UNIVERSITY OF CAPE COAST

CLOUD AND IN-HOUSE DATACENTERS: DETERMINANTS OF SECURITY INNOVATIONS AT THE COLLEGES OF EDUCATION, GHANA

TECHIE-MENSON HENRY

2019

UNIVERSITY OF CAPE COAST

CLOUD AND IN-HOUSE DATACENTERS: DETERMINANTS OF SECURITY INNOVATIONS AT THE COLLEGES OF EDUCATION, GHANA

BY

TECHIE-MENSON HENRY

Dissertation submitted to the College of Distance Education, University of Cape Coast, in partial fulfillment of the requirements for award of Master of Education Degree in Information Technology

January, 2019

DECLARATION

Candidate's Declaration

I hereby declare that this dissertation is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature……..... Date……....

Name: Techie-Menson Henry

Supervisor's Declaration

I hereby declare that the preparation and presentation of the dissertation were supervised in accordance with guidelines on supervision of dissertation laid down by the University of Cape Coast.

Supervisor's Signature……..... Date……..

Name: Dr. Paul Nyagorme

ABSTRACT

The study sought to investigate the determinants of security innovation for cloud and in-house datacenters for the Colleges of Education in Ghana. The study attempted to establish how cloud datacenters differ from in-house implementation in terms of security issues. The descriptive survey design was used for the study. In all, 300 respondents were purposively selected from 3 colleges of education to participate in the study. Questionnaire was the main data collection instrument. The study found out that both datacenter implementation types were vulnerable to attacks. The study revealed that both datacenters types for Colleges of Education were vulnerable to an attack even though in-house datacenters had better control measures. Again, the study found out that among the determinants examined, top management support and complexity was found to have a significant influence on whether Colleges of Education adopted security innovation technology. It was recommended that information security awareness, education and training be given to stakeholders as a means of improving security at the Colleges of Education.

ACKNOWLEDGEMENTS

My supervisor, Dr. Paul Nyagorme at the College of Distance Education was so meticulous in his scrutiny of this dissertation and his immense contribution has resulted in the production of this final work. He further exhibited a lot of patience, tolerance, love and devotion throughout the process of carrying out this dissertation.

Similarly, I am grateful to Henrietta Techie-Menson and Portia Akorsah Sarpong for their assistance in varied ways that contributed to the success of this study.

DEDICATION

To Henrietta Techie-Menson, Portia Akorsah Sarpong and all my family members

TABLE OF CONTENTS

LIST OF TABLES

List of Figures

CHAPTER ONE

Background to the Study

Globally, education plays a key role in maintaining economic growth as well as molding personality traits. Scholars such as Koutsopoulos and Papoutsi (2016) see education as a form of learning in which knowledge, skills, values, beliefs and habits are transferred only under the guidance of educators, to the belief that learners should energetically participate in the educational process. The introduction of the internet, software and hardware applications have compelled educational institutions to focus on the acquisition of hardware and computer network infrastructure in the pursuit of educational technology goals.

There is the need for reflection on changes observed in education due to technology as Parsad and Jones (2005) have tracked such innovations over time and have stated that it ranged from an introduction of a single classroom computer usage, to stand-alone computer laboratories coupled with partial skill-based software, to school wide distributed networks of computers running curriculum-based applications, to wide area networks equipped with broadband internet access and the streaming of multimedia contents.

There has been an increase in the use of datacenter computing as the paradigm of choice for most application domain. Currently, Colleges of Education in Ghana have deployed massive datacenters for the purposes of storing large amounts of personal and educational information that operate round-the-clock, serving content and retrieving data from thousands of users (David & Anbuselvi, 2015).

A datacenter is defined as a physical or virtual infrastructure used by many enterprises to put their networking systems and components for the company's information technology needs, which typically involve storing, processing and serving large amounts of mission-critical data to clients (Lam, Zhao, Xi & Chao 2012). Applied in the educational context, datacenter operations improve learning environments, provide students with a vital firsthand experience that connects theory with practice, foster greater staff and research collaboration, and support business-critical administrative services (Mircea & Andreescu, 2011).

Security concerns has currently become a core issue which need regular updates, alerts and is now a measure of failure or success of any business, thus requiring the establishment of best technologies and security systems (Yadav, 2012). Therefore, issues related to information security and privacy has become one of the core apprehensions of corporations and information technology managers (Ayyagari, 2012). Criminal attacks and intrusions into computer and information systems are spreading quickly with unlimited frequency and no geographical boundaries. In this technological era, data are sent and received in many electronic forms, often exposing educational institutions to increased data hacks, threats, and losses (Sabnis, Verbruggen, Hickey, & McBride, 2012).

Cloud computing has been described as an emerging technology that is very attractive in supporting collaborative learning and have been incorporated in social theories of education, especially in higher education (Thorsteinsson, Page & Niculescu, 2010). By accessing different programs, such as Twitter, Facebook, and Gmail, these Colleges of Education students already are consumers of cloud

computing technologies (Ercan, 2010). In-house Datacenters mean software installed and run on computers on the premises of organizations or institutions using the software (McFarlane, 2005). An in-house model is what is mostly known as the traditional approach (McFarlane, 2005). With an In-house implementation, servers are located on premises, they are managed by purchasing hardware and software licenses, fixing any issues, keeping it up to date, applying patches and are the property of that organization or institution.

There are some uncertainty about the secure nature of in-house implementation whilst Cloud computing is also not an exception due to its own security concerns. Andras Cser (2016) was of the view that because native security controls or mechanisms introduced in cloud services are insufficient, companies tend to use extra security layers aimed at safeguarding their security and workloads. In order to guarantee safety, in-house datacenters should then be kept in a physically secure location that prevents unauthorized access to data as well as safeguarding against maliciously placing corrupted files on servers. Again, datacenter's physical location must be secure such that floods, fire outbreak or other forms of natural disaster may not compromise its contents by possibly mounting its data at somewhere safe (Mathisen, 2011).

The continuous development of datacenter technology and its use in Colleges of Education has led to security challenges, especially those seeking a competitive advantage through innovation (Tipton, Harold & Krause, 2004). Innovation is an idea, practice, or project that is perceived as new by an individual or another unit of adoption" (Rogers, 2003, p. 12). Innovation may exist for a

longer period of time, but if end-users perceive it as new, then possibly it can still be regarded as an innovation for them. Other scholars regarded innovation as the possession of ideas, systems, practice, products or technologies that are new to the adopting organization (Damanpour & Wischnevsky, 2006). Likewise, West and Farr (1990) saw innovation as the intentional introduction and application within a role, group or organization of ideas, processes, products or procedures, new to adopting unit, aimed at benefiting individuals, organisations and the wider society. The adoption of innovation is seen as the generation, development and implementation of new initiatives or activities (Damanpour, 1991).

The concept of security innovation within the context of this research, henceforth, can be explained as the implementation of products, ideas, processes aimed at improving the Confidentiality, Integrity and Availability (CIA) of Information System (IS) assets of Colleges of Education which was previously nonexistent. Confidentiality refers to the restriction of access to IS assets only to those who are authorized to use it; integrity refers to the assurance that the IS assets have not been altered in an unauthorized way and availability refers to the "uptime" of computer-based IS assets or the assurance that its services will be available when it is needed.

The process of ensuring successful implementation of security innovation in academic institutions is complex which requires commitment from all stakeholders and not just individual perspectives. This is further echoed by innovation serving as the development and implementation of new ideas by people who over time engage in transactions with others within an institutional

order (Van de Ven, 1986) which emphasis the interactive process among people about new ideas in an organizational context.

Statement of the Problem

A secured educational datacenter means compliance with standards that facilitate the protection of sensitive and confidential data whiles cooperating and partnering other institutions to ensure goal attainment and achievement of mutual benefits. A secure datacenter for educational institutions ensures the empowerment of its users to focus on their core mandate of research, teaching and learning processes rather than the inconveniences and stress of losing critical and confidential data.

However, educational datacenters serve as attractive targets where a hacker can make financial and personal gains (Aboagye, 2018). There is a lack of institutional awareness of current security risks, together with the development and implementation of appropriate security controls (Spears & Barki, 2010) because research work related to security innovation is limited and is focused on an individual's perception and decision to adopt security innovations (Sinclaire,2005; Vance et al., 2012). Most importantly, Colleges of Education are ignorant of the factors facilitating or inhibiting the adoption of such security controls that can safeguard their IS assets.

There is inadequate research that focuses on information security innovation (Kotulic & Clark, 2004; Paulson, 2002) and there is none related to the datacenters of higher educational institutions like Colleges of Education in Ghana. The few scholarly work related to security innovation has only examined behavior

and attitudes of individuals with the help of user acceptance theories such as Theory of Planned Behavior, Technology Acceptance Model (Venkatesh & Morris, 2003 ; Ajzen, 1991) which aims to explain individual or users acceptance and decision to adopt security innovations (Lee and Kozar, 2005; Safa et al., 2015; Jones et al., 2010)

There is a gap from these previous scholarly works related to security innovations because they failed to include and capture how external pressures in the economic and political environment, as well as internal pressures of new technologies and the changing attitudes of members, influence innovation decisions of an entire organization. Nevertheless there is the need to examine adoption processes within educational institution that captures the organization as a whole. Failure to do so will lead to unprotected critical assets, limited accessibility, performance degradation, communication difficulties, loss of reputation and the inability to gain competitive advantage. It is within this context that this research seeks to assess and fill the knowledge gap by examining the determinants of security innovation of cloud and in-house datacenters within educational settings

Purpose of the Study

This study is designed to explore the determinants of security innovations of cloud and in-house datacenters of Colleges of Education.

Research Objectives

The main objectives for this study are listed below:

1. Identify security issues within cloud computing datacenters in Colleges of Education, Ghana
2. Identify security issues within in-house datacenters Colleges of Education, Ghana
3. Explore the factors that determine the adoptions of security innovations for in-house datacenters at Colleges of Education, Ghana
4. Explore the factors that determine the adoptions of security innovations for cloud datacenters at Colleges of Education, Ghana

Hypothesis

The hypothesis for the study are listed below:

H_o1– There is no statistically significant difference among Colleges of Education in terms of security issues within cloud datacentres

H_o2– There is no statistically significant difference among Colleges of Education in terms of security issues within in-house datacenters

H_o3 – There is no statistically significant difference among Colleges of Education in terms of factors that determine security innovation adoption for cloud datacenters

H_o4 – There is no statistically significant difference among Colleges of Education in terms of factors that determines the adoption of security innovations for in-house datacenters

Significance of the Study

First, the study will develop a theoretical model that combines technological, organizational, environmental constructs to offer new sets of determinants for theory building in the broader information security innovation literature

Second, management can make sound innovation adoption decisions based on the findings of this research. It will offer an understanding of factors that facilitate or inhibit security innovations within organizational settings

Third, the findings and results of the study may be useful to future researchers and stakeholders with interest in examining further security issues, innovation adoption, cloud and in-house implementations. This should lead to the generation of new ideas for the better understanding and implementation of cloud and in-house security controls.

Delimitation

As cloud and in-house computing consists of many security issues, this work may not be focus on all possible security issues related to them

Limitation

The study was conducted in three selected Colleges of Education and the sample was not representative of all Colleges of Education in Ghana. As a result, the current research project may therefore lack generalizability.

Furthermore, because the survey items were based on a 5-point Likert-type scale, the findings of the project may lack depth and richness. Future research may

account for this by carrying out a qualitative or answer open-ended questions, structured interviews etc.

Operational Definition of Terms

Information security: The process of protecting the availability, privacy, and integrity of information

Innovation: Novelty in products, methods of production and markets

Technology: It is the machinery and devices developed from scientific knowledge.

Security innovation: It is the awareness, acquisition and finally implementation of unique products, ideas, processes that are new to an organization which aims to safeguard its Information System (IS) assets

Organization of the Rest of the Study

The study consists of five chapters. Chapter one sets the stage for the research as it covers the background to the study, the statement of the problem, the purpose of the study, the research questions, significance of the study, limitations and delimitations. Drawing on the relevant literature, the second chapter constitutes the review of related literature of the study by providing an overview of cloud computing and in-house datacenter and their security issues. It also reviews literature on ICT innovation adoption among organisations as well as the incentives for and barriers to adoption.

Chapter three forms the methodology and procedure for conducting the study. It describes the research design, population, sample and sampling

techniques as well as research instruments. It also discusses the data collection and analysis procedure.

The fourth chapter is the analysis and discussion of data. It unfolds the emerging trends from the data using descriptive statistics to bring out the key findings of the study. Chapter five gives the summary, conclusions, recommendations and suggestions for future research.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

Introduction

This chapter reviews literature related to this study. Scholarly work that focuses on cloud and in-house datacenters security innovations are analyzed. The rationale for this review is to provide the standard for identifying similar and divergent views of researchers and in so doing uncover gaps that will serve as the motivation for this study. The review will be categorized under theoretical, conceptual and empirical review. The theoretical review will assess the theoretical foundation of this study whiles the conceptual review will be related to the terms or constructs within the study whiles the empirical review will be related to previous works done.

Theoretical Review

The research is applied within a theoretical framework or context to explain the studied phenomenon throughout this chapter. The user acceptance theories such as the Theory of Planned Behavior (TPB) (Ajzen, 1991), the DOI (Rogers, 1983), the TAM (Davis & Venkatesh, 1996 ; Venkatesh & Morris, 2000) and the Theory of Reasoned Action (Fishbein & Ajzen, 1975) have been used to predict and explain innovation adoption intention and actual user behavior.

