the

nonpeak times in computing power demands anymore by purchasing new equipment. Instead, the peak computing demands are handled by cloud servers.

Cloud computing also leads to lower software costs. Organizations no longer have to buy separate software packages for each computer (Miller, 2009). Instead, a particular application is accessed only by the employees using that application. Moreover, this also means saved cost of installing and maintaining that software on each computer. Another software-related cost benefit is that organizations do not have to pay for a software upgrade in order to have the latest versions of the applications (Miller, 2009). As all applications are in the cloud, they are upgraded automatically by the provider. Organizations can also greatly reduce their maintenance costs (Miller, 2009). This refers to both hardware and software maintenance. Less computers and servers means lower maintenance costs. The IT staff in organizations does not have a software to maintain as all applications are in the cloud and are maintained by the cloud provider. In relation to the above statements, we argue that the software costs depend on the cloud deployment and delivery models. This means that the software costs vary according to the levels of control and maintenance allowed by those models. Consequently, public clouds and SaaS assume lowest software costs, whilst in private clouds and IaaS lowering the software costs is most difficult. The same relation also applies to security costs.

We argue that from a customer`s perspective cloud computing can be seen as a means for increasing productivity and effectiveness of organizations, which in turn increases their income. Increased computing power significantly enforces organizations` productivity. According to Miller (2009 p. 26), organizations are "*no longer limited to what a single desktop PC can do*" and now can "*perform supercomputing – like tasks utilizing the power of thousands of computers and servers*." Thus they can perform greater tasks and increase significantly their productivity and efficiency. On the other hand, from a provider`s perspective the main cost benefits for the vendors are the predictable incomes and the broader customer base (Goncalves and Ballon, 2011). Cloud computing lowers the administrative costs and allows an organization to offload three kinds of administration (Rosenthal et al., 2009). Firstly, it offloads the administration responsible for system infrastructure, e.g. hardware maintenance, infrastructure software, adding new machines and spare parts. Secondly, after specifying the backup policy the provider executes it. Thirdly, once installed, the application is available to all authorized users. Besides the cost benefits of cloud computing, organizations have to address the dangers in terms of security while migrating to the cloud. This subject will be addressed in the following section.

2.3 Security risks

While cost benefits are the key driver for organizations to migrate to the cloud, security risks are the major impediment. According to Pearson (2012), security of cloud computing is the biggest concern for the organizations. The security problems associated with cloud computing come from the abstraction of infrastructure, which results in "*lack of visibility and capability to integrate many familiar security controls - especially at the network layer*." (Cloud Security Alliance, 2009, p.25). On the other hand, it is argued (Pearson, 2012) that these problems come from the ambiguity regarding which parties are responsible for which aspects of security as cloud APIs are yet to be standardized. The security risks may be different

according to the deployment and delivery models employed by organizations. That`s why it is critical for organizations` risk management to understand the relationships and differences between deployment and delivery models, and security trade-offs. These relationships and security trade-offs were reviewed in section 2.1. Cloud computing adoption and utilization might present numerous security risks to organizations. All these risks relate to the security of the data and its confidentiality. It is imperative organizations to have a protected sense of preservation of the data they process, store and transfer while using cloud applications by other party.

The main risks regarding data security are that data may be lost, collected and used by unauthorized parties, which is a result of an inadequate data handling and protection by cloud providers (Pearson, 2012). Besides an inadequate security handling, there is a risk related to the Service Level Agreements (SLAs) between provider and customer. In some cases they may not include any provision of the necessary security services (Pearson, 2012). The problem is that in these agreements there are no clauses that ensure the level of security. As the terms and conditions of service are set in favor of the cloud provider, "*if anything goes wrong it is often the customer that will be made liable."* (Pearson, 2012, p. 28). For instance, this applies to the cases when the customer transfers a security risk to the provider according to the delivery model employed. As not all risks can be transferred, the cloud customer may become legally accountable (Pearson, 2012). We argue that in such cases, an organization has to have an enough financial power to legally defend itself, which is very difficult, especially for small-sized organizations. In addition, Pearson (2012) states that customer may want to monitor whether the service agreements have been fulfilled, but the cloud infrastructure may not provide an appropriate information or analysis due to its complexity.

The data protection within the cloud environment necessitates an appropriate level of access control (Pearson, 2012). However, this control may be inadequate. As a result, there is a risk of unwanted access to confidential information by unauthorized parties, resulting in either stolen or compromised data. These parties may be governments, the internal IT staff of cloud provider, data thieves, attackers and customers of the same cloud service (Pearson, 2012). Such customers may do so due to an inadequate isolation of the different customers` data (Pearson, 2012). This risk occurs because of multi-tenancy feature of the cloud, where one software application serves several customer organizations within a SaaS environment. If the software mechanisms fail to virtually separate the data, a tenant may access and compromise data of other tenants. Data may also be accessed and compromised through the management interface. This applies especially to the public clouds where the management interface is remotely accessed through Internet and a web browser (Pearson, 2012). If a remote access vulnerability occurs, it would put the customer`s data in danger.

The lack of interoperability standards also endangers the data stored in cloud. The architectural standards (e.g., Open Virtualization Format, Open Cloud Computing Interface, SAML, etc.) developed by different cloud providers are mutually incompatible (Pearson, 2012). This incompatibility hampers establishing standardized security frameworks for all cloud providers. As a result, it is difficult for customers to migrate from one cloud provider to another or bring back data in-house (Pearson, 2012). We argue that thus the avoidance of security risks by migrating to a provider offering better data protection is straitened.

