Organizational Cloud Security and Control: a Proactive Approach

Abstract

Purpose: The purpose of this study is to unfold the perceptions around additional security in cloud environments by highlighting the importance of controlling mechanisms as an approach to the ethical use of the systems. The study focuses on the effects of the controlling mechanisms in maintaining an overall secure position in the cloud and the mediating role of the ethical behavior in this relationship.

Research Methods: The methods applied for this research, followed a case study about the adoption of managed cloud security services as controlling mechanisms, as well as a large scale survey with the views of IT decision makers about the effects of such an adoption to the overall cloud security.

Findings: The findings indicate that there is indeed a positive relationship between the adoption of control mechanisms and the maintenance of overall cloud security, which increases when the users follow an ethical behavior in the use of the cloud. A framework based on the findings is built suggesting a research agenda for the future and a conceptualization of the field.

Limitations of the study: One of the major limitations of the study is the fact that the data collection was based on the perceptions of IT decision makers from a cross-section of industries; however the proposed framework should also be examined in industry-specific context. Although the firm size was indicated as a high influencing factor, it was not considered for this study, as the data collection targeted a range of organizations from various sizes.

Originality/value: This study extends the research on IS security behavior based on the notion that individuals (clients and providers of cloud infrastructure) are protecting something separate from themselves, in a cloud-based environment, sharing responsibility and trust with their peers. The organization in this context is focusing on managed security solutions as a proactive measurement to preserve cloud security in cloud environments.

Keywords: cloud, IS security, usage control, ethical behavior, IS misuse intention

1. Introduction

There is an emerging interest in cloud computing utility model within organizational landscapes. The cloud has increased in use over the last decade, driven by cheaper computation, storage, and increasingly available bandwidth. The enormous potential the cloud environment provides as part of the digitalization process increased the interest in the adoption of cloud services by individuals and organizations worldwide. The increasing acceptance, usage, and adoption of cloud services have raised issues related to the economic and business models around them, as well as questions about how moving to cloud platforms pays-off the initial investments and meets the initial intended purposes. Cloud adoption and the adoption of services provided in cloud-based platforms (e.g., security services) in general have significant impacts on organizational landscapes (e.g., decreasing costs, increasing productivity, transforming traditional business models, providing efficient and flexible solutions to meet the increasing IT demands, etc.).

A critical aspect of ensuring the sustainability of the cloud utility model is the development and delivery of efficient control systems for maintaining the overall security position of the systems and the infrastructure. Cloud infrastructure and security vendors often try to ensure the protection of the cloud through the development of managed additional security services. Security services are provided in different forms based on the deployment model of the cloud, e.g., for SaaS as an add-on application, for PaaS at the runtime of the OS or IaaS when the cloud vendor provides security of the infrastructure as well. Security services in cloud environments include anti-virus applications, authentication mechanisms, anti-malware, anti-spyware, security management and intrusion detection, as well as other security and control functions for organizations or individual cloud users.

The interesting aspect of cloud security solutions compared with traditional server installations comes with the ethical use of the systems and the shared responsibility between all clients and the infrastructure provider. Failure of one client to efficiently use the cloud; increases the risk of other clients and also the infrastructure provider. To ensure, and proactively protect their resources and assets in cloud environments, organizations seek for controlling mechanisms for maintaining a safe position of their organization while working in cloud infrastructures. This research focuses on the adoption of additional cloud security services as a mechanism to proactively control and maintain the overall security status in the cloud.

With this study, we aim to explore the cloud security challenges and requirements by examining the adoption of controlling mechanisms as a proactive approach for preserving the overall security and ethical use of the cloud. The research focuses on the direct and indirect effects of the controlling mechanisms to the overall security position of the organization in the cloud. A conceptual framework has been created based on the combination of the theoretical background as well as the interview and survey data. Our contribution in the area provides an academic base for researchers on cloud services and more specifically cloud security services and their adoption in organizations.

2. Background

This study extends the research of security behavior based on the notion that individuals (clients and providers of cloud infrastructure) are protecting something separate from themselves, in a cloud-

based environment, being responsible for the shared cloud infrastructure and trusting their peers. The organization in this context is trying to proactively control the usage of the cloud by adopting additional security services (instead of developing in-house security solutions or additionally to their in-house developed solutions) to maintain its "safe" overall presence and also protect others in cloud environments.

While Information Systems (IS) Security research analyses the behaviors, decisions, and motivations of individuals (employees) following security compliance, regulations or even ethical behavior around IS use, so far the research towards this direction is focusing on the organizational level and the individual level of home users. Organizations are investigated in the context of their employees; however, they should also be examined at management (decision-making) level more precisely. Thus, this study will focus on the security behavior on an organizational level particularly.

Initially, we review studies around challenges identified for the cloud, user behaviors, and the associated security attributes, namely shared responsibility, trust, and security management. We also provide an overview of the theoretical background of IS Security and the associated behavioral theories. We do that by exploring aspects around proactive attitudes in IS security research as the usage and security control (controlling mechanisms), the ethical use and misuse intentions (ethical use) and ways of maintaining a high-security status for the cloud (overall security position). Building on these aspects, we develop a holistic view of the way proactive attitudes are formed and triggered. By studying these concepts, we propose an approach (framework) of the way organizations proactively maintain their overall security in the cloud.

2.1. Security Challenges in Cloud Environments

Cloud computing has generated significant emerging interest in both academia and industry, although it is almost a decade since the concept initially appeared (Armbrust et al., 2010). Cloud computing concept applies the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources (Takabi et al., 2010). A commonly accepted definition of cloud computing is provided by NIST (Mell and Grance, 2011) as *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes the availability and is composed of five essential characteristics, three delivery models, and four deployment models".* Although this definition is commonly accepted, there are still ongoing discussions on how cloud differs from other computing models and how these differences affect its adoption (Shahzad, 2014).

During the last years, companies and organizations have increasingly adopted cloud-based solutions as a means to reduce the burden of managing IT infrastructures (Marston et al., 2011) and simultaneously take advantage of the provided computational resources (e.g. networks, servers, storage, applications and services) offered by cloud providers on an on-demand basis (El-Gazzar, 2014; Garrison et al., 2012). However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a massive failure (Shahzad, 2014). Several studies indicate that security, privacy, and trust in shared cloud environments, also require shared responsibility and ethical use of the resources (Ali et al., 2015;

Alshamaila et al., 2013; El-Gazzar, 2014; Mezgár and Rauschecker, 2014; Zissis and Lekkas, 2012) for preserving the full potential of the cloud utility model.

The major security challenges of cloud computing for organizations can be considered as the shared responsibility, trust, and organizational security management (Rodero-Merino et al., 2012). Understanding the security and privacy risks in cloud computing and developing efficient and effective solutions appear as critical determinants for its adoption and success (El-Gazzar, 2014; Rodero-Merino et al., 2012; Takabi and Joshi, 2012). Although clouds entail multiple economic and operational benefits for customers, their unique architectural features also raise security concerns which can be prevented if they are proactively avoided (Ali et al., 2015; Vaquero et al., 2011; Zissis and Lekkas, 2012).

Shared Responsibility: The cloud computing model is based on the perception that providers and customers must share the responsibility for security and privacy for themselves and the other cloud tenants (Buyya et al., 2009; Takabi et al., 2010). For Takabi et al. (2010) the way the responsibility for privacy and security is shared between consumers and cloud service providers differs between the various delivery models. The clients and cloud providers share the responsibility according to the three delivery models of the cloud (Takabi et al., 2010).