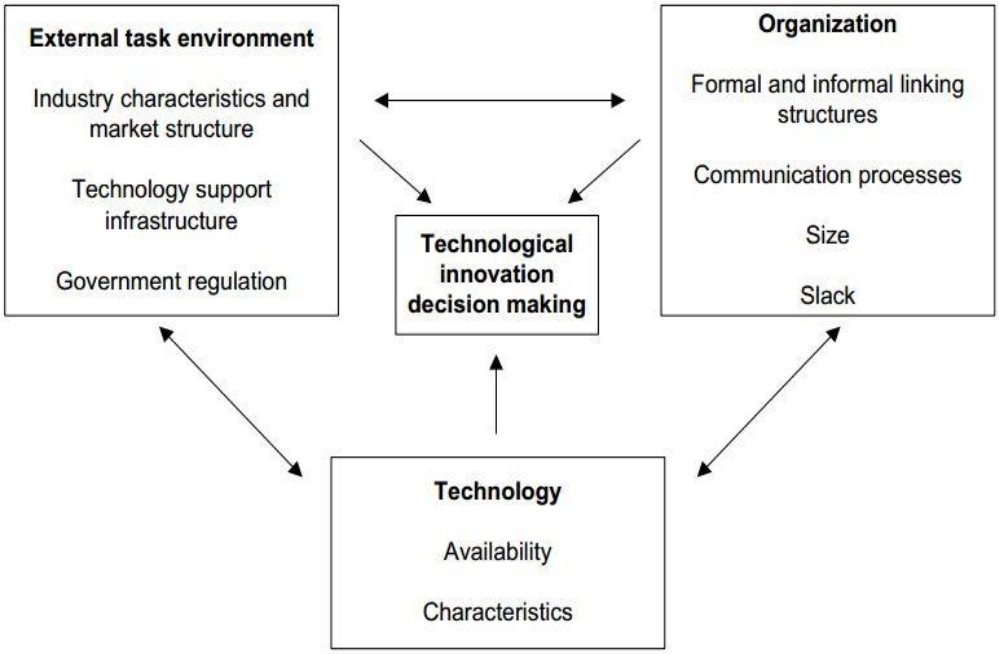
The principal assumptions for acceptance theories have included the causal relationship between perceived use and ease of use and the attitudes,

intentions and actual utilization of innovation by decision-makers. The intention to use innovation is preceded by the adoption of innovation behavior (use). The only exact predictor of the actual adoption and use of innovation is the intention to adopt and use innovation (Chang & Cheung, 2001). There are constraints in the sense that adopters do not themselves have a perception of innovation to explain it but to use it. In other words, the innovation perceived by the adopters is not an explanation of its spread but of its perception of the use of innovation. Again, a large number of constructs explaining the results of technology acceptance discovered in innovation adoption-dissemination studies are lacking that have required several extensions to include such attributes in particular in the TAM. Moreover, as it has been suggested by Peres et al. (2010), additional growth drivers, such as interpersonal communications, describes both the level and variety of use as well as an extended range of data sources need to be included in order to ensure that user acceptance and adoption theories remain a state of the art modeling framework.

This research is underpinned by the TOE framework by Tornatzky and Fleischer introduced in the "The Processes of Technological Innovation" book (Tornatzky & Fleischer, 1990). Three contexts are explained by this general framework: technological, organizational and environmental which can affect technological innovation at the company level. In this context, the technological significance is linked both to an organization's internal and external technology. The organizational framework explains the adverse effect of company characteristics on the adoption of innovation. The external environment is the

platform for an organization to undertake its business (Tornatzky & Fleischer, 1990).

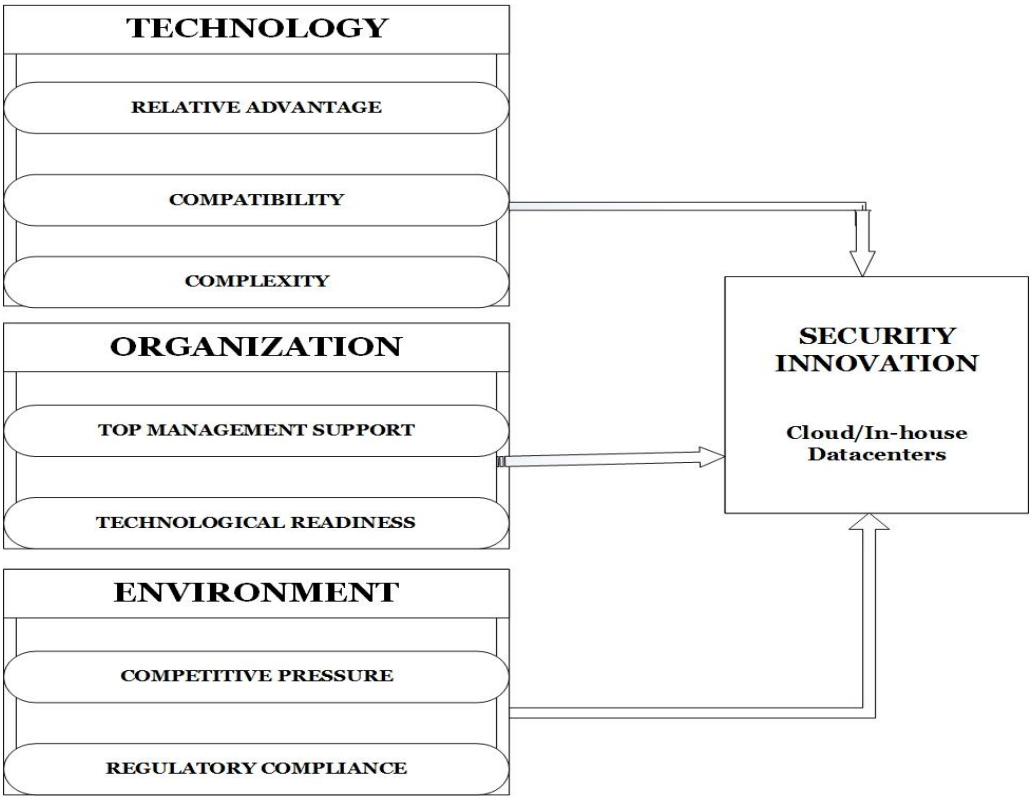
Figure 1: Technology-Organization-Environment Framework



Source: (Tornatzky & Fleischer, 1990)

Ramdani and Kawalck, (2009) examined the TOE in nine SMEs across northwest England and established that the development of broadband development influenced technology, organization, and environment. The TOE framework also received empirical support from studies of other innovations (Thong, 1999).

Figure 2: The Adapted Theoretical Framework



Technological Context

Several influences on the adoption of innovation and five critical characteristics influencing the adoption of innovation (Rogers, 1995) were identified which comprise relative advantage, observability, compatibility, complexity, and trialability. Tornatzky and Klein (1982) argued that only three characteristics that would have the most important influence on innovation were identified, which were relative advantage, compatibility, and complexity. Tornatzky and Klein (1982) reported on ten features, most frequently dealt with in the articles, including compatibility, relative benefits, complexity, cost, communicability, divisibility, profitability, social approval, trialability, and observability, based upon a meta-analysis study of 75 innovation articles. Only

three out of the total number of characteristics of innovation were, however consistent and significant with innovation adoption (compatibility, relative advantage and complexity). This study will now focus on the technological context of only the three constructs.

Relative Advantage

Relative advantage is defined as how much innovation is better seen than the idea it replaces (Rogers, 1995). In this research, relative advantages lie in the management of assets in order to see whether innovative security technologies are suitable. It examines how advantageous new technology is to existing security technologies. The continuous confidential information and privacy of the system shall be ensured by the acquisition, development and maintenance of deployed systems to deter Infosec failure. A relative benefit is taken from the adoption of new innovation as a central indicator. The higher an organization perceives security innovation, the greater the likelihood that innovation can take place (Rogers, 2003; Lee, 2004). Moore and Benbasat (1991) showed that the construct of relative advantage is comparable to the perceived concept of usefulness in the TAM model.

In previous studies, the effects of the relative advantage on technology adoption were widely studied (Premkumar & King, 1994; Gibbs and Kraemer, 2004; Lee, 2004; Ramdani and Kawaiek, 2007). The probability of adoption has been shown to increase if organizations experience a relative advantage in innovation (Thong, 1999).

Compatibility

Compatibility with this research paper will focus on issues including physical and environmental security and how they maintain an institution's existing values and aspirations. The newly defined security mechanisms ought to be in accordance with current policies and procedures. It must be congruent and coherent with the adopting organizations ' values and technological needs from an institutional viewpoint, with the technological and procedural requirements of the innovation (Lertwongsatien & Wongpinunwatana, 2003). This could make a positive impact on the adoption process if the innovation is perceived to be very compatible with the technologies used in an institution (Tornatzky and Fleischer, 1990).

The role of compatibility, a key determinant for IT-innovation adoption, is described in published studies (Rogers, 1983; Teo et al., 1997; Premkumar & Roberts, 1999; Ching and Ellis, 2004; Daylami et al., 2005). For example, Thong (1999) found out in 166 Singaporean small companies that the compatibility of innovation had a major impact on information systems adoption in these enterprises. Likewise, compatibility is considered one of the most important drivers for post-adoption innovation diffusion phases (Zhu et al., 2006). Corporate owners are extremely worried that the innovation adopted does not correspond to their organization's values and technological demands (Jungwoo, 2004).

Once more, the compatibility determinant often has an effect on the use of new technologies (Borgman et al., 2013). The compatibility of security and

control technologies in securing different enterprise systems, hardware and software in the last decade has improved but new security concerns arise, and such issues cannot be dealt with by current security technologies (Hashem et al., 2014). There is, therefore, a better chance of adopting solutions if a company perceives compatibility between its current security technology and control with its datacenter security needs.

Complexity

Complexity pertains to how difficult innovation is perceived to comprehend and use (Rogers, 2003). Rogers (2003) contend that if innovation is regarded as more difficult to use, the adoption will be less likely. In order to increase the adoption rate, new technologies must be user-friendly and easy to use (Sahin, 2006). Innovation features are specific for an innovation that is compatible with the lifestyles of the organization that adopts it. Many recent studies have found that complexity is an important factor in decision-making on innovation (Tiwana & Bush, 2007; Chaudhury & Bharati, 2008; Harindranath et al., 2008).

The need to use security technologies and controls, which are sufficiently flexible to deal effectively with changing requirements, in an educational institution environment can affect the complexity perceived by organizations. Through a higher level of complexity, the successful adoption and implementation of new technology will create a higher amount of uncertainty. (Tornatzky & Klein 1982).

This element is not only negatively linked to the probability of innovation, but also key to the successful integration of new technological innovation in organizations, as opposed to other innovative features (Eder & Igbaria, 2001; Daylami et al., 2005).

Organizational Context

The organizational framework refers to the organization's properties and resources (Tan & Felix 2010). It examines the mechanism and structure of an organization, which restricts or facilitates innovative adoption and implementation (Chau & Tam, 1997). There are two features within the organizational context that are top management support and technological readiness. Support for top management is extremely important for the resources necessary for the adoption of new technology (Low, Chen & Wu, 2011; Wang, Wang & Yang, 2010). The technological readiness means the existing infrastructure and the ability to understand and adopt new technologies for the human resources of IT (Zhu, Kraemer & Xu, 2006; Oliveira & Martins, 2011).

Top Management Support

The support of top management is pivotal for effectively incorporating new innovative technologies in businesses (Eder & Igbaria, 2001). Top management in this study is considered to play the role of sharing power, control and knowledge links. The willingness to invest in security areas such as Infosec training, the development and implementation of information security policies will demonstrate a high degree of management support. Again, risk management

procedures and audibility controls are at stake. The culture of security and thus the desire to take risky decisions will also be affected. In their review of IT indicators and predictors (Jeyaraj et al., 2006) concluded that the main bond between an individual and corporate IT innovation adoption was regarded as top management support. Top management support is generally essential to preserve the importance of any potential change by expressing a vision for the company and sending signals for other members of the firm on the importance of new the technology (Low et al., 2011). As a result, top management support has an impact on the adoption of IT innovation (Thong, 1999; Stuart, 2000; Daylami et al., 2005).

Top management or executive have the power to motivate, acquire, and implement innovations with satisfactory organizational resources (Premkumar & Roberts, 1999). Some researchers have shown that the cultural security of organizations and the enforcement of security policies are expanding after the top management support has been increased (Hu et al., 2012; Knapp et al., 2004).

The top management can express support for security practices by participating actively in security risk assessment, information system security formulations, and the observation of corporate security practices (Kankanhalli et al., 2003). Research findings show that top management support in smaller and big businesses in a range of IS innovations is directly linked to the implementation of new technologies (Thong et al., 1996; Premkumar & Roberts, 1999; Hameed, et al., 2012).

Technological Readiness

As it was reviewed in their paper, (Zhu & Kraemer, 2005) stated that infrastructure, relevant systems, and technical expertise readiness are important factors in the successful adoption of IS innovation (Li et al., 2011) and likewise endorsed by several empirical studies (Armstrong and Sambamurthy, 1999; Zhu et al., 2006). This definition reflects technological readiness, which is complementary not only to physical resources but also to physical assets (Mata et al., 1995). Technological infrastructure provides a platform for the development of e-Businesses, with IT staff providing information and knowledge to develop applications for e-Businesses (Zhu and Kraemer, 2005). This factor can be associated with the decision maker's human features since several studies have found previous experience important for decision-making in technology (Dholakia & Kshetri, 2004).

The availability of financial, technology and human resources affect the intention of organizations to adopt new technology (Hameed et al., 2012). Financial resources include capital available for investment in innovation in technologies, subsequent changes, and ongoing expenditure coverage during use (Dholakia & Kshetri, 2004). Organizations are therefore in a better position to initiate, accept and routinely innovate with greater technological availability.

Environmental Context

Organizations can better introduce, accept and innovate with the increased availability of technology routinely (Low, Chen & Wu, 2011; Oliveira & Martins, 2011). Environmental contexts are the areas within which the Company is responsible for business activities (Tornatzky & Fleischer, 1990), that is the environment of the organization (Teo et al., 2009). The introduction of security innovations can be a result of pressures and environmental exerted support for that organization. Low et al. (2011) recommended that competitive and trading partners pressure be considered as two factors in the environment.