Another security risk of cloud computing is an inadequate deletion of customer`s data (Pearson, 2012). Customers want to be sure that the data are completely deleted and not recoverable. In fact, cloud providers do not give any evidence for that and everything relies on trust. Moreover, there are multiple backups of the data on different servers and places, which makes their deletion even more difficult because some backups may be held by different entities. Besides, the provider might not want to destroy a disk that contains other customers' data. The data backups may also be vulnerable (Pearson, 2012), meaning that they may be accessed by attackers, resulting in lost, compromised and unrecoverable data.

Besides all aforementioned security risks that cloud computing poses to organizations, the security benefits must also be examined. However, the extant research is still problematic in that it fails at addressing the security benefits for organizations. For this purpose, this research explores the potential security benefits, which are shown in the conclusions chapter. Thus, in the conclusions chapter both the cost risks and security benefits of cloud computing is shown, along with implications and suggestions for avoidance of the risks identified. An explanation on how this research was conducted will be presented in the following chapter.

3. Methodology

This chapter describes the research method used for this thesis. It begins with describing the research design and approach taken (3.1). Thereafter, the literature review is discussed (3.2), followed by an explanation of the processes of collecting empirical data and data analysis (3.3). Finally, the last section contains a summary of the methodology (3.4).

3.1 Research design and approach

The successful and efficient research requires a preliminary planning of the structure of its conduction. This planning follows the step of defining the research problem and is known as "reseach design". Kothari (2004) describes the research design as *"..the conceptual structure within which research is conducted; it constitutes the blueprint for the collection, measurement and analysis of data."* Choosing a reseach design in advance is of big importance for the research because it makes the research as efficient as possible and provides maximal information with minimal effort and time (Kothari, 2004). Therefore, it is crucial an appropriate design to be chosen. This allows the researcher to refine its ideas in the best way and track the research process for omissions and weaknesses.

There are three main types of research designs: exploratory, descriptive, and hypothesis-testing (Kothari, 2004). According to Kothari (2004), the main goal of the exploratory research studies is *"formulating a problem for more precise investigation or of developing the working hypotheses from an operational point of view"*. As the research topic of this paper has many facets that were to be explored necessitating more precise investigation, the research design taken here is exploratory design. Furthermore, Kothari (2004) argues that the exploratory research studies emphasis on the discovery of ideas and insights. The research problem they investigate is broadly defined initially, but afterwards is transformed into one with more precise meaning. Hence, the exploratory research design was taken in this research as it aims to discover the important and relevant insights of how cloud computing affects

organizations in terms of cost and security and more precisely what cost risks and security benefits it brings.

There are two basic approaches used for researches, quantitative and qualitative. The quantitative approach generates a numerical data which can be used for precise quantitative analysis (Kothari, 2004). It is mainly focused on the deductive part of the research and on theory testing, gathering data through questionaries, interviews and statistical techniques (Bryman & Bell, 2007). On the other hand, the qualitative approach generates a non-numerical data. Kothari (2004) argues that:

> *"Qualitative approach to research is concerned with subjective assessment of attitudes, opinions and behaviour. Research in such a situation is a function of researcher's insights and impressions. Such an approach to research generates results either in non-quantitative form or in the form which are not subjected to rigorous quantitative analysis." (Kothari, 2004, p. 5).*

The aim of this research is to explore the benefits and risks of cloud computing for organizations in terms of cost and security. Its purpose is not providing exact enumerations or measurements for particular benefits and risks. Instead, the focus is to create a detailed and complete picture of the cost and security impact of cloud computing by identifying all existing benefits and risks. Thus, the paper aims to fill the existing gap in extant research, which is the lack of research regarding the cost risks and security benefits. Therefore, the goal of this research does not implicate generation of a numerical data and rigorous quantitative analysis. Rather, it assumes findings based on subjective assessment of opinions. Hence, the qualitative approach was taken in this research. In accordance with the design and approach taken, this research reviews extant literature and uses it along with empirical data collected from interviews for the purposes of data analysis (Kothari, 2004).

3.2 Literature review

As Crawford (1997) argues that in data collection process the review of extant research precedes empirical data collection, this research reviews firstly what have been investigated and discovered by researchers and then collects the empirical data. According to Bryman & Bell (2007), in the area of business and management studies the role of previous research is continuously increasing. The review of extant research is an important part of the qualitative research and has several advantages. Thanks to the extant research researchers are able to get a clearer picture on the phenomena than if using only their own data (Crawford, 1997). Moreover, the overview of previous reliable researches gives the opportunity for a deeper and more detailed understanding on how cloud computing affects organizations. This, in turn, improves the preparation for the empirical data collection process, leading to more relevant and fruitful outcomes. In addition, getting information from the literature is less time-consuming than obtaining empirical data (Crawford, 1997).

For the purpose of this research several preliminary sources were used such as articles, journals, books and information from web-sites. The search for a relevant material had two objectives. The first was to find a material that is as focused as possible and fits the best with the research topic as the research area is rather broad. The second objective was to find a

sufficient amount of literature to make sure that the extant research fails at addressing the cost risks, security benefits and possible suggestions how these issues to be avoided. Afterwards, the selected literature was synthesized and analysed in order the important results to be extracted for the purposes of data analysis. In this case these were the cost benefits and security risks of cloud computing for organizations.

3.3 Data collection and analysis

For the purposes of this research a collection of empirical data was conducted. Collecting empirical data is integral part of qualitative research. The empirical data is a data, which is collected for the first time and is based on people`s experience (Kothari, 2004). Following the recommendations made by Kothari (2004), interviews were used in this research for empirical data collection. Conducting an interview as an empirical data source has both advantages and disadvantages. Its advantage is that it helps the researcher in answering the research question through providing a reliable, accurate and relevant data. The disadvantage is that it needs better preparation and is more time-consuming than questionnaires. The most time-consuming part of it is connecting with interviewees and synchronising the time schedule.