- In SaaS (Software-as-a-Service) models, the security responsibility is mostly for cloud providers as they have to protect the application services of their users. This approach is more relevant to the public than the private cloud environment as the clients follow more strict security requirements than in private cloud.
- In PaaS (Platform-as-a-Service) model, users are responsible for the applications that they build and run on top of the platform, while cloud providers are responsible for protecting the others from these applications.
- In IaaS (Infrastructure-as-a-Service) model, users secure and share responsibility for operating systems and applications, whereas cloud providers must provide low-level essential protection for the data of their users.

Shared responsibility in multi-tenant clouds falls on the cloud providers' side as they have the responsibility to manage resource utilization more efficiently by partitioning a virtualized, shared infrastructure among various customers (Takabi et al., 2010). However, from a client's perspective, using a shared infrastructure is challenging regarding resource sharing and available protection mechanisms in place (AlZain et al., 2012; Buyya et al., 2009; Zissis and Lekkas, 2012).

Trust and Accountability: Trust and accountability are often discussed from different perspectives (Huang and Nicol, 2013). These perspectives could be: a)the ability to develop positive associations and relationships with providers (Garrison et al. 2012), b) establishing trust and reputation systems (Habib et al., 2012), c) data stewardship and preventive controls (Pearson, 2013), d) access control and trust management policies (Zhang and Joshi, 2009) or even e)heterogeneity among cloud provider security policies (Takabi et al., 2010). In the cloud, multiple service providers coexist and collaborate in providing various services; however, their security approaches and privacy

mechanisms usually differ (Takabi et al., 2010) and also the level of trust and relationships between the clients of the cloud infrastructure providers (Ali et al., 2015; Rebollo et al., 2015; Shahzad, 2014; Subashini and Kavitha, 2011; Vaquero et al., 2011; Zissis and Lekkas, 2012).

Trust and accountability issues on the cloud have more space for further investigation regarding how the relationships of clients and infrastructure providers have developed and the incentives for adopting cloud security services (Armbrust et al., 2010; Pearson, 2013; Rea et al., 2012). Additional exploration and development of trust frameworks can provide efficiency in capturing a generic set of parameters required for establishing trust and managing the evolving trust and the interaction/sharing requirements. Another important aspect is the integrated, trust-based, secure interoperability that helps establish, negotiate, and maintain trust to adaptively support policy integration (Takabi et al., 2010; Takabi and Joshi, 2012; Zhang and Joshi, 2009).

Organizational Security Management: Security literature in the field of IS has developed models and theoretical background around security management and information security life-cycle models (Anderson and Agarwal, 2010; Bulgurcu et al., 2010; Goodall et al., 2009), however this theoretical background changes when enterprises adopt cloud computing. Shared responsibility and governance can become a significant issue if not adequately addressed in cloud transitions (Takabi et al., 2010).

According to the report published by the Cloud Security Alliance (CSA, 2015), IT professionals see the top security issues facing their organizations as malware (63%), advanced persistent threats (53%), compromised accounts (43%), and insider threats (42%). Specific cloud attacks within these categories can take many forms and take advantage of multiple security weaknesses involving insecure storage, shared workloads, communication issues, protocol vulnerabilities, insecure networks, shared workspaces, unveiling the nature of VMs, hypervisor exploits, among others (Vaquero et al., 2011). Additionally, the organizations are concerned about risk and management issues encountered as less coordination within client organizations, dependence on external entities (questioning responsiveness to security incidents), data leakage within multi-tenant clouds and resiliency issues such as their provider's economic instability and local disasters, insider threats and tenants highly targeted attack victims in multi-tenant environments (Wang et al., 2015).

Following these concerns, research should focus on developing best practices and standards to ensure the deployment and adoption of secure clouds (Kerschbaum, 2011). These issues necessitate proactive approaches available from the security industry. However, the global nature of cloud computing increases so does the complexity of such offerings. In our study, we explore the solution of add-on security managed services provided by a cloud infrastructure vendor to the tenants and the intentions and decision determinants of the tenants to adopt this solution in their cloud environment. The following sections present the theoretical framework and the research design for this study.

2.2. IS Security Research

To frame out our research, we initially reviewed the Information Systems (IS) Security literature for the identification of relevant concepts. IS Security research often focuses on security phenomena related to the behavior of the individuals or organizations from a reactive perspective. Prior security studies provide solutions and explanations of how the security issues can be solved and showcase examples to avoid. However, recently there is a growing interest in IS Security area about proactive

approaches, where the individual and the organizations develop insight for their behaviors to protect, control or plan their IS environment from malicious attacks or breaches of security. We reviewed the associated studies with a particular focus on security behaviors. We aimed to build a theoretical framing for our empirical research on the organizational security for cloud environments and to emphasize the effects of the solutions targeting cloud security purposes. The IS research is focusing on three prevailing areas (Table 1) as precautionary measurements for maintaining systems security, namely: a) systems usage control, b) the ethical use of the systems and c) building an overall security attitude (i.e., through understanding, security training, awareness, education programs, etc.).

Table 1. Construct generation from IS Security Literature

<Table 1 here>

An essential part of IS Security research is based on the organizational theory of Ouchi (1979) which explains the controls that should be in place as a precautionary organizational measurement (Boss et al., 2009). The controls are analyzed at an individual level as control of one's own self (Chen and Zahedi, 2016; Hu et al., 2015; Liang and Xue, 2010), but also at a social level (Chen and Zahedi, 2016; D'Arcy et al., 2009; Hu et al., 2015; Liang and Xue, 2010), where ethical behavior should be promoted for maintaining overall IS Security. In the case of protective and controlling precautionary measures, users' awareness of computer monitoring has a significant effect on users' perceived certainty and severity of sanctions (D'Arcy et al., 2009). These measures provide empirical support for monitoring and controlling computing activities as auditing the use of IS assets can avoid the IS misuse intention (D'Arcy and Herath, 2011). Organizations often use the security policies to proactively safeguard their IS and their information resources (Doherty et al., 2009; Herath and Rao, 2009). The influence of monitoring practices was stronger than any of the other security countermeasures, suggesting that computer control is a useful mechanism for convincing users that IS misuse should be avoided, as well as such behaviors and intentions (Anderson and Agarwal, 2010).

Information Security research is also formed around predictions of the 'IS misuse intention.' This approach focuses on an individual's intention to perform a behavior (Magklaras and Furnell, 2001) defined by the organization as a misuse of IS resources. Studies in this area of focus use the Theory of Planned Behavior (TPB) of Ajzen (1991) for predicting with the use of perceived behavioral control the actual behavior. The domain of IS misuse is quite varied, ranging from actions that are unethical and inappropriate or illegal (Baskerville et al., 2014; D'Arcy et al., 2009). The study of D'Arcy et al. (2009) attempted to examine a range of IS misuse behaviors in various contexts by introducing a set of scenarios of misuse. Investigating the attitude toward unethical IS use is required for understanding ethical background associated with the IS use. The unethical IS use increases the likelihood of causing harm to others (Baskerville et al., 2014; Chatterjee et al., 2015) and can result in harm by decreasing an organization's revenues and subsequently the belief that technology should not be used to harm others (Chatterjee et al., 2015; D'Arcy et al., 2009). The studies towards this direction aimed at understanding employees' security behaviours, as systems' misuse (D'Arcy et al., 2009; Herath and Rao, 2009), security awareness (D'Arcy et al., 2009; Pahnila et al., 2007) and compliance with organizational regulations and security standards relevant to the industrial sectors (Chen et al., 2012; Herath and Rao, 2009; Pahnila et al., 2007; Siponen and Vance, 2010). In the area of precautionary countermeasures, the security education and training are highly commented as a

precaution for security. The results on the impact of security education and training programs are particularly noteworthy (D'Arcy et al., 2009; Tsohou et al., 2012) followed by evidence that user awareness of these programs can help reduce IS misuse due to their ability to increase perceptions of the certainty and severity of punishment for such behaviour (D'Arcy et al., 2009; Puhakainen and Siponen, 2010).