Competitive Pressure

The intensity of competitiveness is considered as the extent to which a rival or competition in the market affects a company (Zhu et al., 2006). Competition can first encourage organizations to launch and innovate to maintain a competitive edge. The strategic basis for IT innovations has been studied in a conceptual context. Porter and Millar (1985) argued that organizations may change their competition rules, influence the structure of the industry and find ways to leverage new ways to surpass competitors. The creation of security expectations will lead to indirect pressure with sensitive data sectors unwilling to innovate. The need to gain a competitive advantage over their competition will once again motivate companies to take security measures.

Another strong incentive to adopt the relevant new technologies is the competitive pressures facing a firm (Majumdar, 2002). Previous empirical studies

have shown the importance of adoption drivers of competitive pressure (Crook & Kumar, 1998). For instance, competition has been reported to be putting strong pressure on organizations to seek new alternatives in order to improve their production (Premkumar & Roberts, 1999). It has been found that a decisive driver of innovation is competitive pressure. In the outsourcing literature, where many organizations are outsourcing their IT infrastructure to improve effectiveness, this factor was also proposed (Lacity & Willcocks, 1998). The better option of new technology can help businesses improve their deal, enabling them to increase their profit margins (Majumdar et al., 1992). Competitive pressures are the level of competition between companies operating in a particular industry (Thong & Yap, 1995).

Porter and Millar (1985) have established five competitive forces, including new entrants, customer bargaining power, supplier bargaining power, product and services substitutes, and market rivalry. The last two of these competing forces, the rivalry between companies and the potential threat of substitution in products, are attributed to competitive pressure in this study. It should be noted however that companies in a far more competitive environment are being pressured to move swiftly from one technological innovation to another by competitive pressure (Abrahamson, 1991). Mata et al. (1995) argue that the chance for organizations to learn gradually, carefully, and sustainably is reduced through the cycle of developing skills.

Regulatory Compliance

Compliance with regulations can influence competitive pressures favorably or adversely for organizations. Competitor pressures, laws, rules, and professional standards may support or impede decisions including personal privacy and customer privacy. The geographical position of the organizations will implement certain security policies to ensure decent safety practices in business. The outside environment can directly influence the decision of the company. The environment has been understood as a critical element affecting innovation dissemination in the environmental context (Zhu et al. , 2006). For example, the company's views on compliance, economic advantages along with non-compliance costs were highly affected by conformity with Infosec (Bulgurcu et al., 2010). This idea is similar to the government policy which has been tested and empirically tested in relation to IT diffusion (Umanath & Campbell, 1994).

It has been established that companies in a public policy environment have minimum IT adoption (Zhu and Kraemer, 2005) as organizations from their operating environment are increasingly pressured to innovate or achieve such legitimacy. Similarly, (Herath & Rao, 2009; Shaw, 2012; Kankanhalli et al., 2003) have observed that failure to respect security policies causes fear and, therefore, compliance with safety measures. For instance, the existence of various Infosec laws and regulations often obliges organizations to innovate and to act to ensure credibility by government departments (Edwards et al., 2009). All of this is in agreement with Kraemer et al. (2006) who summed up two ways that public regulation could impact on innovation diffusion. Organizations often cited

inadequate legal protection as contentious issues for e-business activities for online business activities, unclear business law and concerns about security and privacy (Kraemer et al. 2006). However, the literature on innovative adoption finds external pressure within the geographical location of an organization in terms of regulations, norms and compliance as drivers of innovation and survival (BEN-NER & Lluis, 2011).

Conceptual Review

Innovation Adoption

Innovation is a complex construct and is studied from multiple perspectives at different levels of analysis by scholars from a variety of academic disciplines. At the organizational level, researchers have generally defined ‘‘innovation’’ as the development (generation) and/or use (adoption) of new ideas or behaviors (Amabile 1988; Damanpour & Wischnevsky 2006; Zaltman, Duncan, and Holbek 1973). Others defined innovation as “a technology or practice that an organization is using for the first time, regardless of whether other organizations have previously used the technology or practice” (Klein, Conn, & Sorra, 2001, p. 811). Researchers such as Drucker (1985) defined innovation as the specific tool of entrepreneurs, the means by which they exploit change as an opportunity for a different business or service.

The benefits associated with innovation are crucial as Porter (1990) argued that companies achieve competitive advantage through acts of innovation. They approach innovation in its broadest sense, including both new technologies and

new ways of doing things. Some organizational researchers regard innovation as a process of bringing new, problem-solving, ideas into use (Kanter, 1983). Again, Mexias and Glynn (1993) defined innovation as "non-routine, significant, and discontinuous organizational change that embodies a new idea that is not consistent with the current concept of the organization's business" (p.78).

It has been argued that innovative outputs depend on the prior accumulation of knowledge that enables innovators to assimilate and exploit new knowledge (Damanpour & Wischnevsky, 2006). The adoption of innovation in a broader sense can be explained as a process that results in the assimilation of a product, process, or practice that is new to the adopting organization.

Stages of Innovation Adoption.

The organizational adoption of an innovation is not a binary event but rather a stage-based process that unfolds over time (Fichman & Kemerer, 1993). Studies on organizational innovation adoption, therefore, target distinct stages on the adoption continuum, the stages used to describe the adoption process (Fichman & Kemerer, 1993). As such, ambiguity in the conceptualization of the adoption construct can lead to issues with misinterpretation and misunderstandings of both the research model and results (McKinnie, 2016).

From a technological diffusion perspective, adoption describes the organizational effort directed toward diffusing an IT innovation throughout the firm (Cooper & Zmud, 1990). In the views of Rogers (1995), the adoption of innovation starts with the firm's initial awareness, knowledge, and evaluation of

the innovation. These initial stages include "both identifying and prioritizing needs and problems on one hand, and searching the organization's environment to locate innovations of potential usefulness to meet the organization's problems" (p. 391).

Following the decisions to adopt comes restructuring or re-invention of the innovation to fit the organizational needs, clarification of the role and purpose of the innovation, and routinization of the innovation by incorporating it into the regular activities of the firm. Adoption usually starts with the recognition that a need exists and moves to searching for solutions as it has been argued by (Damanpour and Schneider 2006; Gallivan 2001; Mendel et al. 2008). The initial decision to attempt the adoption of a solution and finally to the actual decision to attempt to proceed with the implementation of the solution (Damanpour and Schneider 2006; Gallivan 2001; Mendel et al. 2008).

Hence, drawing upon the innovation diffusion literature (Rogers, 1983; Fichman, 1999), security innovation is defined in terms of assimilation; the sequence of stages from a firm's initial awareness and evaluation of security innovation, to the formal allocation of resources for its acquisition and deployment, and, Finally to its incorporation of the technology into the regular activities of the firm:

While some studies depict assimilation as a six-stage process (Cooper & Zmud, 1990; Fichman, 2001), others use a seven-stage model (Rai, et al., 2009; McKinnie, 2016; Greenhalgh et al. ,2004) characterized in the adoption process:

pre-adoption (awareness of innovation), peri-adoption (continuous access to innovation information), and established adoption (adopters' commitment to the adoption decision). Alternatively, Frambach and Schillewaert (200) discussed two stages associated with adoption: the organization's decision to pursue adoption and the staff's acceptance and initiation of their individual processes of accepting the innovation.

Datacenter Definition

The concept datacenter has been defined as consisting of backup power supplies, network connection mediums and security policies governing the running of core applications as well as environmental conditions which include air conditioning, humidity and fire systems (Frihati, Moldoveanu, & Moldoveanu, 2009). On the other hand a datacenter is viewed as a physical or virtual infrastructure used by many enterprises to put their networking systems and components for the company's information technology needs Lam, Zhao, Xi and Chao (2012) which typically involve storing, processing and serving large amounts of mission critical data to clients

Kant and his colleagues (2011) have outlined the characteristics of datacenter network infrastructure which is : Stable, secure and reliable, in line with the organization regulations and meets organization customers or users need, supports modern technologies such as virtualization and cloud computing, scalable and can easily meet the requirements of organizations network communications in peak usage. (Kant, Le & Jajodia, 2011).

In today's information era datacenter represents the core of many organizations for achieving their own business objectives. Several researchers have emphasized on the reliance of data stored by organizations for interacting with employees and customers. Organizations highly relied on data stored in their data center to interact with its employees and customers (Lam, Zhao, Xi & Chao, 2012; Udez , Okafor, Inyiama & Okezie, 2012). The components and technologies that make up data center networking generally include:

- ✓ Networking equipment (routers, switches, modems, etc.)
- ✓ Network cabling (LAN/WAN and network interface cabling)
- ✓ Network addressing scheme(IP v4 or IP v6)
- ✓ Network security (security protocols/encryption algorithms, firewalls, IDS, etc.)
- ✓ Internet connectivity (satellite, DSL, wireless, optical)

Datacenter is not a choice but rather an integral part of modern organizations. It can be considered as an area that holds, a means of hosting critical data, applications, and servers, as well as contains basic assets of customer information, intellectual property, and other business critical data. Communication among organizations is delivered through creating connection within them. In the view of Carrie (2014), proliferation of technologies especially internet-based ones make data centers more prone to security attacks. Security attacks on data center may destroy the whole organization's network and data.

Bagchi and Udo (2003) added up to the security aspect by arguing that with the internet growing at a faster rate various forms of attacks are directed towards data center networks that hinder it. They further advocated for proper security features to ensure a reliable service delivery.

Characteristics of Datacenter

The process of building data center facility appears to be simple on the inception but, it has several aspects that must be done correctly. Perrin (2014) has elaborated on features that should be considered during the designing phase of data center. The following are some of the characteristics of data center that has been listed by Perrin.

- ✓ Manageability: is core attribute of a data center that should be in the first place. A data center should provide easy and integrated management of all its elements. That can be achieved through automation and reduction of human intervention in common tasks.

- ✓ Availability: a data center should function and be accessible every day for assuring the availability of information whenever required. In short, it means that there is no downtime. Unavailability of information leads to loss of information and could cost a lot to the business of an organization.

- ✓ Fault Tolerance: is the property that enables a data center to continue operating properly in the event of the failure (one or more faults) of its components. If its operating quality decreases at all

then, it is proportional to the severity of the failure. Fault tolerance is particularly required after highest availability.

- ✓ Security: is a notion such that standards, policies and procedures are central components and to meet together to prevent unauthorized access to the information.

- ✓ Scalability: is a planned, monitored, predictable nature for the growth of data center infrastructure. Business growth is almost in a continual progress that always requires deploying more servers, applications and additional databases etc.

- ✓ Performance: is a means to measure the state of all elements found in the data center infrastructure to establish a comfortable environment for service delivery. Performance management is to make sure that all the elements of the data center provide optimal functionality at the required level.

- ✓ Capacity: is a necessity of an organization to rely upon their data center to provide the service. When capacity requires increase, the data center must provide additional capacity without interrupting availability or with minimal disruption.

- ✓ Monitoring: is a continuous process of gathering information on various elements and services running in the data center. The reason is to come up on with predicting unknown events in the data center.

- ✓ Reporting: is a contextual generation of information about resources performance, capacity and other utilization information gathered together at certain point of time (Perrin, 2014).

Cloud Computing Definition

Several studies have suggested that it is not easy to define cloud computing (Kim, W, Kim, SD, Lee, E & Lee., 2009). It has been concluded that the definitions of cloud computing have changed consistently over the years and there is the possibility of further alterations in the years to come (Kim, W, Kim, SD, Lee, E & Lee., 2009). Other scholars have expressed related concerns, for instance Vaquero et al. (2009) and Weinhardt et al. (2009) reckon that the lack of well-established definition for cloud computing has made the concept to be confused with related technologies such as grid computing. Moreover, other scholars have called for a universally acceptable definition of cloud computing. For instance, it has been argued by Vaquero et al. (2009) that it is essential in arriving at a cohesive definition that clearly spells out the scope of research in that field and the probable benefits that are associated with cloud computing.

The Berkeley definition which is considered to be the first and commonly cited definition of cloud computing was published by Armbrust et al. (2010). It states that: Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

The widely used definition of cloud computing is the one provided by the National Institute of Standards and Technology (NIST) (Mell & Grance, 2012). They defined cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2012, p. 2).

The NIST (2009) definition captures most element of the cloud computing concept that is the characteristics, services, deployment modes and the foundation or underlying technologies. As seen in previous definitions, the burden is lifted from customers and given to service providers the set of configurations and activities that makes the system work. The differences in the definition of cloud computing is seen in the differences of aspirations, visions of various stakeholders in the areas of engineering, education, developers, designers, consumers and management. The core elements in most definition has focused mainly on the technical and service features of cloud computing.

Cloud Service Delivery Models

Cloud computing has three service models or layers which are hierarchically structured. They include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The infrastructure layer according to Zhang, Cheng and Boutaba (2010) provides the base upon which

other services are delivered and hence lower layers provide services to above layers

Software as a Service (SaaS)

Researchers such as Masiyev, Qasymov, Bakhishova and Bahri (2012) concluded that the most visible layer of cloud computing layers is the SaaS that delivers on-demand applications over a network. It delivers those services due to the underlying infrastructure of cloud computing in which service providers are tasked with the duties of configuring, managing and controlling.

Again, an overview of how SaaS layers work has been given by Dillon, Chen and Chang (2010) that end-user applications are organized in a single logical environment which has the purpose of achieving economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance. Examples of SaaS applications include: Gmail, Google Drive, Dropbox, Google Apps Office 365, Facebook, Twitter, Salesforce, Netsuite.

Platform as a Service (PaaS)

At the middle of the cloud hierarchy architecture is the PaaS service model in which Zhang et. al (2010) stated that resources such as operating systems support and framework for software development are provided by this architecture layer. In line with the words of Masiyev et al, (2012), it is a cloud architecture layer that can be used to launch operating systems and other hardware independent application development through frameworks by software developers. End users have the ability of configuring environmental variables and

controlling deployed application but cannot access the underlying infrastructure. Examples of PaaS include: Windows Azure, App Engine, Coghead, Pipes, Dapper.net, Amazon's Relational Database Services, and Rackspace Cloud.