For this research seven interviews were conducted. Four out of seven were with IT companies as one of them was a cloud computing provider. The rest were one with a university, one with a regional innovation system, and one with a trading company. All organizations are situated in Sweden. Two of the interviews were conducted by phone, and the rest were face-to-face. Among the interviewees were IT managers, university representatives, coordinators, consultants and developers. They were chosen due to their roles within the organizations. All of them were IT professionals at different levels in the organizational structure. This implies in-depth view on the influence of cloud computing over their organizations in terms of cost and security as well as insights of how to avoid the potential dangers. The cloud computing provider was chosen as to show both the customer`s and provider`s perspective on the research topic. The list with the interviewed organizations, their main activities, the respondent`s role, the duration of the interviews and their type is shown below in Table 1. For the interviews a semi-structured approach was used, allowing new questions to emerge in accordance with responses given. An interview guide was developed containing the main themes that were an object of exploration (appendix 1). The duration of the interviews was between 30 and 50 minutes. They were recorded and transcribed as to enable a more thorough analysis of the empirical material.

When the empirical material was collected, a data coding and analysis of the empirical data was conducted. Both of them were informed by theory, which means that the preliminary results from the literature review outlined the gap in extant research and what had already been explored. While the goal of this research was to examine the impact of cloud computing on organizations in regard to cost and security, all benefits and risks in this area had to be explored. Thus, on the one hand, the data analysis was focused on the empirical data related to the already examined in the previous research area of cost benefits and security risks. On the other hand, the analysis had to focus on the empirical data related to the extant research gap, namely exploring the cost risks and security benefits as well as suggestions for overcoming the risks. For this purpose the preliminary results were applied to the empirical data. The

interviews were firstly red and systematized into cost and security category. Then, they were categorized into benefits, risks and suggestions. Empirical statements were extracted which were to be used to answer the research question and fill the research gap.

Organization	Main activity	Respondent`s role	Duration	Type
University (A)		IT Strategy chief	52 min	Face-to-face
Regional Innovation System (B)	Process and engineering ICT companies, industries and universities	Project coordinator	49 min	Face-to-face
Company (C)	Publishing news and events	IT procurement manager	30 min	Phone
Company (D)	Providing software solutions for enterprises	System requirement consultant	35 min	Face-to-face
Company (E)	Providing network equipment and services	Technology business manager	40 min	Face-to-face
Company (F)	Providing web services, trading	Web developer	45 min	Face-to-face
Company (G)	Cloud services provider	Service manager	37 min	Phone

Table 1: Interviewed organizations

3.4 Methodology summary

For this research an exploratory design was taken. The reason is that this research aims to discover the relevant insights of how cloud computing affects organizations in terms of cost and security and more precisely what cost risks and security benefits it brings. The purpose of this research is not to provide exact enumerations or measurements for particular benefits and risks, but to focus on creating a detailed and complete picture of the cost and security impact of cloud computing by identifying all existing benefits and risks as well as to fill the existing gap in extant research. The gap in this case is the lack of research regarding cost risks and security benefits. Thus, the aim of the research does not implicate generation of a numerical data and rigorous quantitative analysis. Rather, it assumes findings based on subjective assessment of opinions. Hence, the qualitative approach was taken in this research. In accordance with the research design and approach taken, this research reviews the extant literature and uses it along with the empirical data collected from interviews for the purposes of data analysis. The preliminary sources used for this research include articles, books,

journals and information from web sites. They were synthesized and analysed so that the important results to be extracted for the objectives of data analysis. An empirical data was gathered via semi-structured interviews. Seven interviews were conducted with IT professionals from different kinds of organizations utilizing cloud computing. They were chosen because they were experienced enough to provide an in-depth view on the influence of cloud computing over their organizations in terms of cost and security as well as insights of how to avoid the potential dangers. One of the interviews was with a cloud computing provider. This gave an opportunity for exploration from both customer`s and provider`s perspective. A data coding and analysis of the empirical data was conducted. Both of them were informed by theory. The interviews were red and systematized into cost and security category. Then, they were categorized into benefits, risks and suggestions. The preliminary results were applied to the empirical data and empirical statements were extracted for the needs of the discussion section. The research limitations are put at the end of the paper (see 7.).

4. Results

This chapter presents the empirical findings obtained from the interviews. It contains opinions of interviewed IT professionals on the benefits and risks of cloud computing in terms of cost and security. It also includes their opinions on how the identified risks can be avoided.

4.1 Cost benefits

The interviewees` opinions regarding cost benefits of cloud computing are presented in a tabular form below:

Interviewee	Opinions in terms of cost benefits of Cloud Computing
A	Cost reductions are the key driver for a cloud computing implementation. A big role for the cost reductions within organizations plays elasticity of cloud services. The major part of cost reductions currently comes from reducing the staff, unlike as it used to be in the past when it used to come from the hardware and software. *"The cost nowadays is not so much about the hardware, it is about staffing. The better stable system you have that can be run and maintained by fewer staff that can be shared between each other, the cheaper it would be for everybody"*. Also, running some complex applications in the cloud is cheaper than developing the same by a university. *"At least half of the cost could be saved by outsourcing in the cloud for each application."* Cost savings from software licenses are more important for private organizations as they pay three times more for licenses than universities. Unlike large organizations, the small- and medium-sized gain more benefits as they do not have to invest in infrastructure and applications.
B	Cloud computing is highly beneficial for the companies *"as they no more need to invest huge amount of money for powerful servers in order to do their calculations."* Also, it leads to cost savings through significantly reducing the