Maintaining an overall security position and building the security awareness of the organizations is studied with a focus on precautionary control measurements and also the employees' overall knowledge and understanding of potential issues related to information security and their ramifications (Bulgurcu et al., 2010). Beyond general security precautions, organizations have specific expectations for their employees for awareness as an employee's knowledge, and understanding of the requirements prescribed in the organization's security policies (Puhakainen and Siponen, 2010; Siponen and Vance, 2010). Employees' overall security awareness is an important part of effective control and security management programs (Cavusoglu et al., 2009; Yoon and Kim, 2013) building confidence and alertness with security issues (LaRose et al., 2008). Overall Security Awareness is analyzed mostly conceptually in various studies (Siponen et al., 2006; Siponen and Vance, 2010; Vance et al., 2012; Yoon and Kim, 2013) suggesting methods to enhance the system control based on several theoretical models and perspectives. The importance of information security awareness education and training is highlighted as a crucial point for increasing IS Security (Bulgurcu et al., 2010; Tsohou et al., 2012). The organizations can use three security countermeasures for maintaining overall security according to D'Arcy et al. (2009): a) user awareness of security policies (awareness programs); b) security education, training, and c) system control monitoring, which in turn reduce users' IS misuse intention (Bulgurcu et al., 2010; D'Arcy et al., 2009; Tsohou et al., 2012).

From a general point of view, IS security theoretical background shows that organizations try to explain the employees' attitudes towards IS security choices (Bulgurcu et al., 2010) and to predict IS security behaviour (Cavusoglu et al., 2009; Gal-Or and Ghose, 2005; Herath and Herath, 2008; Pavlou and Fygenson, 2006), as well as understanding phenomena and conditions related to the likelihood (increase/decrease) to adopt measures or technology to solve their security problems (Ba and Pavlou, 2002; Hsu et al., 2012; Lee et al., 2016; Pavlou and Fygenson, 2006). Our study is also following this direction, as we focus on the motivation of organizations to adopt technological solutions for solving their security problems on the cloud as a precautionary measurement.

2.3. The research framework and propositions

This section presents the framework developed for the study. The framework proposes that the controlling mechanisms will have an impact on the overall security position of the organization in the cloud both directly and also indirectly through the ethical use of the systems. Using literature support, we developed the initial constructs and propositions relating to these variables, and we propose the expected relationships among the controlling mechanisms, the ethical use and overall security position as our initial framework for research.

Figure 1: The research framework

<Figure 1 here>

The organization in the framework is proactively seeking to adopt controlling mechanisms for the cloud and therefore adopts/intends to adopt additional cloud security services as a controlling mechanism. The controlling mechanisms will maintain and promote the overall security position of the organization in the cloud. However, the overall security position in the cloud will be stronger if added to the controlling mechanisms; the ethical behavior is promoted. Therefore we follow three propositions which we investigate further in this study:

P1: *The adoption of controlling mechanisms impacts positively the overall security position of the organization in the cloud.*

P2: *The adoption of controlling mechanisms impacts positively the ethical use of the organization's systems in the cloud.*

P3: *The ethical use of the systems strengthens the overall security position of the organization in the cloud.*

3. Research Methodology

The proposed framework (Figure 1) was evaluated further through a case study and a large-scale survey. The development of the survey instrument included four stages: (1) initially the framework constructs were developed from IS Security Literature, (2) the construct items were generated through the literature review and an exploratory case study, (3) a pilot study was conducted to pre-test the validity and reliability of the instrument, and (4) finally a large-scale survey was used for the data collection and analysis. The questions and the items for each of the constructs are listed in Table A2 (in Appendix). Stages one and two were described in the previous section (more information about the case study discussions will follow in this section). For stage three a pilot study was designed to assess the convergent and discriminant validity of the scales. Stage four used statistical analysis to determine the validity and reliability of the instrument constructs. The research framework and the associated propositions were then tested using structural equation modeling (SEM) techniques.

3.1. Exploratory Case Study

The exploratory case study used a qualitative approach and aimed to generate a deep understanding of the phenomena under investigation by examining the meanings that participants assign to them following a particular social or organizational setting (Orlikowski and Baroudi, 1991). The study of the cloud security cannot be separated from its organizational context and - more specifically - the perspective of the adopting organizations and their behavior towards security and shared responsibility and also their motivation for investing in controlling mechanisms as proactive solutions for their overall security. Another reason is also the fact that this approach allows concepts to emerge from the data according to Miles and Huberman (1994) while for Yin (2009) case studies are the preferred strategy when how or why questions are being posed, when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context.

The case study supports this research by identifying and familiarizing with the context of cloud security services and more specifically with the identified constructs (presented in section 2.2). This stage intended to enrich the conceptual framework built from the IS Security Literature with further insight for each of the three constructs and a research agenda for the survey phase of the study (Table A1 in Appendix). The case study was conducted in January and February 2016 focusing on the security services provided by a specific cloud security vendor. The interviewees were selected based on their involvement in cloud security decision-making and experience (cloud security Vendor, Adopters, and Potential Adopters). The data from the interviews were analyzed through the various phases of thematic analysis (Boyatzis, 1998; Braun and Clarke, 2006) and theory-driven themes were generated, leading to an initial coding scheme (Table A1 in Appendix). Further thematic analysis was carried out to indicate the sub-themes and divide them into sub-groupings

There are many variations of qualitative sampling described in the literature and much confusion and overlapping types of sampling (Coyne, 1997). Improved quality of research synthesis is critical; and this can be achieved through the informed decisions about sampling (Suri, 2011). According to Suri (2009), purposeful sampling requires access to key informants in the field who can help in identifying information-rich cases. Sample bias from the case study (Benbasat et al., 1987; Siggelkow, 2007) was avoided by employing an intensity sampling approach; followed to collect rich data about the study. Patton (2002) referring to intensity sampling addressed the cases selecting for intensity sampling were 'excellent or rich examples of the phenomenon of interest, but not highly unusual cases. Cases that manifest sufficient intensity to illuminate the nature of success or failure, but not at the extreme' (Patton, 2002).

3.2. Pilot Study

A pilot study followed the initial research framework and the case study, for validating the constructs and the items generated by the previous stages of this research. Content validity is a fundamental requirement for measurement instruments, for ensuring that the items cover the major content of the construct (Churchill, 1979). Content validity was achieved through a comprehensive literature review and the exploratory case study. The items identified in the literature were discussed and re-evaluated through structured interviews with the case study participants around the three thematic areas identified by the IS security literature (Table A1 in Appendix). The three thematic areas discussed were namely: a. cloud usage control, b. overall cloud security maintenance, and c. ethical use of the IT assets and the infrastructure of the cloud. Based on the exploratory discussions, redundant and ambiguous items were either edited or eliminated, and new items were added wherever deemed necessary. The instrument was pilot-tested (N=25) and then based on the feedback, the readability factor of the questions was improved for content validity purposes. Reliability and validity tests on the sample provided support for all constructs of the instrument. The reliability values were all greater than 0.7 and therefore of an acceptable standard (Nunnally, 1978).

3.3. Large-scale survey

The research model is formed around the proactive decision to adopt additional cloud security services as a controlling mechanism for the cloud from a potential security vendor and the motivation behind such a decision. Additionally to the case study and developing the proposed framework (Figure 1), we designed a survey for the exploration and confirmation of the framework

constructs and the model fit. The survey was conducted during the period of August-September 2017 in firms of different sizes (SMEs and larger organizations) from a cross-section of industries having implemented the cloud deployment model for conducting their operations.