A key distinction between SaaS and PaaS is that SaaS hosts completed applications in the cloud whiles PaaS gives the development platform for hosting both completed and uncompleted or in-progress applications. PaaS platform reduces the cost, difficulties and complexity of purchasing, managing and configuring related hardware and software for development purposes

Infrastructure as a Service (IaaS)

Numerous researchers have given their explanation for this layer and Zhang et al, (2010) described the IaaS layer as the foundation environment on which the cloud computing in built involving on-demand provisioning of infrastructural resources. Again, Buyya, Ranjan, and Calheiros (2010) saw IaaS as a means of building and environment where end-users can perform activities such as starting and stopping it, configuring access permissions and firewall rules and customization by installing applications, fixing virtual disks.

Cloud Deployment Models

There are several models in which cloud services are deployed to customers and that the model deployed is based on technical, business and operational requirements of end-users (Masiyev et al., 2012). The deployment models for cloud services include: private clouds, public clouds, hybrid clouds, and community clouds with each have its benefits as well as drawbacks

Public Clouds

Public cloud is regarded as a cloud which is made available in a pay-as-you-go manner to the general public (Armbrust et al., 2010). Savu (2011) also shared his thought on public clouds and has defined it as a cloud that is sold to the public and considered a cost-effective way to deploy IT solutions. The cloud infrastructure is made available for use by general public cloud consumers and is owned by an organization selling cloud services with its own policy, and charging model

Public cloud services are rendered to the public at reduced prices and in most cases does not require initial infrastructural investments from end-users. The users of the cloud pay for the services being received and all risks involved are taken care of by the cloud providers. The categories of entities that can own public clouds include business organisations, academic institutions, and governmental organizations. Examples of public clouds include: Amazon EC2, S3, Google AppEngine, and Force.com.

Private Clouds

Most organisations decide to rather set up their own private clouds for exclusive usage rather than public cloud (Zhang et. al, 2010). Private cloud can be explained as an internal datacenter of a business or other organization, not made available to the general public (Armbrust et al., 2010). When private clouds are deployed, the business units within the organization rather become the consumers or end-users of the private cloud. Instead of allowing third parties to build and

manage the cloud, an organization can decide to do it themselves or both in which the infrastructure can be situated in-house or off-premises

Hybrid Clouds

The introduction of hybrid clouds is seen as a means of finding solutions to the shortcomings or weaknesses of both private and public clouds (Zhang et. al, 2010). Hybrid clouds offer on-demand services from external resources, capabilities and expertise which at the same time comply with internal resources and expertise. Hybrid cloud infrastructure consist of two or more cloud infrastructure in which organizations use to optimize their resources whiles controlling mission-critical activities in-house by using private clouds (Dillon et al., 2010). The main premise is that non-critical activities or information are outsources possibly in the public cloud whiles mission-critical and sensitive business services and data are kept within organizational control

Community Clouds

Community clouds are owned or managed by single organization within a specific community or by multiple organisations in which the creation and management of the cloud infrastructure can be outsourced to a third party (Mell & Grance 2012). It is, further, argued that shared interest such as policies, requirements, values, concerns and compliance are the motivating factors (Mell and Grance, 2010; Marston et al., 2011). Community clouds can be hosted internally by a member of a community or outsourced to a third-party vender. The

reasons for community clouds could be due to shared policies, shared mission, security concerns or requirements of the parties involved

Empirical Review

There have been some empirical studies that evaluate organizational security practices and their effectiveness but not the drivers for security innovations. Siponen, Mahmood and Pahnila, (2009). provided a conceptual foundation for organizational information security whereas Vroom and von Solms (2004) provided components of effective security Protection motivation and deterrence governance, including information security policies. Both of these papers discuss the role of human factors in the success of security initiatives. In a similar vein, von Solms (2001) has argued that information security is a multidimensional discipline and that various dimensions such as the human/personal dimension and the policy/ governance dimension have interconnected roles that impact overall organizational information security. As Dhillon and Backhouse (2001) have pointed out, there is a great need for more empirical research that uses socio-organizational perspectives to develop key principles for the prevention of negative events in order to help in the pursuit of information security innovations in organizations by management

In a related work, Albrechtsen (2007) conducted a qualitative study of user views on information security and found that users do not perform many information security actions and that they prioritize other work tasks in front of information security. Albrechtsen (2007) argued that the main problem regarding

user roles in information security work is their lack of motivation and knowledge regarding information security and related work within organizations.

In an evaluation of security policy compliance, Chang (2007) studied the security climate in organizations and found that management practices and co-worker socialization have an impact on employee perceptions of the information security climate which, in addition to self-efficacy, positively impact security policy compliance behavior. Similarly, Stanton et al. (2003) examined the effect of organizational commitment on a variety of security behaviors including security policy compliance. It was found that employee attitudes, normative beliefs, and habits all have a significant effect on employee intentions to comply with IS security policy whereas threat appraisal and facilitating conditions have a significant impact on shaping attitudes towards compliance.

In another research work, He et al. (2016) proposed an organizational-level security evaluation framework to alleviate the security information asymmetry issue. Specifically, the authors designed a policy for organizations' security information disclosures to provide more economic motivations for organizations to improve their Internet security protection. Such disclosure of information helped reduce the information asymmetry issue within organizations. Due to insufficient internal resources and policies, organizations may not have a full understanding of their security problems (D'Arcy et al. 2009). Organizations will underinvest on security when their customers cannot distinguish companies with strong security from those with weak security. Publicizing evaluation reports

can force organizations to raise their security awareness for the fear of losing customers to their competitors (Gal-Or & Ghose, 2005; Tang et al., 2013).

In a related work, Knapp et al. (2006) also identified senior management as key players as the study found that senior management support is positively related to both an organization's security culture and the level of policy enforcement. While the study did not directly explore managerial intentions for innovative information security adoption it did again highlight the importance of management involvement, thus the importance of managerial information security awareness in affecting an organization's information security readiness

Furthermore, Mouratidis, Jahankhani, and Nikhoma (2008) provided empirical support for a positive relationship between awareness and action. In other words, the higher the level of organizational information security awareness, the more likely that it will take action in implementing preventative measures. The study suggested that preventative action usually occurs after the fact. That is, unless an actual information security breach has occurred, organizations usually take no action in adopting security measures. Like various similar studies, Namjoo et al. (2008) implied that by raising organizational information security awareness, information security performance could in fact improve information security performance.

Again, Yeo, Rahim and Miri (2007) explored security risk assessment strategies of an Australian University by identifying security awareness as an important component which must be assessed as part of an organization's risk

assessment. User noncompliance is a serious risk for any organizations, and awareness is positively related to compliance. The study concluded that information security awareness of employees must be risked assessed as part of an overall organizational risk assessment strategies in order to identify areas which need improvements. In other words, the lack of information security awareness poses serious threats to an organization and must be properly risk assessed and mitigated.

Moreover, Hagen, Albrechtsen and Hovden (2008) studied the implementation of organizational security measures and to assess the effectiveness of such measures. It was discovered that many Norwegian organizations placed emphasis on the policies and procedures in implementing any measures, but placed very little emphasis on security awareness. The study also showed that awareness measures were the most effective of any security measures. As a consequence, the study showed an inverse relationship between the implementation of security measures and their effectiveness. In other words, it is important to place emphasis on security awareness as well as technical controls when adopting security programs.

Summary of Literature Review

Despite recent attention in organizational security issues by several researchers, the investigation of determinants for security innovations is still embryonic and poses many opportunities for empirical research. These studies have focused primarily on understanding employees' attitudes, and behavior on

information security compliance in organizations. The studies provide an understanding of how human, organizational, and technological elements interplay to explain how different factors lead to sources of security breaches and vulnerabilities within organizations. In spite of the importance of innovation adoption to the organization, information security literature exhibits a knowledge gap in understanding and identifying the factors that influence the security innovation adoption process. The set of factors that either facilitates or hinders security innovation adoption are yet to be identified. There is, however, the need for better understanding of the drivers of institutional innovativeness on information security compliance in organizations with a thorough understanding of factors underlying the innovation adoption decisions by potential adopters

CHAPTER THREE

METHODOLOGY

Introduction

This chapter relates to the research design and the rationale for the design. It also deals with the population, sample and the sampling procedure. Again, it looks at the instruments used, how they were developed, data collection procedure and data analysis.

Research Design

Researchers argued that a research design is the conceptual structure within which research would be conducted (Dawson, 2002). This study adopted the descriptive research design. Descriptive research was used because; the data collected examined the determinants of cloud datacenter adoption within higher education institutions. Descriptive research was deemed most appropriate for the study because it involved the collection of data in order to answer questions concerning current status of the subject matter under study. Glatthorn aruged that the purpose of descriptive research is to describe a phenomenon (Glatthorn, 1998). Descriptive studies report frequencies, averages and percentages from which conclusions can be drawn from numerical values presented.

Fraenkle and Wallen (1993) have listed the following as advantages of descriptive research:

1. It provides a good number of responses from numerous people.

2. It provides a meaningful picture of events and seeks to explain people's perception and behavior on the basis of information obtained.

3. It can be used with greater confidence with regard to particular questions which are of special interest and values to a researcher.

They also provided the following demerits:

1. Answers can vary greatly depending on the exact wording of the questions or statements.

2. It can produce untrustworthy results because they may delve into private and emotional matters that respondents may not be completely truthful about it.

One major weakness of descriptive research is that answers do not enable us to understand why people feel, think or behave in a certain manner, why programs pose certain characteristics, why a particular strategy is used at a certain time and so forth. In spite of these couple of demerits, the rationale for selecting this design was to enable more respondents to be questioned. Also, it allows for greater degree of accuracy, reliability, standardizations of measurement and uniqueness of the study.

This research was approached from the quantitative perspective and in the view of Glatthorn (1998), quantitative perspective indicates that there is an objective reality that can be expressed numerically and be described. Furthermore, a survey design provides a quantitative or numerical description of trends,

attitudes or opinions of a population by studying a sample of that population (Creswell, 2003). From the sample results, the researcher can generalize or make claims about the population.

This study therefore used a cross-sectional survey design which scholars contend is one of the main quantitative methods now well-accepted in the social sciences (Avison & Myers, 2002). The survey strategy was chosen for this study due to convenience and for parsimony reasons. Survey make it possible to reach a large and geographically disperse group of institutions, while at the same time collecting data about each individual respondent in an effective and inexpensive manner.

Additionally, a self-administered survey has the benefit of allowing the respondents to answer anonymously and at their own convenience and is therefore, perceived to be less likely to contaminate or distort the respondent's answers (MacKenzie & Podsakoff, 2012; Saunders, et al., 2007). Again, in research on technology adoption, surveys and case studies have been the dominant strategies at the individual and organizational level (Choudrie & Dwivedi, 2005). Another reason for choosing the survey strategy is that it provides a better basis for generalizing, allow for replicability, and permit some degree of statistical power (Bouchard, 1993). In a cross-sectional survey, the phenomenon of interest and data are collected at one point in time from selected sample to describe some larger population (Pedhazur & Schmelkin, 1991).

Unit of Analysis

It has been established that individuals and organisations have been studied on regular basis and this is echoed by Ramdani (2008) who argued that individuals and organisations are entities widely used as units of analysis for studying the acceptance of technology innovation. This study intends to investigate the determinants of security innovations at the Colleges of Education at the organization level.

Population

Many researchers have attempted to define population and have described it as "the total of all elements that share some common set of the characteristics" (Hair, Black, Babin, Anderson, & Tatham, 2006, p 170). Other scholars argued that in quantitative research, it is important that the sample in use reflects the characteristic of the population under study such that results drawn from the study are applicable to a wider population for the sample to be representative: the higher the representativeness, the higher the generalizability of the findings, the higher the quality of the study (Sarantakos, 1998)

The accessible population for this study consisted of management staff, lecturers and IT support staff at Colleges of Education within the central region. IT support staff are included due to their role and daily interaction with IT related devices and services of which security is paramount in those interactions. Lecturers are included because of their application of IT services in the teaching and learning processes which ought to be done in a secure manner. Again, as

educators they possess the platform for creating awareness of security issues in the discharge of their duties. Management staff are included because they are considered as policy implementers and they influence IT and security innovation adoption at their various Colleges of Education.

Sample and Sampling Procedure

The sample for the research will be chosen from Colleges of Education in the Central Region. Out of the total of 38 public Colleges of Education in Ghana, 3 Colleges of Education were selected for the study. The selection was based on the argument by Amedahe & Asamoah-Gyimah (2003) that in most quantitative studies, a sample size of 5% to 20% of the population size is sufficient for generalization purposes. The sample size selected for the study was based on Krejcie & Morgan's recommendation for determining a sample size from a given population (Krejcie & Morgan, 1970).

Table 1: Determining the sample size of a population

Population Size	Sample Size	Population Size	Sample Size	Population Size	Sample Size
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346

Source: (Krejcie & Morgan, 1970)

Based on Krejcie and Morgan's (1970) assertion, the sample size considered for the target population of 1,300 will be 300. The sample size will consist of 27 management staff, 228 lectures and 45 IT support staff. The sample will thus comprise 9 management staff, 76 lecturers and 15 IT support staff from each of the selected Colleges of Education.

Research experts have put forward the argument that the sample technique and sample size used in research are usually influenced by the availability of the resources (Saunders, Thornhill & Lewis, 2009). Probability sampling was used for this study due to its benefits which includes improving generalization from data collected from a population and most importantly the larger the size, the lower the likelihood of error in generalizing to the population (Saunders et. al, 2009).

Probability sampling also referred to as representative sampling gives equal chance for each unit in the population to be selected. This enables researchers to answer a research question that meets the objectives of the research and to estimate statistical characteristics of the population from the sample (Saunders et. al, 2009). Probability sampling is consistent or typically associated with a survey research strategy.

The type of probability sampling used for the study was stratified random sampling to help identify the stratum in the population (Saunders et. al, 2009). As a result, management staff, lectures and IT support staff were the relevant stratum and the actual representation in the population. Stratified sampling is a sampling technique in which the population is divided into a number of strata and sample is

drawn from each stratum. These sub samples makes up the final samples of the study.