	staff needed for support and monitoring. The investments for building a private cloud are justified only when it comes to large companies, which can afford it and actually need it because of their high power needs.
C	Cloud computing is cost-effective for organizations because it reduces the costs for initial investments. Also, it does not require customers to have their own servers in order to do business operations. *"Instead of purchasing computing power and software, you can use the applications you need directly in the cloud."* Moreover, the lack of internal servers allows customers to significantly reduce their costs for maintenance. Thanks to reliability and accessibility of cloud services companies get more competitive on the market. It is important for small and medium organizations to use cloud services in order to manage their operations and keep server and hosting costs at lower levels. *"Our company is using outsourced servers. It doesn't own any".*
D	When it comes to the cost savings, cloud computing is a very good option thanks to its flexible cost model. *"The good thing with the cloud is that instead of paying for computing resources that we don`t use, we can pay only for the time and scale we have used."* Customer does not have to pay all the time in order to use up-to-date software.
E	What makes cloud computing attractive for organizations is reducing the costs in terms of equipment and resources. *"Since we started using cloud services, the time of services and financial commitments are much lower."* It also reduces operational costs as many of the business operations are shifted to the cloud. The implementation of Cloud Computing is suitable in different extent for different organizations. *"For small and medium size business more useful is a third-party cloud solution and an in-house solution for big enterprise business."*
F	Increased stability, accountability, and predictability of cloud services stimulate the organizations` cost-effectiveness, making them more competitive. *"At present, we are satisfied with what our provider offers. For the same price you get more storage space, you have lower costs and maintenance, sharing with a greater audience is easier, and it is accessible from anywhere. The ratio of cost per GB stored is great too."* The point of utilizing cloud services depends on things such as kind of industry, company size, geographical spread of the company, data type, purpose of data, confidentiality, legal obligations, etc. *"But in general, I would say that cloud computing is most beneficial for small and starting businesses. That`s because they do not need servers and an IT department to do their operations. All computing resources they need are in the cloud."*
G	Cloud computing drives to decreasing the staff in organizations, resulting in cost savings. *"Cloud services reduce the administrative and operation costs. It*

	also reduces warranty costs and the lead times both delivery and support." Another benefit that reflects on cost is that the deployment of software updates is easy. *"Our company provides SaaS because the solutions we provide are accessible through a web browser by multiple clients, mostly small businesses."* In order to make a profit, the cloud provider has to do significant investments that are not affordable for small-sized companies. If a small company has enough capital, the best cloud service model is IaaS as it offers the entire spectrum of cloud services: storage, networks, processing, and applications.

Table 2: Opinions in terms of cost benefits of cloud computing

4.2 Cost risks

The interviewees` opinions regarding cost risks of cloud computing are presented in a tabular form below:

Interviewee	Opinions in terms of cost risks of Cloud Computing
A	A potential cost risk for organizations is the return of investments. It especially concerns organizations building private clouds. *"It is difficult to assess whether there will be a return of the investments you have done and for which period of time."*
B	Currently there are not any particular cost risks of cloud computing.
C	A real problem with cloud computing is that sometimes an application run in the cloud has less functionality in comparison with its equivalent in the standard software. *"In this case, you have to choose between less functionality and higher cost."* Then, organizations could not make cost savings from software.
D	There is concern related to the price of cloud services. Currently, the cloud market is unable to establish cloud prices that allow customers to do a precise cost calculation. *"It is early to have a price-clarity of the cloud services; at the moment the market has not mature enough to establish a market conform price in which we can project future cost."*
E	Assessment of the actual costs of the migration from a traditional platform to cloud is difficult. Hence, it is difficult for an organization to estimate what is the real cost benefit from this move. *"Actually it is not very easy to move to another cloud. If you want to change your provider, then you will have to pay additionally for that."*
F	Currently in the cloud market there are not pricing models that are sophisticated enough. This hampers customers to do an accurate calculation of the costs for cloud services which varies according to used applications and the case. This, along with the growing number of providers makes it difficult to estimate the

	appropriate provider according organization`s needs.
G	The problem with the provision of cloud services is how to estimate what an organization actually uses as a service out of the entire service consumption. This is important for calculation of the bill for each customer. *"It is also difficult to calculate the price for different services because there is not a proper model."*

Table 3: Opinions in terms of cost risks of cloud computing

4.3 Security benefits

The interviewees` opinions regarding security benefits of cloud computing are presented in a tabular form below:

Interviewee	Opinions in terms of security benefits of Cloud Computing
A	A benefit of cloud computing in terms of security is the data safety. *"Your data is more secured in the cloud. Whatever happens with your data, it is always out there in the cloud."* Thanks to cloud computing organizations reduce both financial and risk management`s efforts regarding security.
B	Despite ubiquitously shared big concerns regarding security, clouds *"are more secure than in-house data centers and servers."* Besides data safety, cloud computing provides easier security control to the customers in cases when they control the data. Instead of controlling several servers, customers direct their security efforts into one location. This enhances their security capabilities.
C	The main security benefits of cloud computing are the improved security software mechanisms and security maintenance. Cloud providers have the capacity to develop more sophisticated security software. In addition, cloud customers, especially of SaaS, do not have to care about the security maintenance as the entire maintenance is executed by provider. Besides, they get the latest security software updates automatically.
D	Data safety, better security control and reduced security costs make cloud computing very attractive for organizations. *"Having several backup copies of your data on different servers in the cloud, it is very difficult to lose it. Anyway, this has never happened so far."* Furthermore, cloud providers` measures to protect customers' data are being constantly improved.
E	Among the security benefits of cloud computing for organizations are the lower financial security commitments and faster data recovery. Cloud providers perform data recovery much faster than companies that do not use cloud services.
F	In case of a data intrusion, the data can be immediately transferred from one location (server) to another. It does not take as much time as in the traditional

	platforms. *"Users no longer have to wait until the data is available again."*
G	Cloud computing makes handling the data and its security much easier. *"Unlike traditional computing architectures, in the cloud you can handle the security systems support from a central location."* Also, the deployment of security software updates is easier.