A total sample of 537 participants was asked to fill out anonymously the online questionnaire which was individually emailed. The study received a sample of 215 responses from IT-decision makers in companies with any form of cloud infrastructure (public, private, hybrid or community cloud). From the N=215 final responses, N=202 were complete and usable, indicating a 37.6% response rate which is relatively high. The profile of the respondents is illustrated in Figure 2. By applying online questionnaires as a data collection method, we were concerned with the common method bias and the possible measurement error which could bias the survey results (Churchill, 1979; Podsakoff et al., 2003). Harman's single-factor test was used to assess common method variance which was of an acceptable standard (Podsakoff et al., 2003).

For the analysis of both the measures and the model; Exploratory Factor Analysis (EFA) and Structural Equation Modelling (SEM) techniques were applied. SEM is widely used in social sciences to analyze structure and measurement models (Anderson and Gerbing, 1988; Hair et al., 2014), the proposed research model was examined through IBM SPSS AMOS 23. The exploratory factor analysis (EFA) used IBM SPSS 23 for the dimension reduction and other statistical purposes.

Figure 2. Descriptive statistics of the respondents

<Figure 2 here>

4. Results

The data from the case study discussions were analyzed through the various phases of thematic analysis, developing an initial coding scheme (Boyatzis, 1998; Braun and Clarke, 2006) where the theory-driven themes, sub-themes, and other groupings were based (Table A1 in Appendix). A subsequent step after the case study was the development of the primary instrument which was pilot-tested for the convergent and discriminant validity of the proposed scales. Statistical analysis was conducted for the large scale survey to determine the validity and reliability of the instrument constructs. Finally, the proposed framework was tested using structural equation modeling (SEM) as the most appropriate method for assessment of the validity and reliability of scales (Hair et al., 2014) followed in similar studies.

4.1. Case Study Results

The case study involved initial discussions and interviews with stakeholders from the vendor organization, the adopters and the potential adopters of security services as controlling mechanisms for the cloud. The interviewees were involved in cloud security decision-making and had relevant experience. The discussions were formed around the three topic areas as these were identified in the IS Security Literature, namely a) the systems usage control in their organization, b) the ethical use of the systems and c) the ways they can build an overall security attitude. Other discussion topics focused on the security and control services available in the market, their intention to adopt controlling mechanisms, and their concerns about cloud security. We will present briefly here the

major ideas expressed throughout the discussions. The themes and sub-themes from the interviews are also summarized with their explanation in Table A1 in Appendix.

In cloud security adoption, the social environment strongly influences decisions about cloud security adoption as '*the size of the firms, the industry they work in, and also the regulatory standards are main determinants of such decisions,'* which was a major discussion point during the interviews. The system's social structure affects adoption of cloud security services and shows that different motivation drives organizations to seek for cloud security solutions. The categorization of the organizations according to their type can be summarized as:

1. **Public organizations** (i.e., government, local authorities, NGOs) follow '*high regulatory and compliance standards'* as well as some specific policies and directives for security.
2. **Private organizations** (i.e., SMEs, Start-ups, larger companies) have to follow the regulatory standards for security; however, they are more concerned about their data security on the cloud, but also their customers' trust for their practices.

The underlying reasons for adoption of security and control mechanisms for the cloud also depend on the size of the organization and can be briefly outlined in three broad categories:

SMEs and start-ups are interested in adopting cloud controlling mechanisms from a trusted vendor because as it was stated '*customers ask for that, they cannot trust in-house security provided by these small companies'.* The organizational decisions around security and control for the cloud depend heavily on the field they are doing their business, as '*the industry requires security of the customer data stored and shared on the cloud.'* There was an indicator that the level of security required for each industrial sector relates to the regulatory and security standards they have to comply with for their industry. In the case of start-up organizations, while trying to expand their cloud application market, they collaborate with vendors of security services by '*launching their services on the security vendor's cloud,' so as they also* expand their business relationships. Small organizations and start-ups also find that the security and control is *'a complex and costly problem for new, inexperienced organizations to deal with only in-house developed solutions.'* The level of the security education and training in such organizations cannot allow them to build *'a strong overall security status'* when they work in the cloud.

Large companies are interested in the internal security of their cloud applications and how to ensure that their applications on the cloud are secure '*within their company.'* For the security and control of the cloud, they also develop their in-house services as their customers trust them in the market and also believe in their ability to promote ethical use of their systems. They use in-house developed solutions for control and ethical use of their systems, while they promote *'security awareness and shared responsibility as core targets of the security strategy'* within their organization. Large organizations are mostly motivated to adopt the latest update and release of controlling mechanisms for securing their applications developed for the cloud infrastructure.

Government, local authorities and public sector organizations follow high compliance standards and specific policies, and also they try to reduce their costs mostly by adopting the services from a cloud security provider rather than developing in-house solutions. This approach has '*focus mostly on cost-reduction'* and also keeping *'business relationships with the vendor for future collaborations*

in other cloud projects' and launching services on vendor's cloud so they would be able to get additional revenue increase.

The discussions with the interviewees also showed that the motivation for using cloud security and control services is size-dependent (SMEs and start-ups or large organizations) and the industry-specific (public or private sector where the organization operates). At this instance, there was not an industry-level investigation, however as the interviews showed that this is a critical differentiating factor. That fact should be taken into account for further research in the area following an industry-specific approach.

4.2. Survey results

Initially, the measurement model was tested based on the convergent and discriminant validity to ensure that the measures are representative for the constructs. Consequently, the model was examined for the validity of the developed propositions. Evidence of convergent and discriminant validity was evaluated through an exploratory factor analysis (EFA) (Fabrigar et al., 1999; Kline, 2013; Osborne and Costello, 2005). Table 2 presents the factor loadings for the solution using principal components analysis with Promax rotation (Osborne, 2015). The total variance explained is 54.9 percent. Each item loaded higher than .40 on one factor (eigenvalues larger than 1), suggesting convergent and discriminant validity, as well as the Kaiser-Meyer-Olkin measure, is 0.910 confirming the adequacy of the sample for this study.

Table 2. Summary of Items and Factor Loadings

<Table 2 here>

At the construct level, convergent validity requires the average variance extracted (AVE) to be larger than 0.5 (Gefen et al., 2011; Hair et al., 2014). The results show that the AVEs are larger than 0.5 (Table A2) which is acceptable. The discriminant validity of the model was established (Table 3). The square root of AVE (diagonal elements) was larger than the correlation between factors and less than 0.7, which fulfills the acceptable standards for the model (Fornell and Larcker, 1981).

Table 3. Correlation and square root of AVE

<Table 3 here>

Cronbach alphas for each measure (Table A2) indicated that construct reliability was acceptable. Composite reliability (CR) is larger than the suggested threshold of 0.7 which represents a high level of internal consistency (Bagozzi and Yi, 1988; Fornell and Larcker, 1981; Hair et al., 2014).

Table 4. Fit Indices

<Table 4 here>

Subsequent to the exploratory factor analysis (EFA), a structural equation model (SEM) using maximum likelihood was estimated with AMOS 23 (Gefen et al., 2011; Hair et al., 2014). Fit indices were of an acceptable standard (Table 4). The results of the path tests are shown in Table 5. The standardized regression weights for Controlling Mechanisms (CM), Overall Security Position (OS) and Ethical Use (EU) are .23 (CM to OS), .68 (CM to EU), and .64 (EU to OS) respectively, which supports

the three propositions. The effects of the adopted controlling mechanisms to the overall security position of the organization are becoming higher when the ethical use of the systems is in place, which indicates that the indirect effects of ethical use are very strong.