Stratification is used to help lower known variances, in the population (Lohr, 1999). Thus, the rationale of stratification or stratified random sampling helps to increase precision and representativeness. It is, therefore, very economical, offers accurate results and a high degree of representativeness (Lohr, 1999). A representative number of respondents was asked to take part in the research study on the basis of strata comprising management staff, lectures and IT support staff which will be representative enough of the population.

Instrumentation

In this research project the self–administered questionnaire was used. The adoption of quantitative techniques and survey research methods is a widely used strategy for data collection on innovation adoption as against other alternatives (Williams, Dwivedi, Lal & Schwarz, 2009). This is evident in the sense that survey aid in the investigation of the relationships between variables and to produce models of these relationships.

Furthermore, researchers such as Hair et al. (2006) contend that Likert scales are best suited for self-administered survey methods to collect data. Five point Likert-type scales are one of the most commonly used survey formats. The belief is that scales with more than 7 points are confusing (Likert scale & surveys – best practices, 2007). The scale in the questionnaire was coded in a 5-point Likert-type scale ranging from 1 "Strongly Disagree" to 5 "Strongly Agree" as follows:

Option 5: Strongly Agree,

Option 4: Agree,

Option 3: Neutral,

Option 2: Disagree,

Option 1: Strongly Disagree.

Since the response scale has been utilized in similar studies, researchers will have possible wider range of scores and increased statistical analysis (Premkumar & Ramamurthy, 1995; Pallant, 2007). The constructs, measurement items and sources for the survey items are presented in Table 2

Table 2: Constructs and Survey Measurement Items

Construct	Measurement Items	Adapted Source
Relative advantage	**RA1:** Using innovative security technology would make it easier to prevent authorized access and denial of service on our systems **RA2:** Using innovative security technology would improve monitoring and control of communication on our systems **RA3:** Using innovative security technology would enable us to use cryptography to protect against disclosure more quickly **RA4:** Using innovative security technology would enhance our effectiveness in managing malicious code execution **RA5:** Using innovative security technology allows us to protect the confidentiality and integrity of transmitted information. **CY1:** Working with security technology is complicated, it is difficult to understand operational procedures	(Chau and Tam, 1997;Ramdaniet al., 2009; Thong, 1999)

Complexity	**CY2:** It takes too long to learn how to use security mechanisms to maintain audit logs to make it worth the effort **CY3:** Learning to operate innovative security technology is easy for me **CY4:** It takes too much time for me if I want to use secured connection to do my normal duties **CY5:** In general innovative security technology is very complex to use	(Chau and Tam, 1997; Moore and Benbasat, 1991)
Compatibility	**CM1:** I think using innovative security technology fits well with the way our institution usually performs **CM2:** Using innovative security fits into our institution's work style **CM3:** Using innovative security technology is compatible with our institution's norms and culture **CM4:** Innovative security technology can easily be integrated into our existing IT infrastructure **CM5:** Innovative Security technology is NOT compatible with other systems that we are using	(Ramdaniet al., 2009; Thong, 1999; Moore and Benbasat, 1991)
Top Management Support	**TM1:** Top management provides resources for adopting security innovations **TM2:** Top management supports the implementation of security innovations **TM3:** My top management is likely to consider the adoption of security technology as strategically important **TM4:** The Institution's top management provides strong leadership and engages in the process when it comes to information security technologies **TM5:** Our top management exhibits a culture of enterprise wide information sharing.	(Premkumar and Roberts, 1999
Technological Readiness	**TR1:** My institution hires highly specialized or knowledgeable personnel for security technology services. **TR2:** We have sufficient technological resources to implement innovative security systems – unrestricted access to computer.	(Oliveira and Martins,2011)

	TR3: We have sufficient technological resources to implement security systems – high bandwidth connectivity to the internet. **TR4:** We allocate a percent of total revenue for security technology implementation in my institution**.** **TR5:** Our organization has the in-house expertise to implement security systems	
Competitive Pressure	**CP1:** Our institution thinks that innovative security technology has an influence on competition in their industry **CP2:** Our institution is under pressure from competitors to adopt security systems **CP3:** Some of our competitors have already started using innovative security technologies **CP4:** It is easy for our customers/students to switch to another institution due to secure security systems in place **CP5:** We believe that our competitors get many advantages from using security systems	(Kuan and Chau, 2001)
Regulatory Compliance	**RP1:** Ghanaian laws and regulations are sufficient to protect and facilitate the use of security systems **RP2:** Specific and individual controls to meet security systems policies are well documented in my institution **RP3:** Our institution has an implemented procedure to ensure compliance with legal restriction and intellectual property **RP4:** Ghanaian universities and colleges will be adopting security innovations in the near future **RP5:** My institution conducts regular review to ensure compliance with security policies	(Zhu and Kraemer, 2005)

Measuring Security Innovation Adoption

In order to access security innovation assimilation, a seven item Guttmann scale was developed to operationalize the aggregated, two-stage model of security. Each of the seven items corresponds to a distinct assimilation stage: (1)

non-awareness, (2) awareness, (3) interest, (4) evaluation/trial, (5) commitment, (6) limited deployment, and (7) general deployment. The scale is similar to the one that Fichman and Kemerer (1997) used to assess adoption of software process innovations, the scale that was used to measure assimilation of electronic procurement innovations (Rai, Brown and Tang, 2009) and the scale that McKinnie (2016) used to operationalize the adoption of cloud computing. The items are summarized in Table 3.

Table 3: Scale for Measuring Security Innovation

Stage	Criteria to enter	Item	Assimilation stage
1. Non-awareness	The institution is unaware of security technology	My institution is not familiar with security technology	
2. Awareness	The institution is aware of security technology	My institution is familiar with security technology and /or has considered using it	
3. Interest	The institution is committed to actively learn more about security technology	My institution is planning to use security technology within the next 24 months	**Non-Adoption**
4. Evaluation/ Trial	The institution has initiated evaluation or trial of security technology	My institution has launched pilot projects or initiatives for evaluating and/or trailing security technology	**Adoption -decision**
5. Commitment	The institution has committed to using security technology in a significant way	The acquisition of specific security technology are planned, in progress, implemented or cancelled	

Table 3: Scale for Measuring Security Innovation (Cont'd)

Stage	Criteria to enter	Item	Assimilation Stage
6. Limited Deployment	The institution has security technology but a program of limited use	My institution has security technology but we have yet to establish a program of regular use	
7. General Deployment	The institution has security technology and a program of regular use	My institution has security technology and we have established a program of regular use	

Source: (Fichman and Kemerer, 1997; Rai, Brown & Tang, 2009; McKinnie, 2016)

Validity and Reliability

Validity is defined as the extent to which any measuring instrument measures what it is intended to measure (Bryman & Hardy, 2004). The concept of validity has been summarized by Ghosh and Chopra (2003) as "Absence of self-contradiction" (p.56). Essentially, validation is related to the extent to which the research method describes what it is supposed to measure.

Reliability is concerned with how much random error there is in the measurement. The reliability of the questionnaire is concerned with the consistency of the responses to the questions (Gill & Johnson, 2002). With the intention of testing the properties of measurement scales, the Cronbach's coefficient Alpha was used to test the constructs for validity and reliability.

Data Collection Procedure

Data collection as a term has been described by Weimer (1995) as the process of preparing and collecting data. Consent was sought with respect to the collection of data after which the questionnaire were administered to respondents. Data was collected when respondents are done with responding to questionnaires and this took a period of one week.

Data Analysis

The Statistical Package for Social Sciences (S.P.S.S) software version 23 was used to analyze the data. The list of hypothesis as well as statistical tool used to test it is outlined in Table 4

Table 4: Hypothesis and Statistical Tool for Analysis

Hypothesis	Statistical Tool
H_O1	**Two Way ANOVA**
H_O2	**Two Way ANOVA**
H_O3	**Binary Logistics Regression**
H_O4	**Binary Logistics Regression**

Source: The Researcher (2019)

CHAPTER FOUR

RESULTS AND DISCUSSION

Introduction

The study sought to explore the determinants of security innovations in 3 selected Colleges of Education in Ghana. A set of questionnaires were administered to 27 management staff, 228 lecturers and 45 IT support staff of the selected institutions for the purpose of data collection. The data was analyzed by using a combination of descriptive and inferential statistics. The return rate for the questionnaire was 100%. The results are, therefore, presented and discussed in this chapter. The chapter is organized into two sections. The first section deals with the presentation of the background information while the second section focuses on the presentation and discussion of the main results of the study.

Background Information of Respondents

Items in the first section of each questionnaire were meant to elicit responses on the background information on the respondents. Table 5 shows the results on the gender of the participants.

Table 5: Sex of Respondents

	Top Management		Lecturers		IT support Staff			
Gender	**No.**	**%**	**No.**	**%**	**No.**	**%**	**Total**	**%**
Male	16	59.3	170	74.6	24	53.3	210	70
Female	11	40.7	58	25.4	21	46.7	90	30
Total	27	100	228	100	45	100	300	100

Source: Field Survey (2019)

The results in Table 5 indicate that out of the 300 participants, 210(70%) were males whiles 90(30%) were females. Again, top management had 16(59.3%) males with 11(40.7%) females. Moreover, there were 170(74.6%) males for the lecturers and 58(24.4%) females. IT support staff had 24(53.3%) males and 21(46.7) females. This indicates that there were more males than female respondents in this study

The researcher also sought to find out the age range of the participants in the study. The results are presented in Table 6.

Table 6: Age Range (N = 300)

Age Range (Years)	Top Management		Lecturers		IT support Staff			
	No.	%	No.	%	No.	%	Total	%
18-25	-	-	-	-	5	11.1	5	1.7
26-35	-		3	1.3	16	35.6	19	6.3
36-50	6	22.2	191	83.8	17	37.8	214	71.3
51-60	21	77.8	34	14.9	7	15.6	62	20.7
Total							300	100

Source: Field Survey (2019)

From Table 6, it can be observed that 214(71.3%) of the respondents fell within the age range of 36-50. Moreover, 62(20.7%) of the respondents were within 51-60 age range. Again, 19(6.3%) were within 26-35 age range while only 5(1.7%) within 18-25 years. This implies that most of the workers at the various Colleges of Education are not too old and are more likely to be abreast with modern technology. These respondents would, therefore, be able to provide the relevant information that relate to the success of this study.

Table 7: Work Experience (N=300)

Work Experience in Years	No.	%
Less than 2	5	1.7
3-5	50	16.7
6-10	100	33.3
11-20	113	37.7
More than 21	32	10.7
Total	300	100

Source: Field Survey (2019)

Table 7 illustrates the work experience of the respondents at the Colleges of Education. It was found that out of the 300 workers, only 5(1.7%) had been working for less than two years. Also, 50(16.7%) had worked 3-5 years, 100(33.3%) for a period of 6-10 years. Majority of the workers 113(37.7%) had worked within 11-20 years whiles 32(10.7%) had an experience of more than 21 years. This implies that most on the respondent were well experienced in the work they do at the various Colleges of Education which will be reflected in their responses.

Table 8: Name of Institution (N=300)

Colleges of Education	No.	%
Foso College	100	33.3
Ola College	100	33.3
Komenda College	100	33.3
Total	300	100

Source: Field Survey (2019)

Table 8 shows the participants from the various institutions that took part in the research. The three selected Colleges of Education namely, Foso, Ola and Komenda Colleges of Education had equal number of respondents 100(33.3%) each contributing to a total of 300 participants.

Table 9: Role at the Institution

Role at the institution	No.	%
Management	27	15
Lecturer	228	76
IT Support Staff	45	9
Total	300	100

Source: Field Survey (2019)

From Table 9, the study revealed that most of the respondents were lecturers 228(75%) with 27(15%) management respondents whiles IT support staff were represented with 45(9%) respondents.

Main Results

This section focuses on the discussion of the main findings of the study. The results are presented and discussed in line with the various research questions of the study.

Reliability

Reliability is concerned with how much random error there is in the measurement. The reliability of the questionnaire is concerned with the consistency of the responses to the questions (Gill and Johnson, 2002). With the intention of testing the properties of measurement scales, the Cronbach's coefficient Alpha for these constructs were calculated using the SPSS version 23 scale reliability measure. Cronbach's alpha is a measure of internal consistency as it defines whether different items that intend to measure a construct, actually measure that specific construct.

Based on what is indicated in Kline's (1999) handbook of psychological testing, the alpha greater than 0.7 is acceptable. In addition to Cronbach's Alpha I measured the inter-item correlation mean. Inter-item correlation mean of above 0.3 is acceptable. However, Briggs and Clukey (2004) recommend an optimal range for the inter-item correlation of .2 to .4. (Pallant, 2007).

Table 10: Reliability of Study Results

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
RelativeAdvantage	116.2862	67.712	.404	.221	.732
Complexity	118.1313	68.277	.473	.241	.714
Compactibility	117.6229	70.283	.467	.250	.716
TopManagement	117.4882	65.312	.527	.348	.701
TechReadiness	117.8182	64.447	.567	.385	.692
CompPressure	117.9024	72.122	.403	.199	.729
RegCompliance	117.9024	71.987	.399	.198	.730

Source: Field Survey (2019)

Factor analysis

The construct validity of each model which comprised of different variables should be evaluated. This method allows a researcher to analyze the correlation between items; and to determine a new set of variables that are highly correlated to each other. Convergent validity is one component of the construct validity, which determines whether all items that measure one factor converge. Factor loading and reliability test are two methods to check the convergent validity of the construct.