Table 4: Opinions in terms of security benefits of cloud computing

4.4 Security risks

The interviewees` opinions regarding security risks of cloud computing are presented in a tabular form below:

Interviewee	Opinions in terms of security risks of Cloud Computing
A	Security risks of cloud computing mainly relate to legal issues and trust. *"Where is the data going? Who is responsible for it? Do I have the correct agreements? Do I know under which law is my data?"* There is a vagueness regarding where the customer data is stored and at which level is handled and secured. Other issues are the data loss and data confidentiality. Organizations that consider their data confidential do not host the sensitive data in cloud. Such organizations are usually large-scale businesses and non-commercial organizations.
B	Cloud computing is more secure than in-house data centres and servers, but *"the main problem with the clouds is called "trust"*. This problem has two aspects: business data and integrity. Many people do not trust cloud services because they feel insecure when do not know where exactly their information is stored. This especially relates to the business data - *"How do you take care of it?"* There is no problem when it comes to documentation processing or calculation services in the cloud, but many companies are concerned when storing an important business data there. The problem with business data security especially concerns the smaller organizations. *"It is difficult for smaller companies to understand and take care of security, while larger companies are able to calculate the risk for storing their data."* The other issue is the integrity. *"I would not suppose that companies like Microsoft or IBM would be impressed to put their business data in their own clouds. If you do not trust your own cloud, how can you serve it to me?"*
C	With the migration to the cloud some potential security risks occur. One of them is that *"in the cloud the business data may be exposed, and therefore, be stolen, deleted, or compromised."* Unfortunately, there are not regulatory frameworks that determine cloud computing`s legal agreements and standards on supranational level. Thus, security issues occur due to differences in the national legislations, which hinder or stop some organizations to move to the cloud.

	Another issue is that organizations are fully dependent on outsourced server and in a case of down-time they will stop operating. Thus, if that happens, an organization will have no other choice, but to wait for a solution from providers.
D	There is a reluctant use of cloud computing because of fear that a sensitive business intelligence data will be revealed and accessed by non-authorized parties. Data loss is what most organizations fear the most. But the practice shows that the actual security risk is the data intrusion. *"There will always be a risk of data breach, but not data loss."*
E	In cloud computing there is always a risk of unauthorized access to sensitive data and information by unknown users. A lack of clarity exists on how cloud provider hosts, manages, and protects customer's data. Also, it is difficult for cloud customers to understand what are their legal responsibilities regarding data security and whether they will be compensated in case of disaster. Because of the risk for data confidentiality cloud computing is not suitable for high security risk organizations, such as government, military, etc.
F	As the data is not stored in-house all information is accessible from any place around the world. *"In-house data used to be accessible via VPN or similar connections from outside the office at best giving a higher level of security."* Also, the risk of someone copying or corrupting the data is higher than in a closed system/server. *"You wouldn't even notice in case you have a data leak when using the cloud."* As cloud computing crosses the national boundaries, a very relevant issue with data confidentiality is the espionage and hacking by foreign corporations, even governments. Organizations for which cloud computing is not appropriate are those operating with a very sensitive data in areas such as secret services, weaponry, heavy machinery industry, drugs industry, etc.
G	Security depends on network, service and deployment models. As in cloud computing the data is centralized, *"it needs to be secured and handled in a smart way so it's available at any time."* Other security risks relate to a data transfer and access. A particular concern is the user access that requires an enhanced control. *"Improved handling with data separation is needed as cloud computing systems share resources."* The best solutions for businesses are private or hybrid clouds as the sensitive data is not exposed to third parties. In public cloud environment customers from a state with different laws may put the data in danger.

Table 5: Opinions in terms of security risks of cloud computing

4.5 Suggestions

During interviews the interviewees shared some opinions and suggestions regarding how the indicated risks can be avoided. These suggestions were important because organizations need understanding not only the benefits and risks of cloud computing utilization, but also what is the manner to avoid these risks.

In terms of cost the interviewees outlined several risks. Almost all of them relate to the difficult cost assessment due to the lack of sophisticated cost models. Therefore, according to respondent F, *"new and more accurate cost models should be developed which will allow customers to do a precise calculation of their costs for cloud services."* Respondent G shared the opinion that more improved business and cost models should be developed so that cloud providers to be able to calculate better the costs per particular service and user. The cloud market also needs more competition that should be stimulated. According to respondent F, on the current cloud market there is not a sufficient number of providers and their growing number will make the prices for cloud services fall. In terms of applications` functionality, before moving to the cloud organizations should carefully consider whether applications in the cloud have the same functionality as the ones in the standard software (Respondent C).

Among the major security risks outlined by interviewees are data loss and data breach. According to respondent A, each organization needs a serious analysis regarding what data should be stored in the cloud due to its importance and confidentiality. Respondent E stated that *"organizations should keep the most sensitive data in-house and restrict access by investing in high security level network equipment."* Respondent C commented that in a case of down-time, his company might have to change its strategy and start hosting some of its essential applications on internal server (Private cloud). All interviewees shared the opinion that hybrid cloud is the best cloud type for small- and medium-sized organizations as a perfect balance between the sensitive data issue and cost savings. The most appropriate for large organizations is private cloud. Regarding the protection of data confidentiality respondent G stated that the technology should be constantly developed including a better data encryption and improved firewalls.