Table 5. Path tests

<Table 5 here>

5. Discussion

The usage control of the cloud should be explored through the interactions, the behavioral, ethical beliefs and the determining factors for the adoption of additional countermeasures (Straub and Welke, 1998), the members of a social system (the cloud infrastructure at this instance) are the organizations interacting with the reference organization (Boss et al., 2009). Within this context, the social environment strongly influences decisions about cloud security adoption, where the size of the firms, the industry they work in, and also the regulatory standards are main determinants of such decisions. The system's social structure affects upon the adoption decisions around the cloud controlling mechanisms and shows that this decision is strongly dependable in the industrial and regulatory context. The intention to comply with security controls is highly dependent on the setting in which each firm operates and more specifically at the industrial and social forces involving the associated policies (Anderson and Agarwal, 2010; Bulgurcu et al., 2010; Myyry et al., 2009; Pahnila et al., 2007). The industrial and social context around the security adoption was a common concept through our interviews and discussions. Also, the IS misuse intention and the intention for ethical systems use also relies on the sensitivity of the data and IT assets stored and used on the cloud (D'Arcy et al., 2009; D'Arcy and Herath, 2011), which can be considered one of the most severe insider threats (Magklaras and Furnell, 2001).

In our study, we used an expertize-intensive sample of participants from a cross-section of industries of different sizes (SMEs, start-ups, Large Organizations), as we intended to provide a holistic view of the organizational cloud security. However, Lee and Larsen (2009) find that social influence is significant for IT-intensive industry and expert groups but not for non-IT-intensive and non-IS expert groups. At this instance, there was not an industry-level investigation. However, this factor was raised during the interviews as a critical differentiating aspect and should not be neglected. That fact should be taken into account for further research in the area following an industry-specific approach. An industry-specific study should look in further detail if the proposed framework can be applied in various industries and how the effects of the controlling mechanisms to the overall cloud security in each industry can change. In their research Anderson and Agarwal (2010) show that except the controlling mechanisms and the technology that can help safeguard the overall security, ethical behavior of the users should also be considered for maintaining the overall security status. The ethical behavior as supported by the study of Pahnila et al. (2007) is presented as a subjective norm for the security maintenance forming the individuals' intentions for compliance with security standards.

Developing an ethical attitude and shared responsibility while working in the cloud, seems like a key determinant for maintaining a strong overall security position. Building the security awareness of the

organizations is the key determinant with a focus on precautionary control measurements (Bulgurcu et al., 2010) and also training and educating the employees for an understanding of potential issues related to security on the cloud. Controlling mechanisms and control monitoring of the cloud users and employees inside the organization (D'Arcy et al., 2009) can positively impact the overall security status of the cloud. On the contrary, our study findings indicate that when programs around the ethical use of the systems are in place, this can boost the effects of the controlling mechanisms (Vance et al., 2012) and also build confidence and alertness with security issues (LaRose et al., 2008). The point which should be highlighted is that the security awareness, the shared responsibility, and the security education and training seem as crucial proactive approaches for increasing and maintaining an overall secure organisational position for the cloud (Bulgurcu et al., 2010; D'Arcy et al., 2009; Tsohou et al., 2012).

6. Conclusion

Despite the positive impact that cloud service adoption may have for organizations, there are security concerns around their adoption, where providers offer solutions as a service, i.e., cloud security services, as solutions and controlling mechanisms for such problems. This research focused on the adoption of cloud security in general and managed cloud security services in specific, as a controlling mechanism for the cloud usage in organizations. Our study, as presented in this paper, sets a research agenda and puts forward a research framework for the analysis of the effects of controlling mechanisms to the overall security position of the organization in the cloud. The findings indicated that there are direct effects to the overall cloud security position as a result of the adoption of controlling mechanisms (additional cloud security services for this instance). However, the critical aspect in our findings is that rather than the immediate (direct effects), the indirect effects of the controlling mechanisms (through the ethical use of the cloud systems) can make the overall security position stronger. Future research in this field could be expanded in industry-specific contexts and/or different sizes of organizations, as the problem depends highly on the industrial context (industry specific), the number of employees and the overall turnout (size of the organization).

7. References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179–211.

Ali, M., Khan, S.U. and Vasilakos, A. V. (2015), "Security in cloud computing: Opportunities and challenges", *Information Sciences*, Vol. 305, pp. 357–383.

Alshamaila, Y., Papagiannidis, S. and Li, F. (2013), "Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework", *Journal of Ent Info Management*, Vol. 26 No. 3, pp. 250–275.

AlZain, M.A., Pardede, E., Soh, B. and Thom, J.A. (2012), "Cloud computing security: from single to multi-clouds", *System Science (HICSS), 2012 45th Hawaii International Conference on*, IEEE, pp. 5490–5499.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", *Mis Quarterly*, Vol. 34 No. 3, pp. 613–643.

Anderson, J.C. and Gerbing, D.W. (1988), "Structural equation modeling in practice: a review and recommended two-step approach", *Psychological Bulletin*, Vol. 103 No. 3, pp. 411–423.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., et al. (2010), "A view of cloud computing", *Communications of the ACM*, Vol. 53 No. 4, pp. 50–58.

Ba, S. and Pavlou, P.A. (2002), "Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior", *MIS Quarterly*, pp. 243–268.

Bagozzi, R. and Yi, Y. (1988), "On the Evaluation of Structural Equation Models", *Journal of the Academy of Marketing Science*, Vol. 16 No. 1, pp. 74–94.

Baskerville, R., Eun, H.P. and Kim, J. (2014), "An emote opportunity model of computer abuse", *Info Technology & People*, Vol. 27 No. 2, pp. 155–181.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987), "The case research strategy in studies of information systems", *MIS Q.*, Vol. 11 No. 3, pp. 369–386.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015), "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors", *MIS Quarterly (MISQ)*, Vol. 39 No. 4, pp. 837–864.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 151–164.

Boyatzis, R.E. (1998), *Transforming Qualitative Information: Thematic Analysis and Code Development.*, Sage Publications, Inc., Thousand Oaks, CA, US.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77–101.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly: Management Information Systems*, Vol. 34 No. 3, pp. 523–548.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009), "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *Future Generation Computer Systems*, Vol. 25 No. 6, pp. 599–616.

Cavusoglu, H., Raghunathan, S. and Cavusoglu, H. (2009), "Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems", *Information Systems Research*, Vol. 20 No. 2, pp. 198–217.

Chatterjee, S., Sarker, S. and Valacich, J.S. (2015), "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use", *Journal of Management Information Systems*, Vol. 31 No. 4, pp. 49–87.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2012), "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?", *Journal of Management Information Systems*, Vol. 29 No. 3, pp. 157–188.

Chen, Y. and Zahedi, F. (2016), "Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China", *Management Information Systems Quarterly*, Vol. 40 No. 1, pp. 205–222.

Churchill, G.A.J. (1979), "Paradigm of for developing constructs measures", *Journal of Marketing Research*, Vol. 16 No. 1, pp. 64–73.

Coyne, I.T. (1997), "Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries?", *Journal of Advanced Nursing*, Vol. 26 No. 3, pp. 623–630.

CSA. (2015), *Cloud Adoption Practices & Priorities Survey Report*, available at: https://cloudsecurityalliance.org/research/surveys/.

D'Arcy, J. and Herath, T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, Vol. 20 No. 6, pp. 643–658.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285–318.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79–98.

Doherty, N.F., Anastasakis, L. and Fulford, H. (2009), "The information security policy unpacked: A critical study of the content of university policies", *International Journal of Information Management*, Vol. 29 No. 6, pp. 449–457.

El-Gazzar, R.F. (2014), "A literature review on cloud computing adoption issues in enterprises", *International Working Conference on Transfer and Diffusion of IT*, Springer, pp. 214–242.