Factor loading shows the correlation between each item and the related constructs and according to Hair et al. (2006) a factor loading above 0.5 is acceptable; and the factor loading above 0.7 is ideal. The second component of construct validity that needs to be checked is discriminant validity. Discriminant validity defines whether a construct is different than other constructs. Explanatory Factor Analysis is one way to test the discriminant and convergent validity of the instrument

Table 11: Communalities of Exploratory Factor Analysis

Constructs	Initial	Extraction
RelativeA1	1	0.533
RelativeA2	1	0.619
RelativeA3	1	0.594
RelativeA4	1	0.616
RelativeA5	1	0.53

Table 11: Communalities of Exploratory Factor Analysis (Cont'd)

Construct	Initial	Extraction
Complexity1	1	0.56
Complexity2	1	0.674
Complexity3	1	0.594
Complexity4	1	0.605
Complexity5	1	0.619
Compactibility1	1	0.639
Compactibility2	1	0.681
Compactibility3	1	0.56
Compactibility4	1	0.545
Compactibility5	1	0.438
Top Management1	1	0.618
Top Management2	1	0.691
Top Management3	1	0.572
Top Management4	1	0.56
Top Management5	1	0.591
TechReadiness1	1	0.552
TechReadiness2	1	0.473
TechReadiness3	1	0.574
TechReadiness4	1	0.544
TechReadiness5	1	0.56
CompPressure1	1	0.634
CompPressure2	1	0.672
CompPressure3	1	0.565
CompPressure4	1	0.586
CompPressure5	1	0.632
RegCompliance1	1	0.547
RegCompliance2	1	0.658
RegCompliance3	1	0.681
RegCompliance4	1	0.494
RegCompliance5	1	0.518

Source: Field Survey (2019)

As it can be seen from table 11, 3 items were dropped due to low communalities below 0.5(<0.5) in accordance with the recommendations by (Worthington & Whittaker, 2006; Hair et al.,2006; Field,2009). One Item

associated with Compatibility CM5, Technological Readiness TR2 and Regulatory Compliance RP4 were all dropped and excluded from the analysis. The updated table with communalities loading above 0.5 is represented in table 12 below

Table 12: Updated Communalities of Exploratory Factor Analysis

Constructs	Initial	Extraction
RelativeA1	1	0.52
RelativeA2	1	0.62
RelativeA3	1	0.606
RelativeA4	1	0.616
RelativeA5	1	0.529
Complexity1	1	0.562
Complexity2	1	0.712
Complexity3	1	0.615
Complexity4	1	0.691
Complexity5	1	0.634
Compactibility1	1	0.646
Compactibility2	1	0.701
Compactibility3	1	0.62
Compactibility4	1	0.547
Top Management1	1	0.612
Top Management2	1	0.7
Top Management3	1	0.577
Top Management4	1	0.562
Top Management5	1	0.587
TechReadiness1	1	0.556
TechReadiness3	1	0.593
TechReadiness4	1	0.571
TechReadiness5	1	0.591
CompPressure1	1	0.656
CompPressure2	1	0.688
CompPressure3	1	0.581
CompPressure4	1	0.642
CompPressure5	1	0.663

Table 12: Updated Communalities of Exploratory Factor Analysis (Cont'd)

Constructs	Initial	Extraction
RegCompliance1	1	0.576
RegCompliance2	1	0.686
RegCompliance3	1	0.693
RegCompliance5	1	0.532

Extraction Method: Principal Component Analysis.

Source: Field Survey (2019)

Relative Advantage

Relative advantage is this study context is the degree to which innovative security technology is perceived as being better than the idea it supersedes at the Colleges of Education. In this study relative advantage was measured by different items RA1, RA2, RA3, RA4 and RA4. Table 13 summarizes the descriptive analysis of relative advantage. As it can be viewed in figure 4, majority of the respondents in our sample feel positive about the relative advantage of security innovation.

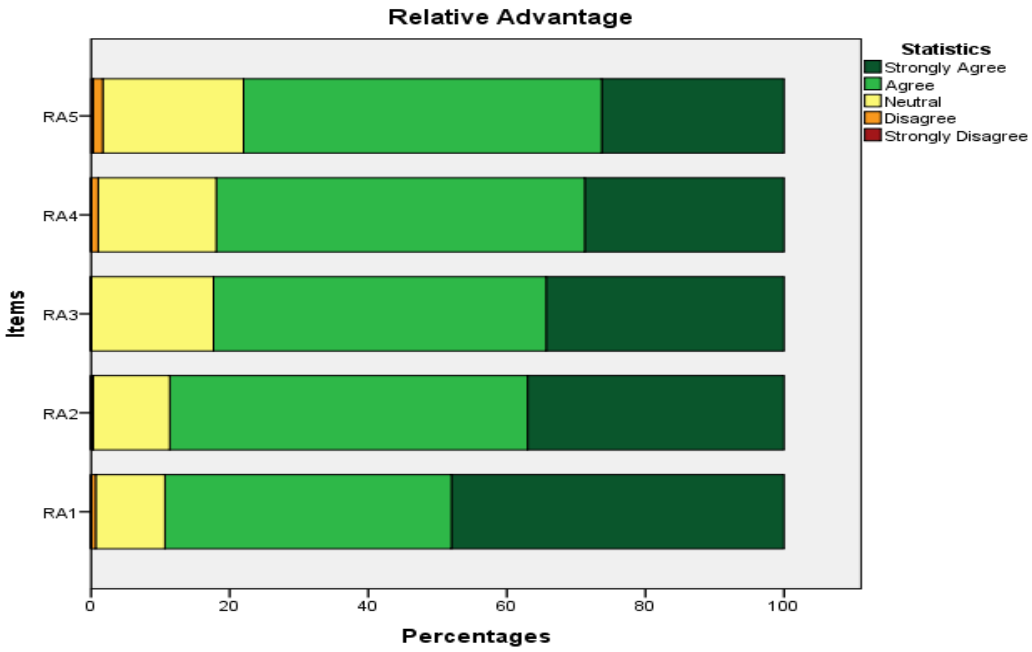
More than 80% perceive security innovation as advantageous for operations of their institutions. At the same time, more than 90% of the respondents feel that security innovations prevent unauthorized access, denial of service attacks on systems and improve the monitoring and control of communication systems. Overall, majority of participants have found security innovations to be advantageous for their Colleges of Education; therefore in our sample the perceived relative advantage of using innovative security is high.

Table 13: Descriptive Analysis of Relative Advantage

Items	Mean	Median	Std. Deviation
RA1	4.37	4.00	.688
RA2	4.25	4.00	.656
RA3	4.17	4.00	.703
RA4	4.09	4.00	.702
RA5	4.02	4.00	.742

Source: Field Survey (2019)

Figure 4: Analysis of Respondent's Perception about Relative Advantage



Source: Field Survey

Complexity

Complexity is related to how difficult it is to understand and use innovative security technologies at the Colleges of Education and it is measured by the items CY1, CY2, CY3, CY4 and CY5. Table 14 summarizes the descriptive analysis of complexity, the CY standing for Complexity. From figure

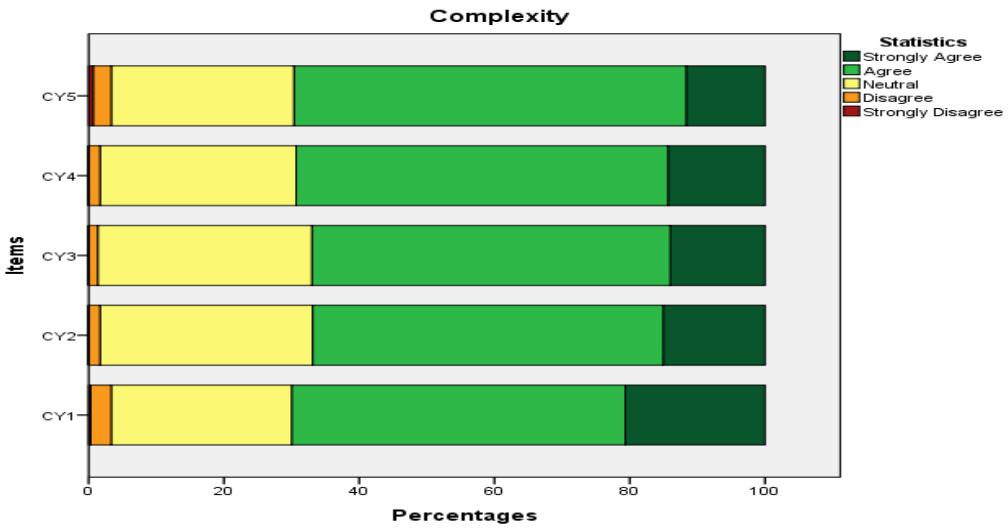
5, more than 70% of the participants agree that working with security is complicated because it is difficult to understand operational procedures as well as taking up much of their time. However, about 60% are of the opinion that learning to use secured processes such as maintaining audit logs prolongs the total allocated period for the task. Overall majority of the respondents have found innovative security complex.

Table 14: Descriptive Analysis of Complexity

Items	Mean	Median	Std. Deviation
CY1	3.87	4.00	.780
CY2	3.80	4.00	.703
CY3	3.80	4.00	.686
CY4	3.82	4.00	.685
CY5	3.77	4.00	.710

Source: Field Survey

Figure 5: Analysis of Respondent's Perception about Complexity



Source: Field Survey (2019)

Compatibility

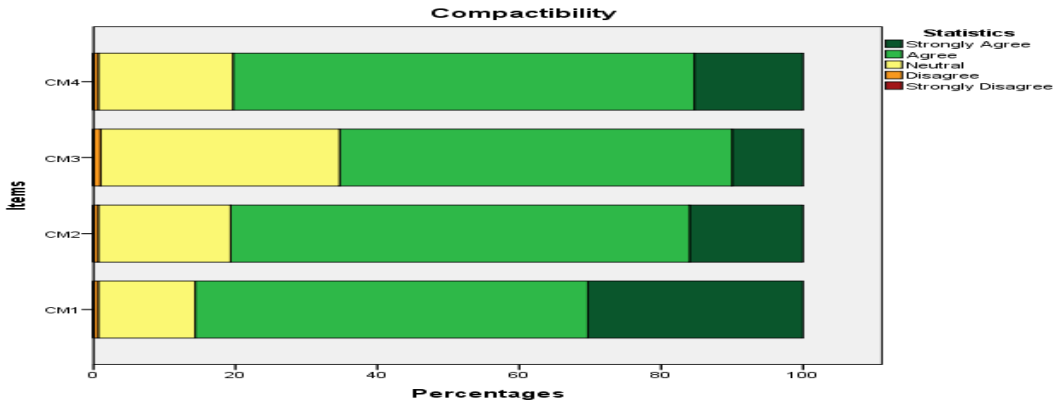
Compatibility relates to how new security technologies are consistent with an already existing ones at the Colleges of Education. In order to measure compatibility, items CM1, CM2, CM3 and CM4 were used. Table 15 summarizes the mean and standard deviation of items that were used to measure the perceived compatibility. As it can be viewed from figure 6, more than 75% feel, that innovative security technology were compatible with the institution's work style and existing IT infrastructure. However, 65% believe that security innovation is compatible with norms and culture of their institution. In general participants were very positive about the compatibility of security with different aspects of their work.

Table 15: Descriptive Analysis of Compatibility

	Mean	Median	Std. Deviation
CM1	4.15	4.00	.667
CM2	3.96	4.00	.611
CM3	3.74	4.00	.642
CM4	3.95	4.00	.607

Source: Field Survey

Figure 6: Analysis of respondent's perception about Compatibility



Source: Field Survey (2019)

Top management support

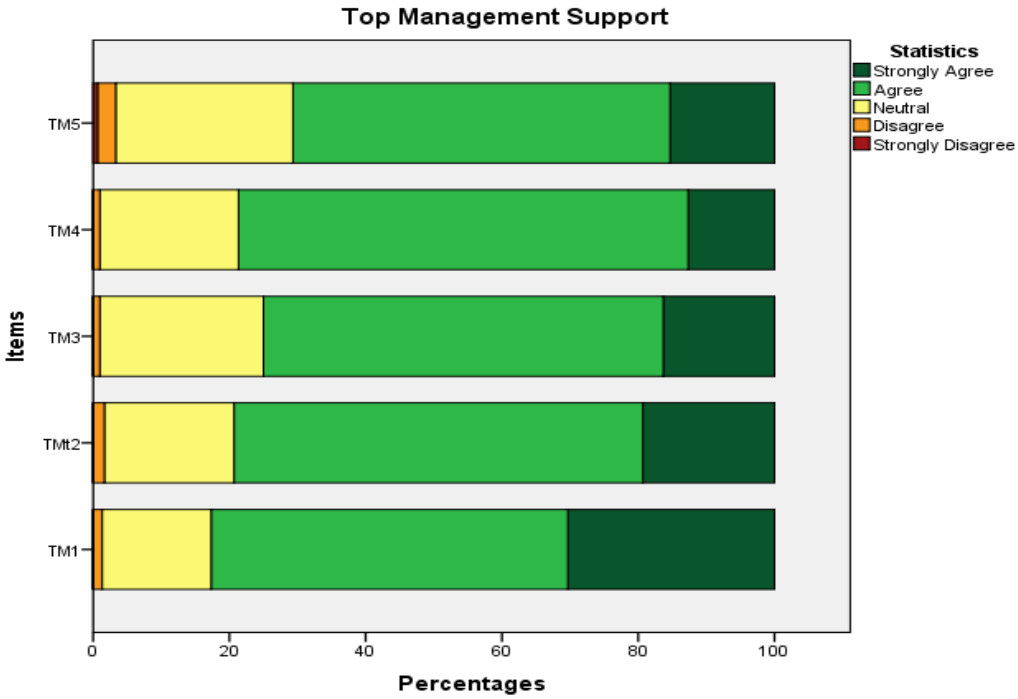
Top management is regarded as having the role of power, control and information links sharing to invest in the security domains at the Colleges of Education. The items TM1, TM2, TM3, TM4 and TM5 measured the support of management in innovative security technologies. Table 16 summarizes the mean and standard deviation of items that were used to measure the perceived .From figure 7, more than 70% feel that top management offer strategic planning, strong leadership in the implementation of security innovations at their institutions. However, 65% are of the opinion that management share information related to security issues.