Another issue related to the risks for security in the cloud is trust. According to respondent F *"There is never a chance to avoid risks, no matter if in-house or cloud computing systems."* But he highlighted that the transparency should be increased. This, in turn, will increase the trust in cloud computing. The problem is that many organizations do not have enough information in terms of what cloud computing is, what it has to offer, and what cloud providers offer as security measures. This leads to a potential disappointment of utilizing cloud computing. Organizations should have enough information in order to understand what security measures are taken by the cloud provider. This will help them make the best choice possible between different providers.

The lack of interoperability and international security standards poses big risks for security in the cloud. Respondent C argued that the security risks of cloud computing would be hardily overcome without resolving these issues. According to him cloud computing needs establishing universal interoperable and security standards that cross the national boundaries. Therefore, legislation on supranational level should be conducted.

5. Discussion

The purpose of this thesis has been to explore the impact of cloud computing on organizations in terms of cost and security by answering the following research questions: *What are the cost benefits of cloud computing for organizations and are there any cost risks?; What are the security risks of cloud computing for organizations and are there any security benefits?*

The previous chapter presented the empirical findings obtained from interviews with IT professionals in terms of the benefits and risks of cloud computing for organizations in cost and security aspect. As a result, firstly, this research has identified several findings that are not addressed in the extant research. They relate to the cost risks and security benefits of cloud computing. Thus, the research extends existing knowledge and contributes to the area of research regarding the impact of cloud computing on organizations. Secondly, it also contributes by presenting some major implications as well as suggestions on how to avoid cost and security risks identified.

5.1 Cost impact

Previous research has shown that the attractiveness of cloud computing mainly comes from its cost effectiveness and more precisely cost savings. One of the features of cloud computing that leads to cost savings is elasticity. Even in cases when buying cloud services is more expensive than buying a server for similar operations and period of time, finally those services cost cheaper thanks to the elasticity (Armbrust at al., 2009). Elasticity has been pointed out by respondents A and D as a very important feature that had made them move to the cloud. Cloud computing has a flexible cost model that allows organizations to pay only for the time and scale that they actually use, instead of paying for computing resources they do not use (Respondent D).

Other cost benefits outlined in previous research are the cost savings from hardware, software and infrastructure (Miller, 2009; Goncalves and Ballon, 2011). The lack of initial investments for hardware is a big financial benefit due to the fact that organizations no longer need to purchase high-powered and high-priced computers to run applications as those applications are in the cloud (Miller, 2009). Respondent B has stated that organizations do not have to invest a huge amount of money for powerful servers in order to do their calculations. This point of view has also been shared by respondents C and E. The same applies also for the investments for software, where organizations can use applications directly in the cloud instead of installing them on their own machines (Miller, 2009). According to respondent A, at least half of the cost of each application can be saved through outsourcing in the cloud. Also, with decreasing the needed hardware, software and infrastructure, the costs for their maintenance also decrease (Miller, 2009; Goncalves and Ballon, 2011). This statement has also been shared by respondent C, who has stated that with reduction of the amount of internal servers the costs for maintenance also decrease (Respondent C). All aforementioned potential expenses can be used by organizations for other operations, for instance marketing and innovation, resulting in higher profits.

There are also other factors that reflect positively upon the organizations` income through enforcing their productivity and effectiveness. As such, the previous research has outlined increased computing power, easier group collaboration, universal access to documents,

improved compatibility between operating systems, and improved document format compatibility (Miller, 2009). Empirical findings have presented some additional factors. Increased stability, accountability, and predictability of cloud services stimulate the cost-effectiveness by making organizations more competitive (Respondent F).

While previous research has shown that the main cost savings come from hardware, software and infrastructure, the empirical findings have displayed that currently the cost savings are mainly associated with staff reduction. Respondent A has argued that nowadays the cost is not so much about the hardware and software, it is about staffing. In other words, nowadays for organizations that utilize cloud computing the cost savings mainly come from reducing the operational and administrative costs (Respondent A, B, and G).

Previous research has shown that cloud computing in its cost aspect is most appropriate for small and medium-sized organizations. This is due to cost benefits such as little initial investments, lower cost of ownership of resources and ability for elimination of the software management activities (Goncalves and Ballon, 2011). In addition, smaller organizations do not have the budget and resources to build their own data centers and to develop and maintain their own applications (Miller, 2009). The cost of utilizing cloud services is higher than in-house data centers, but only when it comes to large-sized organizations (McKinsey & Company, 2009). Similar point of view has been shared by respondents. Small and medium organizations gain more benefits because they do not need their own infrastructure, applications and IT department in order to do their operations (Respondent A, C, and F). The investments for building private clouds are justified only when it comes to large organizations that can afford them and actually need them because of their high power needs (Respondent B and E). Cloud computing is profitable for provider, but requires significant investments that are not affordable for small-sized organizations (Respondent G).

In previous research little effort has been made in examining the cost risks which cloud computing brings to organizations. As a result of the research conducted several cost risks have been identified. The main cost risk that has been identified and from which the rest emanate is the lack of accurate and sophisticated cost models on the current cloud market. This risk makes the cost estimation of cloud computing utilization difficult. At present the market is not mature enough to establish a market conform price through which organizations can project future cost (Respondent D). As a result, it is difficult for organizations to assess whether to move to the cloud or not. This risk has different aspects. First, it is difficult for organizations which consider moving from traditional systems to the cloud to estimate the return of their initial investments, especially in a long-term perspective (Respondent A and E). Organizations which are already utilizing cloud computing also have cost difficulties if they want to move to another cloud. As respondent E has stated, transition from one to another cloud is accompanied by additional costs. Second, as the costs for cloud services vary according to used applications and the use case, this additionally embarrasses their accurate calculation by customers. This along with the growing number of providers makes it difficult to estimate the best provider`s offering (Respondent F). Third, from provider`s perspective the calculation of the costs is difficult as well. Because of the lack of proper cost model providers hardily estimate what the user actually uses as a service from the entire service consumption. This embarrasses calculation of the bill for each customer (Respondent G). There is also a risk

some of applications in the cloud to have less functionality in comparison with their equivalents in the standard software. Then, the organizations could not make cost savings from software (Respondent C), meaning that they may eventually have to run other more expensive applications.