Fabrigar, L.R., Fabrigar, L.R., Wegener, D.T., Wegener, D.T., MacCallum, R.C., MacCallum, R.C., Strahan, E.J., et al. (1999), "Evaluating the use of exploratory factor analysis in psychological research.", *Psychological Methods*, Vol. 4 No. 3, pp. 272–299.

Fornell, C. and Larcker, D.F. (1981), "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics", *Journal of Marketing Research*, Vol. 18 No. 3, p. 382.

Gal-Or, E. and Ghose, A. (2005), "The Economic Incentives for Sharing Security Information", *Information Systems Research*, Vol. 16 No. 2, pp. 186–208.

Garrison, G., Kim, S. and Wakefield, R.L. (2012), "Success factors for deploying cloud computing", *Communications of the ACM*, Vol. 55 No. 9, pp. 62–68.

Gefen, D., Straub, D. and Rigdon, E. (2011), "An update and extension to SEM guidelines for admnistrative and social science research", *MIS Quarterly*, Vol. 35 No. 2, pp. iii–xiv.

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2009), "Developing expertise for network intrusion detection", *Info Technology & People*, Vol. 22 No. 2, pp. 92–108.

Habib, S.M., Hauke, S., Ries, S. and Mühlhäuser, M. (2012), "Trust as a facilitator in cloud computing: a survey", *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 1 No. 1, p. 1.

Hair, J.F.J., Hult, G.T.M., Ringle, C. and Sarstedt, M. (2014), *A Primer on Partial Least Squares*

Structural Equation Modeling (PLS-SEM), *Long Range Planning*, Vol. 46, available at:https://doi.org/10.1016/j.lrp.2013.01.002.

Herath, H.S.B. and Herath, T.C. (2008), "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit", *Journal of Management Information Systems*, Vol. 25 No. 3, pp. 337–375.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: A framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106–125.

Hsu, C., Lee, J.-N. and Straub, D.W. (2012), "Institutional Influences on Information Systems Security Innovations", *Information Systems Research*, Vol. 23 No. 3-, pp. 918–939.

Hsu, J.S.-C., Shih, S.-P., Hung, Y.W. and Lowry, P.B. (2015), "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness", *Information Systems Research*, Vol. 26 No. 2, pp. 282–300.

Hu, Q., West, R. and Smarandescu, L. (2015), "The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective", *Journal of Management Information Systems*, Vol. 31 No. 4, pp. 6–48.

Huang, J. and Nicol, D.M. (2013), "Trust mechanisms for cloud computing", *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 2 No. 1, p. 1.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and Information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3.

Johnston, A.C., Warkentin, M. and Siponen, M.T. (2015), "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric.", *MIS Quarterly*, Vol. 39 No. 1, pp. 113–134.

Kerschbaum, F. (2011), "Secure and sustainable benchmarking in clouds", *Business & Information Systems Engineering*, Vol. 3 No. 3, pp. 135–143.

Kline, R.B. (2013), "Exploratory and Confirmatory Factor Analysis", *Applied Quantitative Analysis in Education and the Social Sciences*, pp. 169–207.

LaRose, R., Rifon, N.J. and Enbody, R. (2008), "Promoting personal responsibility for internet safety", *Communications of the ACM*, Vol. 51 No. 3, pp. 71–76.

Lee, C.H., Geng, X. and Raghunathan, S. (2016), "Mandatory Standards and Organizational Information Security", *Information Systems Research*, Vol. 27 No. 1, pp. 70–86.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 177–187.

Liang, H. and Xue, Y. (2009), "Avoidance of information technology threats: A theoretical perspective", *MIS Quarterly: Management Information Systems*, Vol. 33 No. 1, pp. 71–90.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: A threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7, p. 394.

Magklaras, G.B. and Furnell, S.M. (2001), "Insider threat prediction tool: Evaluating the probability of

IT misuse", *Computers & Security*, Vol. 21 No. 1, pp. 62–73.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011), "Cloud computing — The business perspective", *Decision Support Systems*, Vol. 51 No. 1, pp. 176–189.

Mell, P. and Grance, T. (2011), "The NIST definition of cloud computing", *NIST Special Publication*, Vol. 800, p. 145.

Mezgár, I. and Rauschecker, U. (2014), "The challenge of networked enterprises for cloud computing interoperability", *Computers in Industry*, Vol. 65 No. 4, pp. 657–674.

Miles, M.B. and Huberman, A.M. (1994), *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed., Sage, Thousand Oaks ; London.

Mookerjee, V., Mookerjee, R., Bensoussan, A. and Yue, W.T. (2011), "When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination", *Information Systems Research*, Vol. 22 No. 3, pp. 606–623.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009), "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 126–139.

Nunnally, J. (1978), *Psychometric Theory*, *New York: McGraw-Hill*, available at:https://doi.org/10.1037/018882.

Orlikowski, W.J. and Baroudi, J.J. (1991), "Studying information technology in organizations: Research approaches and assumptions", *Information Systems Research*, Vol. 2, pp. 1–28.

Osborne, J.W. (2015), "What is Rotating in Exploratory Factor Analysis?", *Practical Assessment, Research & Evaluation*, Vol. 20 No. 2, pp. 1–7.

Osborne, J.W. and Costello, A.B. (2005), "Best Practices in Exploratory Factor Analysis : Four Recommendations for Getting the Most From Your Analysis", *Practical Assessment, Research & Evaluation*, Vol. 10 No. 7, pp. 1–9.

Ouchi, W.G. (1979), "A conceptual framework for the design of organizational control mechanisms", Springer, pp. 63–82.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", *System Sciences, 2007. HICSS 2007. 40Th Annual Hawaii International Conference on*, IEEE, p. 156b–156b.

Patton, M.Q. (2002), "Designing qualitative studies", *Qualitative Research and Evaluation Methods*, Vol. 3, pp. 230–246.

Pavlou, P.A. and Fygenson, M. (2006), "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior", *MIS Quarterly: Management Information Systems*, Vol. 30 No. 1, pp. 115–143.

Pearson, S. (2013), "Privacy, security and trust in cloud computing", Springer, pp. 3–42.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879–903.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information

systems security training: an action research study", *Mis Quarterly*, pp. 757–778.

Rea, A., Cao, X., Gupta, A. and Shenoy, N. (2012), "A secure cloud internetwork model with economic and social incentives (SCIMES)", Vol. AMCIS 2012.

Rebollo, O., Mellado, D., Fernández-Medina, E. and Mouratidis, H. (2015), "Empirical evaluation of a cloud computing information security governance framework", *Information and Software Technology*, Vol. 58, pp. 44–57.

Rodero-Merino, L., Vaquero, L.M., Caron, E., Muresan, A. and Desprez, F. (2012), "Building safe PaaS clouds: A survey on security in multitenant software platforms", *Computers & Security*, Vol. 1 No. 1, pp. 96–108.

Shahzad, F. (2014), "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", *Procedia Computer Science*, Vol. 37, pp. 357–362.

Siggelkow, N. (2007), "Persuasion with case studies", *Academy of Management Journal*, Vol. 50 No. 1, pp. 20–24.

Siponen, M., Baskerville, R. and Heikka, J. (2006), "A design theory for secure information systems design methods", *Journal of the Association for Information Systems*, Vol. 7 No. 1, p. 31.

Siponen, M. and Iivari, J. (2006), "Six Design Theories for IS Security Policies and Guidelines.", *Journal of the Association for Information Systems*, Vol. 7 No. 7.

Siponen, M. and Vance, A. (2010), "Neutralization: New insights into the problem of employee information systems security policy violations", *MIS Quarterly: Management Information Systems*, Vol. 34 No. SPEC. ISSUE 3, pp. 487–502.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012), "Information security policies in the UK healthcare sector: a critical evaluation", *Information Systems Journal*, Vol. 22 No. 1, pp. 77–94.