Table 16: Descriptive Analysis of Top Management Support

Items	Mean	Median	Std. Deviation
TM1	4.12	4.00	.710
TM2	3.97	4.00	.671
TM3	3.90	4.00	.660
TM4	3.90	4.00	.602
TM5	3.82	4.00	.741

Source: Field Survey (2019)

Figure 7: Analysis of respondent's perception about Top Management Support



Source: Field Survey (2019)

Technological Readiness

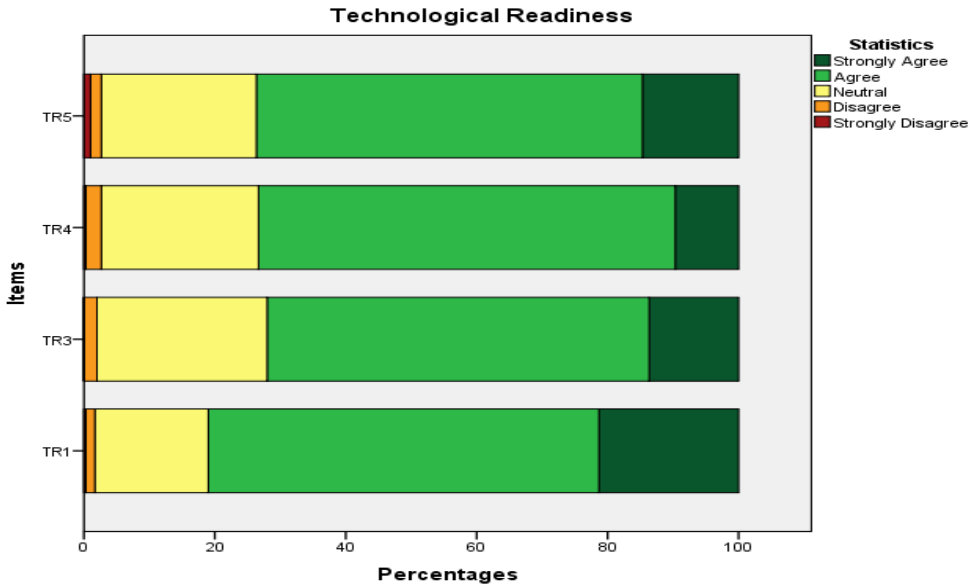
Technological readiness deals with the physical assets and human resources available to the Colleges of Education to implement security innovations. Items TR1, TR3, TR4 and TR5 measured technological readiness. Table 17 summarizes the mean and standard deviation of items that were used to measure the perceived .As it can be seen from figure 8 more than 80% agreed that their institutions hire specialized personnel for security technology services. Moreover, 70% are confident of sufficient technological resources, proper allocation of revenue and a highly qualified in-house expertise to address security issues within their institutions.

Table 17: Descriptive Analysis of Technological Readiness

Items	Mean	Median	Std. Deviation
TR1	4.00	4.00	.687
TR3	3.84	4.00	.672
TR4	3.80	4.00	.649
TR5	3.85	4.00	.720

Source: Field Survey (2019)

Figure 8: Analysis of respondent's perception about Technological Readiness



Source: Field Survey (2019)

Competitive Pressure

Competitive pressure is the degree to which the Colleges of Education is affected by competitors which drive them to initiate and adopt security innovations to maintain a competitive edge. Items CP1, CP2, CP3, CP4 and CP5 measured competitive pressure. Table 18 summarizes the mean and standard deviation of items that were used to measure the perceived competitive pressure.

Figure 9 depicts the respondents' opinion about the competitiveness of the market they operate in. The results indicate that the majority of the respondents perceive a high level of pressure from competitor institutions.

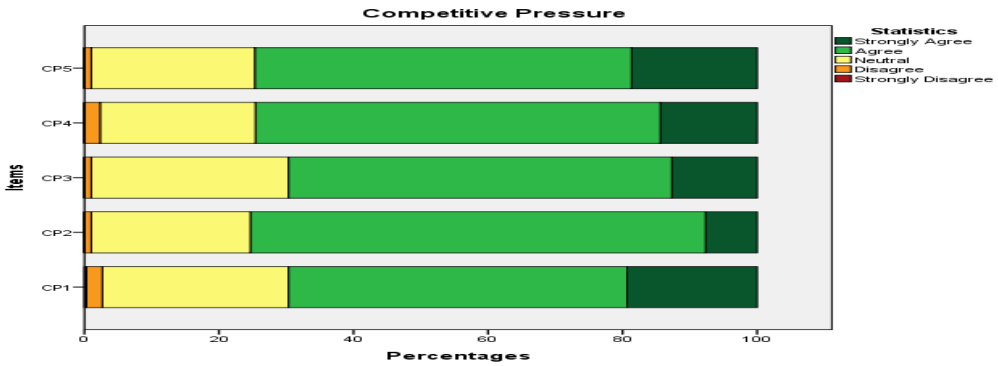
More than 75% feel that it is easier for students/workers to switch to other institutions and the fact that there are pressures on them due to the advantages in the use of secure systems. However, more than 65% believe that most of their competitors are already using secured systems that creates the impression that innovative security technologies have influences on competition among Colleges of Education

Table 18: Descriptive Analysis of Competitive Pressure

Items	Mean	Median	Std. Deviation
CP1	3.86	4.00	.759
CP2	3.82	4.00	.567
CP3	3.81	4.00	.653
CP4	3.87	4.00	.672
CP5	3.92	4.00	.682

Source: Field Survey (2019)

Figure 9: Analysis of Respondent's Perception about Competitive Pressure



Source: Field Survey (2019

Regulatory Compliance

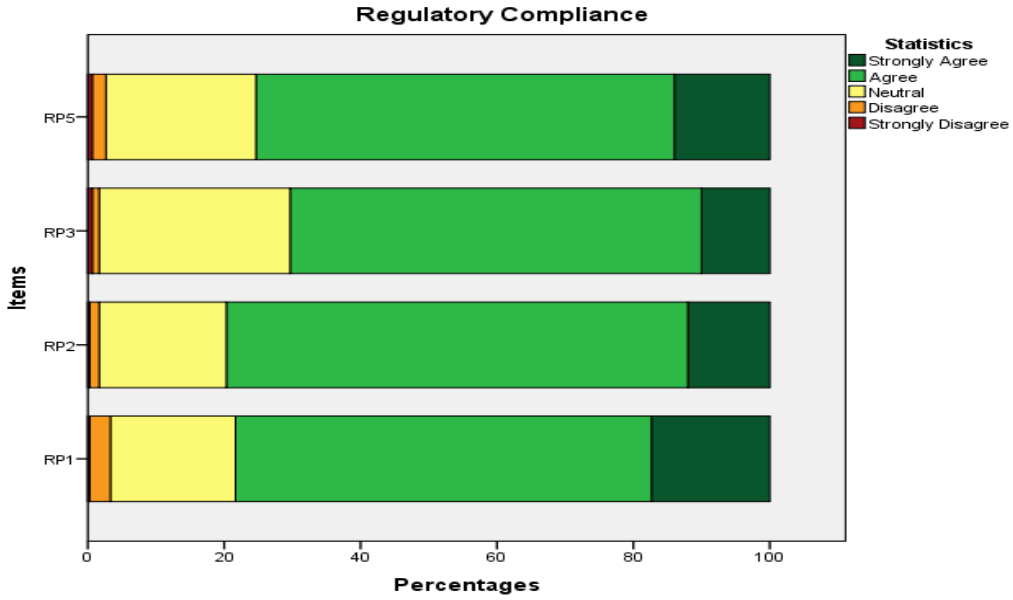
Regulatory compliance is concerned with how Laws, regulations and professional standards including privacy and client confidentiality can support or inhibit decisions of Colleges of Education to adopt innovative security technologies. Regulatory compliance was measured with items RP1, RP2, RP3 and RP5. Table 19 summarizes the descriptive statistics for regulatory compliance. From figure 10, it can be observed that more than 80% feel that Ghanaian laws can facilitate the use of innovative security systems and policies on security are well documented in their institutions. However, over 75% believe that their institutions have managed to implement procedures to ensure compliance. Over 65% are confident that their Colleges of Education conduct regular reviews to ensure compliance with security policies.

Table 19: Descriptive Analysis of Regulatory Compliance

Items	Mean	Median	Std. Deviation
RP1	3.92	4.00	.708
RP2	3.90	4.00	.617
RP3	3.78	4.00	.658
RP5	3.86	4.00	.694

Source: Field Survey (2019)

Figure 10: Analysis of Respondent's Perception about Regulatory Compliance



Source: Field Survey

Satisfaction with cloud services

Participants were asked about the intention to use cloud computing services for datacenter at the Colleges of Education, if they have not already adopted cloud. Also for those who already adopted cloud computing services for their datacenters, i asked them whether they are satisfied with the service they received from cloud provider. Below are the descriptive and frequency analysis of these two questions. Figure 11 depicts the frequency of answers to the satisfaction question. As it can be seen, more than 90% of participants were satisfied with the service they receive from cloud providers

Figure 11: Descriptive Analysis of Satisfaction with Cloud Services

Source: Field Survey (2019)

Intention to use cloud services

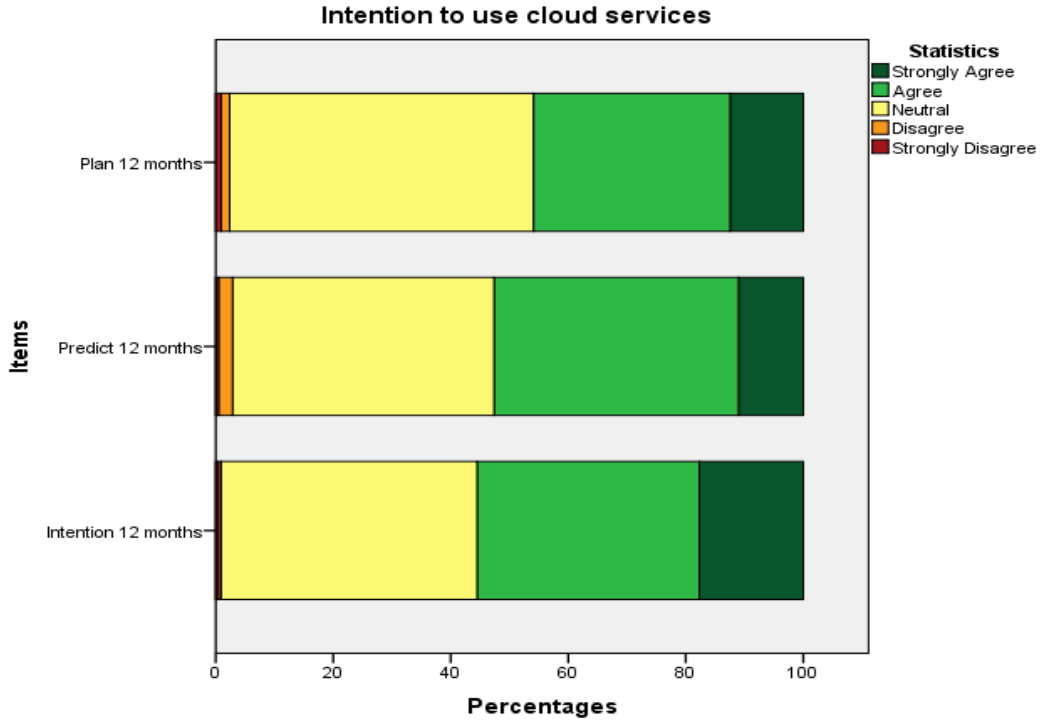
Respondents, who have not adopted cloud computing services yet for their datacenter, answered these questions. I asked them whether they intent to adopt cloud computing in the next 12 months; whether they plan to adopt cloud computing in the next 12 months; and whether they predict to use cloud computing in the next 12 months. Table 19 summarizes the descriptive analysis of intention to use. It includes the number of respondents, the mean and the Std. Deviation. Also figure 12 depicts the summary of the answers and as it can be seen more than 50% of non-adopters intend to adopt cloud services for their datacenter in the near future. Overall the intention to adopt cloud computing is high.

Table 20: Descriptive Analysis of Intention to use cloud services

	Mean	Median	Std. Deviation
Intention 12 months	3.72	4.00	.773
Predict 12 months	3.60	4.00	.734
Plan 12 months	3.55	3.00	.765

Source: Field Survey (2019)

Figure 12: Analysis of Respondent's Intention to Use Cloud Services



Source: Field Survey (2019)

Research questions

Research questions one and two reads;

1. What are the security issues within cloud computing datacenters?

2. What are the security issues within in-house datacenters?

In order to answer the above questions participants were asked to indicate vulnerability, threats and control mechanisms put in place to guard against security issues within their institutions. Table 21 depicts the descriptive statistics of security issues for cloud and in-house datacenters. As it can be seen from the table above, the vulnerability, threats are high and control measures are relatively low for both datacenters in protecting assets.

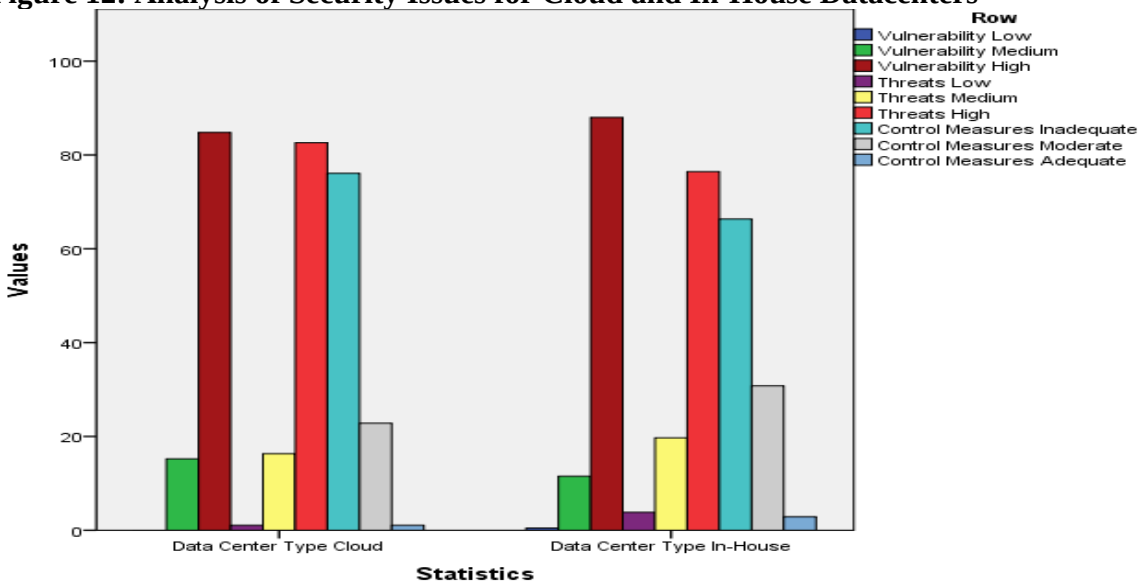
This is evident as 183(88%) of the respondents believe that in-house datacenters are highly vulnerable as compared to 78 (84.8%) for cloud datacenters. However, 76(82.6%) of the respondents attested to the fact that threat rate in cloud datacenters are higher as compared to 159(76.4%) for in-house datacenters. Furthermore, the control measures against attacks are lower for in-house datacenters 138(66.3%) with 70(76.1%) for cloud datacenters. The general low security state of colleges can probably be attributed to the unavailability of funds to procure innovative security systems and the lack of motivation from end-users to adhere to security protocols. This is evident in the lack of control against DDoS, buffer overflow, SQL injections, Man-In-The middle attack for in-house datacenters and insecure APIs, bot-nets, Insecure web applications, malware and phishing attacks on cloud based datacenters.