Empirical findings have presented some suggestions by IT professionals regarding how to avoid the cost risks shown above. There is a necessity of developing new and more accurate cost models which would allow customers to do a precise calculation of their costs for cloud services (Respondent F). More improved business and cost models are needed which allow better calculation of the costs per particular service and user (Respondent G). On the other hand, competition on the cloud market should be constantly stimulated which will lower the prices for cloud services (Respondent F). Before moving to the cloud, organizations should consider carefully whether cloud applications have the same functionality as their equivalents in the standard software (Respondent C).

5.2 Security impact

Previous research has displayed that the main concerns regarding cloud computing utilization relate to security (Pearson, 2012). Several security risks have been reviewed in previous research and all relate to the main organizations` fears of utilizing cloud computing - data loss and data breach. The security risks include unwanted access to sensitive and confidential information, inadequate data deletion, compromise of the management interface, backup vulnerabilities and isolation failure (Pearson, 2012). Organizations` fears concern especially the sensitive business data that can be exposed in the cloud and subsequently copied, stolen, deleted, or compromised. This risk is higher in the cloud than in in-house environments (Respondent C and F).

Unlike previous research, the empirical findings have shown some differences regarding security risks from a practical point of view. Although organizations consider data loss as the biggest security risk of cloud computing, according to respondent D this risk does not exist. According to him, there will always be a risk of data breach, but not data loss.

Other security risks shown in previous research are gap in security, vendor lock-in, missing assurance and transparency, and inadequate monitoring. In cases when cloud provider has a responsibility for the security, there is a risk of inadequate security handling and lack of clauses ensuring the level of security provided (Pearson, 2012). This in turn, according to respondents A and B, leads to another essential obstacle for cloud computing utilization by organizations – trust. They have stated that what actually stops organizations to utilize cloud services are not the security risks itself, but the lack of trust and integrity. As their organizations have never faced security problems in the cloud, they consider the security problems as rather potential than real, but the lack of trust still exists. There is a vagueness regarding where customer data are stored and at which level is handled and secured (Respondent A). It is difficult for cloud customers to understand which are their legal responsibilities regarding data security and whether they would be compensated in case of disaster (Respondent E).

Empirical findings have displayed an essential obstacle for eliminating security risks. At present, there are not regulatory frameworks which determine cloud computing`s legal

agreements and security and interoperability standards on a supranational level. Thus, security risks are additionally exacerbated by differences in national legislations and this either hinders or stops some potential cloud customers to migrate. As cloud computing is crossing the national boundaries, a very relevant issue related to data confidentiality is the espionage and hacking by foreign organizations and governments (Respondent C and F). Recently many scandals and affairs of leak and data hacking have occurred raising the question about the integrity of cloud providers and governments, and how these issues will be resolved on a supranational level. That makes the security question of cloud computing more pertinent than ever.

In extant research little effort has been focused at examining the security benefits of cloud computing for organizations. This research has aimed to explore them and as a result several security benefits have been identified. First and foremost, cloud computing increases data safety. As respondent D argues, customer`s data have several backup copies on different servers allowing its quick restoration in a case of disaster. According to respondent B, clouds are more secure than in-house data centers and servers. That`s because most of the organizations that build in-house data centers cannot afford to install a sufficient number of servers that guarantee the safety of their data. Empirical findings have shown some additional security benefits for organizations. First, centralization of cloud computing provides easier security control to customers of PaaS and IaaS models. Instead of controlling separately several servers customers direct their security efforts into one location and this enhances their security capabilities. On the other hand, customers of SaaS do not have any security commitments. In addition, the centralization of cloud computing also allows better handling of the security systems support by cloud providers (Respondent B, C, D and G). Second, organizations that implement cloud services have lower financial commitments for Risk Management, security maintenance and support (Respondent A, D and E). That`s because the security maintenance and support are executed at different extend by cloud provider. This means that the customers of SaaS do not have any of those financial commitments. Third, the security maintenance and security software mechanisms are improved much better than the traditional systems (Respondent C). Thus, the cloud provider always has a better potential and tools on executing the security control than an organization that owns a data center. Fourth, cloud services provide faster data recovery and transfer. Unlike in traditional environments, organizations that utilize cloud computing do not lose money and time awaiting their data to be restored or transferred to other location in a case of intrusion (Respondent E and F).

Empirical findings have shown some suggestions regarding how to avoid the security risks mentioned above. When it comes to data loss and confidentiality organizations should conduct a serious analysis regarding which data should be stored in the cloud. This requires a preliminary analysis of the security trade-offs which a particular provider allows. Cloud providers should constantly develop the data protection mechanisms, including better data encryption and improved firewalls (Respondent G and A). In terms of which cloud deployment model is most appropriate in security aspect, interviewed professionals have shared the common opinion that small- and medium sized organizations should orient towards hybrid cloud as a perfect balance between the sensitive data issue and cost savings. For increasing the trust in cloud computing a better transparency is needed. This relates to the

security measures taken by cloud providers and the rights of cloud customers, meaning that providers have to develop more user-friendly service level agreements. Organizations should have enough information in order to be able to make the best choice between different providers (Respondent F). Last but not least, the security risks of cloud computing would be hardily overcome without resolving the problem with the lack of interoperability and international regulatory frameworks for security standards (respondent C), meaning that a legislation on a supranational level should be conducted in order to establish ubiquitous interoperable and security standards which cross the national boundaries.