Steinbart, P.J., Keith, M.J. and Babb, J. (2016), "Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication", *Information Systems Research*, Vol. 27 No. 2, pp. 219–239.

Straub, D.W. and Jr., D.W.S. (1990), "Effective IS Security: An Empirical Study", *Information Systems Research*, Vol. 1 No. 3, pp. 255–276.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, pp. 441–469.

Subashini, S. and Kavitha, V. (2011), "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, Vol. 34 No. 1, pp. 1–11.

Suri, H. (2011), "Purposeful sampling in qualitative research synthesis", *Qualitative Research Journal*, Vol. 11 No. 2, pp. 63–75.

Suri, H. and Clarke, D. (2009), "Advancements in research synthesis methods: From a methodologically inclusive perspective", *Review of Educational Research*, Vol. 79 No. 1, pp. 395–430.

Takabi, H. and Joshi, J.B.D. (2012), "Policy management as a service: an approach to manage policy heterogeneity in cloud computing environment", *System Science (HICSS), 2012 45th Hawaii International Conference on*, IEEE, pp. 5500–5508.

Takabi, H., Joshi, J.B.D. and Ahn, G.-J. (2010), "Security and Privacy Challenges in Cloud Computing Environments", *IEEE Security and Privacy*, Vol. 8 No. 6, pp. 24–31.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2012), "Analyzing trajectories of information security awareness", *Info Technology & People*, Vol. 25 No. 3, pp. 327–352.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: insights from habit and protection motivation theory", *Information & Management*, Vol. 49 No. 3, pp. 190–198.

Vaquero, L.M., Rodero-Merino, L. and Morán, D. (2011), "Locking the sky: a survey on IaaS cloud security", *Computing*, Vol. 91 No. 1, pp. 93–118.

Wang, J., Gupta, M. and Rao, H.R. (2015), "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications.", *MIS Quarterly*, Vol. 39 No. 1, pp. 91–112.

Warkentin, M., Johnston, A.C., Walden, E. and Straub, D.W. (2016), "Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination", *Journal of the Association for Information Systems*, Vol. 17 No. 3, p. 194.

Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: A threat control model and empirical test", *Computers in Human Behavior*, Vol. 24 No. 6, pp. 2799–2816.

Yin, R.K. (2009), *Case Study Research: Design and Methods*, 4th ed., Vol. 5, Sage, London.

Yoon, C. and Kim, H. (2013), "Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms", *Info Technology & People*, Vol. 26 No. 4, pp. 401–419.

Zhang, Y. and Joshi, J. (2009), *Access Control and Trust Management for Emerging Multidomain Environments*, Emerald Group Publishing.

Zissis, D. and Lekkas, D. (2012), "Addressing cloud computing security issues", *Future Generation Computer Systems*, Vol. 28 No. 3, pp. 583–592.

8. Appendix

Table A1. Thematic analysis of the case study discussions

<Table A1 here>

Table A2. The survey instrument (5-point Likert Scale ranging from "Extremely Important" to "Not at all important").

<Table A2 here>

Tables

Table 1. Construct generation from IS Security Literature

	Selected Literature	Systems Usage Control	Ethical Use of the Systems	Overall Proactive Security Countermeasures
1.	(Anderson and Agarwal, 2010)		X	X
2.	(Ba and Pavlou, 2002)		X	
3.	(Baskerville et al., 2014)	X	X	
4.	(Boss et al., 2009)	X	X	
5.	(Boss et al., 2015)	X		X
6.	(Bulgurcu et al., 2010)		X	X
7.	(Cavusoglu et al., 2009)	X		X
8.	(Chatterjee et al., 2015)		X	
9.	(Chen and Zahedi, 2016)		X	
10.	(Chen et al., 2012)	X	X	
11.	(D'Arcy and Herath, 2011)	X	X	X
12.	(D'Arcy et al., 2014)		X	X
13.	(D'Arcy et al., 2009)	X	X	X
14.	(Herath and Rao, 2009)	X		X
15.	(Hsu et al., 2015)	X		
16.	(Hsu et al., 2012)	X		
17.	(Hu et al., 2015)		X	
18.	(Johnston and Warkentin, 2010)	X	X	X
19.	(Johnston et al., 2015)		X	X
20.	(Lee et al., 2016)	X		X
21.	(Liang and Xue, 2009)		X	
22.	(Mookerjee et al., 2011)			X
23.	(Myyry et al., 2009)		X	
24.	(Pahnila et al., 2007)	X	X	
25.	(Pavlou and Fygenson, 2006)		X	X

26.	(Puhakainen and Siponen, 2010)	**X**	**X**	**X**
27.	(Siponen and Iivari, 2006)	**X**		
28.	(Siponen and Vance, 2010)		**X**	
29.	(Stahl et al., 2012)	**X**	**X**	
30.	(Steinbart et al., 2016)	**X**	**X**	**X**
31.	(Straub and Jr., 1990)		**X**	
32.	(Tsohou et al., 2012)		**X**	**X**
33.	(Vance et al., 2012)		**X**	**X**
34.	(Warkentin et al., 2016)	**X**		
35.	(Workman et al., 2008)	**X**	**X**	**X**
36.	(Yoon and Kim, 2013)	**X**	**X**	**X**

Table 2: Summary of Items and Factor Loadings

Exploratory Factor Analysis: Pattern Matrix			
	Factor Loadings		
	Controlling mechanisms (CM)	**Overall Security Position (OS)**	**Ethical Use (EU)**
CM1	**0.813**		
CM2	**0.667**		
CM3	**0.658**		
CM4	**0.534**		
CM5	**0.495**		
OS1		**0.863**	
OS2		**0.666**	
OS3		**0.643**	
OS4		**0.621**	
OS5		**0.418**	
EU1			**0.751**
EU2			**0.733**
EU3			**0.484**
EU4			**0.475**
EU5			**0.459**

Table 3. Correlation and square root of AVE

	CM	OS	EU
Controlling Mechanisms (CM)	**0.74**		
Overall Security Position (OS)	0.55	**0.72**	
Ethical Use (EU)	0.44	0.49	**0.74**

Table 4. Fit Indices

Fit criteria	Model value
IFI	0.998
CFI	0.998
NFI	0.990
GFI	0.996
AGFI	0.977
TLI	0.995
RMSEA	0.030

Table 5. Path tests

Proposition	Paths	Standardized Estimate	t-Value
P1	controlling mechanisms (CM) -> ethical use (EU)	0.677	6.045 ***
P2	controlling mechanisms (CM) -> overall security position (OS)	0.225	0.591*
P3	ethical use (EU) -> overall security position (OS)	0.643	1.248*
	* $p \leq 0.05$ *** $p \leq 0.001$		