6. Conclusions

This thesis has examined the impact of cloud computing on organizations in terms of cost and security. Previous research has already shown that the main attractiveness of cloud computing for organizations is its cost effectiveness, whilst the major concern relates to the risks for security. However, little effort has been focused at critically examining the cost risks and security benefits of cloud computing adoption. As a result, the extant research is problematic in that it fails at addressing these issues. This research has addressed these issues through identifying the cost risks and security benefits which organizations experience while utilizing cloud computing. The major cost risk which has been identified is the lack of accurate and sophisticated cost models on the current cloud market. The security benefits identified include increased data safety, security centralization, lower financial commitments for Risk Management, security maintenance and support, improved security software mechanisms and maintenance, and faster data recovery and transfer.

This research has shown several major implications. First, at present organizations consider staff reduction, and respectively reduction of the operational and administrative costs which it brings as the most essential cost benefit. Second, cloud computing is better for small- and medium-sized organizations. Also, hybrid cloud is considered as the most appropriate cloud deployment model for them, representing a perfect balance between the sensitive data issue and cost savings. Third, avoidance of the cost risks for organizations requires developing new and more accurate cost models for precise calculation of the costs for cloud services, as well as an increased competition on the cloud market which should be stimulated. Fourth, the security risks of Cloud Computing can be avoided through serious analysis by organizations regarding which data should be stored in the cloud, developing advanced data protection mechanisms, and improving the transparency regarding security measures taken by cloud providers. Also, there is a necessity of establishing international regulatory frameworks and interoperable and security standards on a supranational level as an essential prerequisite for secure cloud computing environment.

7. Limitations

This research is limited in that it includes a small number of organizations and only one provider of cloud services. It lacks more large-sized organizations as it is more difficult to get in touch with them and conduct an interview. Also, the research is conducted within the boundaries of one single country, which due to the ubiquitous character of cloud computing constitutes a limitation. Therefore, it can offer only a partial view on the impact of cloud computing on organizations in terms of cost and security. Hence, further research is needed which will explore more deeply the impact of cloud computing on organizations from a provider`s perspective. This concerns especially the security issue both in its legal and technical aspects.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A, D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2009). *Above the Clouds: A Berkeley View of Cloud Computing*. *Electrical Engineering and Computer Sciences*, University of California at Berkeley.

Boss, G., Malladi, P., Quan, D., Legregni, L. & Hall, H. (2007). *Cloud Computing*. IBM Corporation.

Bryman A. and Bell E. (2007). *Business research methods*. Second edition, Oxford University press.

Cloud Security Alliance. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing*. https://cloudsecurityalliance.org/csaguide.pdf Retrieved date: 24-05-2012

Cloud computing security alliance. (2010). *Top Threat of Cloud Computing* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf Retrieved date: 03-06-2012

Crawford I. (1997). *Marketing Research and Information Systems*. *Food and Agriculture organization of the UN*. http://www.fao.org/docrep/W3241E/W3241E00.htm Retrieved date: 26-05-2012

Greenwood, D., Khajeh-Hosseini, A., Smith, J. & Sommerville, I. (2011). *The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoption in Enterprise*. Cloud Computing Co-laboratory, School of Computer Science, University of St Andrews, UK.

Goncalves, V. & Ballon, P. (2011). *Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Platform-as-a-Service models*. Telematics and Informatics. Vol. 28 (2011), 12-21.

Hosseini, A. K., Sommerville, I. & Sriram, I. (2010). *Research Challenges for Enterprise Cloud Computing*. Unpublished, http://arxiv.org/abs/1001.3257 (2010).

IDC. (2013). IDC Cloud Reseach. http://www.idc.com/prodserv/idc_cloud.jsp Retrieved date: 15-04-2013

Kothari, C. R. (2004). *Research Methodology*. Second Revised Edition. New Age International Publishers.

McAfee, A. (2011). *What Every CEO Needs to Know About the Cloud*. Harvard Business Review.

Miller, M. (2009). *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online*. Que Publishing.

McKinsey & Co (2009). *Clearing the Air of Cloud Computing*. http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/McKinsey_Cloud%20matters.pdf Retrieved date: 03-06-2012

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology, U.S. Department of Commerce. (Special Publication 800-

145). http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf Retrieved date: 25-05-2012

Pearson, S. (2012). *Privacy, Security and Trust in Cloud Computing*. Springer.

Rosenthal, A., Mork, P., Li, M., Stanford, J., Koester, D., Reynolds, P. (2009). *Cloud computing: A new business paradigm for biomedical information sharing*. Journal of Biomedical Informatics. http://www.sciencedirect.com/science/article/pii/S1532046409001154

Velte, A. T., Velte, T, J. & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach*. McGraw-Hill.

Theme 1: The cost impact of cloud computing

This theme relates to how cloud computing affects organizations in terms of cost, including the cost benefits and risks. It comprises example questions like: According to you what are the benefits of cloud computing adoption in terms of cost? What are the risks?

Theme 2: The security impact of cloud computing

This theme relates to how cloud computing affects organizations in terms of security, including the security benefits and risks. It comprises example questions like: What are the risks of cloud computing adoption in terms of security? Are there any benefits?

Theme 3: Recommendations for risk avoidance

This theme includes questions regarding how the cost and security risks mentioned by interviewees could be avoided. It comprises example questions like: According to you how could cost and security risks be avoided? Can you give any suggestions? Are there organizations for which the cloud computing adoption is not recommendable? Which type of cloud is most appropriate for the organizations according to their size and business model? How do you see the direction of development of cloud computing in near future?