Table A1. Thematic analysis of the case study discussions

Thematic analysis		
Discussion Topic	**Emerging Areas**	**Description**
Organisational Cloud Control	Firm size	The firm size of the adopter (SMEs, large organizations, etc.) cannot always allow the development of in-house controlling security solutions.
	Trial period	The cloud security services are provided on a trial version for a limited basis (trial period) and therefore the adopters can observe the improvements (or not) of their operations and security status when controlling mechanisms are in place.
	Company turnover	The turnover of the adopter is influencing decisions around cloud security adoption; a large company turnover means controlling the overall security position and keeping the risk levels low is crucial.
	Complexity	The cloud security is perceived as a relatively difficult and complex problem to control solely with in-house developed solutions.
	Perceived Benefit	The firm can achieve a perceived benefit from the additional cloud security services compared to the controlling solutions they supersede (prior frameworks/precautions for cloud security).
Overall Cloud Security Maintenance	Potential Security Issues	The potential security issues identified for the cloud environments motivate the cloud clients and the infrastructure provider to protect the IT resources stored and used in the cloud.
	Security Status	The overall security status and the security awareness are already at a very high level, and therefore the organization seeks for additional measurements to upgrade the security position in the cloud with the latest advances.
	Compatibility	The existing controlling and security systems have a compatibility problem with the cloud, and therefore there is a need for additional cloud security solutions in line with the existing systems, processes, and operations.
	Willingness to Pay	There is a high level of understanding and knowledge of potential security issues, and therefore the willingness to pay for additional security is very high, for maintaining a strong security position in the cloud.
	Innovation	Adopting additional security services for the cloud seems like an innovative way to approach the security of the cloud effectively.
Ethical Use of the cloud systems and infrastructure	Industrial Structure	The industrial sector to which the business belongs to is very sensitive to the misuse of IT resources; as there are sensitive/important data and IT assets stored in the cloud.
	Regulatory Pressure	There is pressure for the firm to comply with the associated regulatory and security standards and therefore needs additional countermeasures.
	Experience and security education	The adopter's previous experience with IS misuse is low and cannot support in-house security solutions and security education programs; therefore we need to adopt a solution from a trusted vendor
	Shared responsibility	The way the adopter interacts with the other cloud clients promotes shared responsibility in the cloud and also fosters the use of additional security services as a precautionary measurement
	Competitive Pressure	The firm is forced by the competitors within the industry to assure the overall ethical use, usage control and security of the cloud.

Table A2. The survey instrument (5-point Likert Scale ranging from "Extremely Important" to "Not at all important").

Construct	Items		Factor Loading	Variance extracted (>0.50)	Cronbach's alpha (>0.60)	Composite reliability (>0.70)
CM Controlling Mechanisms		**Controlling Mechanisms** Our firm adopts/intents to adopt additional security services from a trusted security vendor for cloud usage control as:				
	CM1	Our relatively small firm size cannot support the development of in-house security solutions.	**0.81**	**0.55**	**0.81**	**0.71**
	CM2	Our operations and security status have improved, as we noticed through a trial period of controlling mechanisms.	**0.67**			
	CM3	Our large company turnover forces us to control our cloud usage and keep our risk levels low.	**dropped**			
	CM4	Our firm perceives cloud security as a relatively difficult and complex problem to control only with in-house solutions.	**dropped**			
	CM5	Our controlling program benefits from additional security services specialized for the cloud.	**dropped**			
OS Overall Security Position		**Overall Security Position** Based on our overall security knowledge and understanding, we adopt/intend to adopt additional cloud security services as in our firm:				
	OS1	The potential security issues identified for the cloud motivate us to protect our IT resources.	**0.86**	**0.52**	**0.80**	**0.76**
	OS2	There is already a very high level of security awareness, and we seek additional measurements to upgrade out security position	**0.67**			
	OS3	There is a compatibility problem of the security solutions, and therefore we need additional cloud security solutions in line with our existing systems and processes.	**dropped**			
	OS4	There is a high understanding of potential security issues, and therefore our willingness to pay for additional security is very high.	**0.62**			
	OS5	It is an innovative way to approach the security of the cloud efficiently.	**dropped**			
EU Ethical Use of the Systems		**Ethical Use of the Systems** Based on our program for promoting cloud ethical usage, we adopt/intent to adopt additional cloud security services as our firm:				
	EU1	Conducts business in industrial sector very sensitive to the misuse of IT resources.	**0.75**	**0.55**	**0.70**	**0.71**
	EU2	Complies with the associated regulatory standards and therefore needs additional countermeasures.	**0.73**			
	EU3	Is not experienced with IS misuse and we cannot develop in-house security solutions; therefore we need to adopt a solution from a trusted, experienced vendor.	**dropped**			
	EU4	Promotes shared responsibility in the cloud and therefore fosters additional security services as a precautionary measurement.	**dropped**			
	EU5	Is forced by the competitors within the industry to assure the overall ethical use and security of the cloud.	**dropped**			

Figures

Figure 1. The research framework

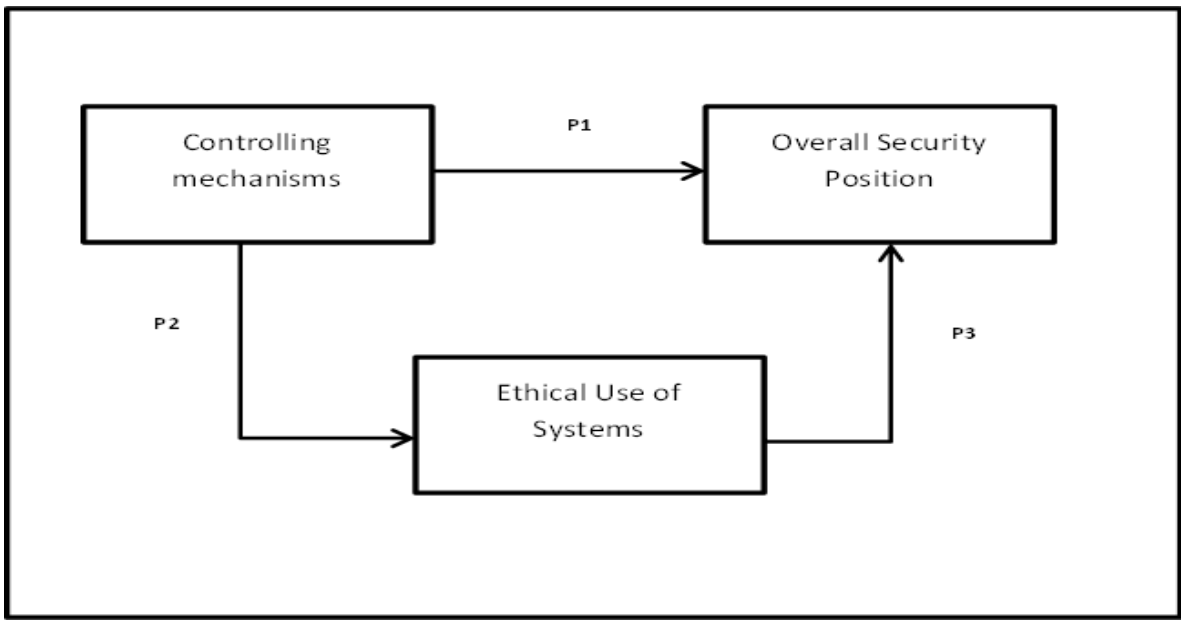

Figure 2. Descriptive statistics of the respondents

Role/ Position	Percentage
Chief Technology Officer	15.8
Chief Information Officer	4.5
Information Technology Manager	28.7
Systems Analyst	8.4
IT Executive	17.8
Security Analyst	6.9
Chief Marketing Technologist	2.0
Senior Network Engineer	2.0
Other	13.9
Total	100.0

Turnover of the organization (in USD per annum)	Percentage
less than 1 million per annum	18.3
1-5 million	28.2
5-10 million	20.3
10-100 million	19.3
more than 100 million	12.9
Other	1.0
Total	100.0

Size of the organization (number of employees)	Percentage
1 - 49	17.3
50 -999	46.0
1,000 -4,999	23.3
5,000 or more	13.4
Total	100.0

Industrial Sector	Percentage
Education	9.9
Food and Agriculture	2.0
Media	5.4
Transport	1.5
Energy and Utilities	5.0
Manufacturing	11.9
Government and Public Sector	2.0
Retail	9.4
Financial Services	7.4
Healthcare	4.0
Technology	30.7
Other	10.9
Total	100.0