Table 21: Descriptive Analysis of Security Issues

Security Issues		Data Center Type			
		Cloud		In-House	
		No.	%	No.	%
Vulnerability	High	78	84.8%	183	88.0%
	Medium	14	15.2%	24	11.5%
	Low	0	0.0%	1	0.5%
Threats	High	76	82.6%	159	76.4%
	Medium	15	16.3%	41	19.7%
	Low	1	1.1%	8	3.8%
Control Measures	Adequate	1	1.1%	6	2.9%
	Moderate	21	22.8%	64	30.8%
	Inadequate	70	76.1%	138	66.3%

Source: Field Survey (2019)

Figure 12: Analysis of Security Issues for Cloud and In-House Datacenters



Source: Field Survey (2019)

In line with research questions 1and 2, I hypothesized that;

H1– ***There is no statistically significant difference among Colleges of Education in terms of security issues within cloud datacentres***

H2– ***There is no statistically significant difference among Colleges of Education in terms of security issues within in-house datacenters***

Two way ANOVA was used to compare the effects of the Colleges of Education and datacenter types on security issues. Colleges of Education included 3 levels (Ola, Komenda and Fosu) and datacenter type consisted of two levels (cloud, in-house). All effects were statistically significant at the .05 significance level. From table 21, the main effect for Colleges of Education yielded an F ratio of $F(2, 294) = 18.6$, $p < .001$, indicating a significant difference between Ola college ($M = 84.80$, $SD = 11.04$), Komenda college ($M = 91.16$, $SD = 8.99$) and Fosu college ($M = 96.17$, $SD = 12.17$.

The main effect for datacenter type yielded an F ratio of $F(1, 294) = 4.511$, $p > .05$, indicating that the effect for datacenter types was significant, cloud ($M = 89.16$, $SD = 10.93$) and in-house ($M = 91.39$, $SD = 12.045$) The interaction effect was significant, $F(2, 294) = 10.433$, $p < .001$.

Table 22: Descriptive statistics on ANOVA

Dependent Variable: Security Issues

Data Center Type	Colleges	Mean	Std. Deviation	N
Cloud	Ola College	85.58	12.875	26
	Komenda College	92.31	6.612	29
	Fosu College	89.22	11.643	37
	Total	89.16	10.930	92
In-House	Ola College	84.53	10.397	74
	Komenda College	90.69	9.812	71
	Fosu College	100.25	10.575	63
	Total	91.39	12.045	208
Total	Ola College	84.80	11.035	100
	Komenda College	91.16	8.999	100
	Fosu College	96.17	12.166	100
	Total	90.71	11.742	300

Source: Field Survey (2019)

Table 23: ANOVA Showing Effect of Colleges and Datacenter Types on Security Issues

Tests of Between-Subjects Effects

Dependent Variable: Security Issues

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power[b]
Corrected Model	9409.381[a]	5	1881.88	17.392	0	86.959	1
Intercept	2052303.221	1	2052303	18966.7	0	18966.7	1
Institution	4025.691	2	2012.85	18.602	0	37.204	1
DataCType	488.124	1	488.124	4.511	0.035	4.511	0.562
Institution * DataCType	2257.798	2	1128.9	10.433	0	20.866	0.988
Error	31812.389	294	108.205				
Total	2509713	300					
Corrected Total	41221.77	299					

Table 23: ANOVA Showing Effect of Colleges and Datacenter Types on Security Issues (Cont'd)

a. R Squared = .228 (Adjusted R Squared = .215)
b. Computed using alpha = .05

Source: Field Survey (2019)

A post hoc analyses using Tukey's HSD indicated that Fosu college (M = 96.17, SD = 12.17) had better security in in-house datacenter as compared to the other Colleges of Education. However, Komenda college (M = 91.16, SD = 8.99) had the best cloud datacenter security compared to the rest of the colleges. Table 24 reveals that there was a significant difference among Colleges of Education in terms of whether they use cloud services or in-house services for their datacenter activities. The significant values were less than the 0.05 level of significance. Therefore the research hypothesis 1 and 2 were rejected

Table 24: Post Hoc Multiple Comparison of Colleges and Datacenter Types on Security

Dependent Variable: Security Issues

Tukey HSD

					95% Confidence Interval	
(I) Colleges	(J) Colleges	Mean Difference (I-J)	Std. Error	Sig.	Lower Bound	Upper Bound
Ola College	Komenda	-6.36*	1.471	.000	-9.83	-2.89
	Fosu	-11.37*	1.471	.000	-14.84	-7.90
Komenda College	Ola	6.36*	1.471	.000	2.89	9.83
	Fosu	-5.01*	1.471	.002	-8.48	-1.54
Fosu College	Ola	11.37*	1.471	.000	7.90	14.84
	Komenda	5.01*	1.471	.002	1.54	8.48

Based on observed means.
The error term is Mean Square(Error) = 108.205.
*. The mean difference is significant at the .05 level.

Source: Field Survey (2019)

Research questions three and four reads;

3. What are the factors that determine the adoptions of security innovations for in-house datacenters

4. What are the factors that determine the adoptions of security innovations for cloud datacenters

In order to answer the above questions participants were asked to indicate whether they have adopted security innovations or they have not. Moreover, since the dependent variable is binary one, the most appropriate analysis method is logistic regression (Hair et al. (2006). In order to answer the questions correctly, the test model is assessed to ensure it is fit.

Table 25 shows the classification table. As it can be seen in the table, in 77(40.8%) of the cases, a Non adopter of security innovation is correctly predicted as being non-adopter. The value is much higher for adopters; 136(80.5%) of the time an adopter is accurately predicted as being an adopter. Our model's classification accuracy is 63.2%, which means in 63.2% of the time, the model correctly predicted the adoption decision which is an acceptable level of prediction accuracy

Table 25: Classification Table for Binary Logistic Regression

Classification Table[a]					
			Predicted		
			Security Innovation		Percentage
	Observed		Non-Adopted	Adopted	Correct
Step 1	Security Innovation	Non-Adopted	53	77	40.8
		Adopted	33	136	80.5

	Overall Percentage			63.2
a. The cut value is .500				

Source: Field Survey (2019)

Table 26 summarizes the results of our regression including the variables that are in the equation; their significance level, their coefficients, and Wald value. Among seven independent variables, only Complexity and Top management has a significant relationship with the security innovation adoption decision for types of datacenters. In the model, based on Wald statistics, Complexity and Top management are defined as the only significant factors. Complexity and Top management has a positive correlation with security innovation adoption decision as it is determined based on the sign of the coefficient (B); Complexity (β=0. 098, $p<0.05$) and Top management (β=132, $p<0.05$) for cloud datacenters and Complexity (β=0. 065, $p<0.05$) and Top management (β=0. 068, $p<0.05$) for in-house datacenters which is positive with the value of Exp ($B > 1$).

This implies that the probability of adopting security innovations for both cloud and in-house datacenters is influenced by how complexity and how top management support such decisions. Again, it can be noticed that significant difference exist among Colleges of Education in terms of factors that influences the adoption of security innovations whether they use cloud services or in-house services for their datacenter activities. Therefore research hypothesis 3 and 4 was rejected

Table 26 Table 24: Summary Results Model of Logistic Regression

Data Center Type			B	S.E.	Wald	Df	Sig.	Exp(B)
Cloud	Step 1[a]	RelativeAdvantage	.013	.039	.103	1	.748	1.013
		Complexity	.098	.040	6.054	1	.014	1.103
		TopManagement	.132	.056	5.545	1	.019	1.141
		CompPressure	-.305	.164	3.439	1	.064	.737
		Compatibility	-.055	.165	.110	1	.741	.947
		TechReadiness	-.067	.133	.253	1	.615	.935
		RegCompliance	.189	.148	1.622	1	.203	1.208
		Constant	-.798	4.939	.026	1	.872	.450
In-House	Step 1[a]	RelativeAdvantage	.001	.025	.002	1	.968	1.001
		Complexity	.065	.025	6.691	1	.010	1.067
		TopManagement	.068	.034	4.155	1	.042	1.071
		CompPressure	.116	.082	1.968	1	.161	1.123
		Compactibility	-.092	.092	.983	1	.321	.912
		TechReadiness	.081	.096	.715	1	.398	1.084
		RegCompliance	-.099	.102	.934	1	.334	.906
		Constant	-3.519	2.115	2.769	1	.096	.030

a. Variable(s) entered on step 1: RelativeAdvantage, Complexity, TopManagement, CompPressure, Compactibility, TechReadiness, RegCompliance.

Source: Field Survey (2019)

The non-significance of relative advantage in predicting security innovation is consistent with Chau & Tam (1997) who found similar results in their study of IT systems. This is contrary to the belief that when an institution perceives an innovation as offering a relative advantage, then it is more likely that they will adopt that innovation (Lee, 2004). It is therefore assumed that educational institutions need to perceive security as a key issue that can help protect their assets whiles improving on profitability.

Compatibility was not found to be a significant factor in determining security innovation. This finding differs from the work of Thong (1999) which suggested that compatibility is an essential attributes of organizational innovation,

and that academic institutions will be more likely to adopt them if they are compatible with existing work practices. One possible explanation for this finding is that compatibility may have significant effects after the innovation has been adopted. Hence, the extent to which the innovation is consistent with the values, experience, and needs of the Colleges of Education may not be clear at the onset until they have been fully acquired and used it.

The significant findings for complexity is consistent with (Grover, 1993; Thong, 1999), who suggested that academic institutions may be less likely to adopt an innovation or technology, if it requires a high level of new skills by members of that organisations. This also contradicts the work of Kendall, (2001); Ramdani and Kawalek, (2009) who found inconsistent results with complexity. These findings can be explained by the fact that various Colleges of Education worry about how easy such security technology systems are to operate since they are not easy to adopt, implement and use.

Top management support was found to be significant which is consistent with the work of Tan and Teo et al. (2009) who identified the role of management as integral in technology adoption. This findings, however, contrasts the work of Thong et al. (1999) who concluded in their research that top managers will possibly not be involved in the critical evaluation for making the adoption decision. One possible reason for the significant findings is the ability to allocate or assign resources by management of Colleges of Education in acquisition of security technologies.

Competitive pressure was found to be non-significant which is in line with previous works Jeon et. al. (2006) and in contrast with (lacovou et al., 1995; Premkumar & Michael, 1995) who arrived at a significance results. One of the possible reasons for the inconsistent result is the lack of competition among the Colleges of Education which may require restructuring and updating of security protocols to gain competitive edge over rivals.

Regulatory compliance was insignificant which was consistent with the work of Delmas (2002). An explanation is the high additional transactional cost involved when Colleges of Education want to adhere strictly to security standards. With limited resources available to such institutions generating additional money to tackle security issues is a daunting task for them.

Technological readiness was not significant which contrasts the work of Iacovou et al. (1995; Armstrong and Sambamurthy (1999) and Zhu et al. (2006). The availability of knowledge, resources, commitment and governance is regarded as a major driver for innovation. One possible reason for this finding is the lack of resources in the form of infrastructure and personnel at the various Colleges of Education that can handle security innovations when the need arises.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Introduction

This chapter gives a summary for the study. In addition, recommendations are made to facilitate a smooth adoption of security innovations at the Colleges of Education

Summary of the study

This study was undertaken to explore the determinants of security innovation at the Colleges of Education for cloud and in-house datacenters. Specifically, the study sought to; identify security issues in cloud and in-house datacenters and to explore the factors that determine the adoption of security innovations for datacenters. Descriptive research design was used for the study. The population for the study consisted of management staff; lecturers and IT support staff at the selected Colleges of Education within the central region.

The sample for the study was 300 which were obtained by the use of Stratified random sampling technique. The research instruments used was questionnaire which was adapted from innovation adoption authors. The instrument was administered by the researcher himself with a return rate of 100% on all participants. SPSS version 23 was used to analyze the gathered data with the use of statistical tools such as percentages, frequency tables and Anova.

Key findings

1. Most datacenters for Colleges of Education were vulnerable to an attack which pose serious threats to the confidentiality, integrity and availability of information assets
2. In-house datacenters are more vulnerable but have low threat rate as compared to datacenters that use cloud services.
3. The control measures against attacks in cloud datacenters are lower, which goes contrary to literature that in-house datacenters have limited mechanisms against possible attacks.
4. The perception about the relative advantage of a security innovation does not guarantee the likelihood that it will be acquired and used.
5. An anticipated complex and cumbersome nature of security technologies negatively influence the rate of acquisition and use at the Colleges of Education.
6. The support of top management is pivotal in safeguarding information security assets due to the power of distributing the needed resources at the Colleges of Education.

Conclusions

From the findings it could be concluded that both cloud and in-house datacenters have security loopholes in them which requires collaborative efforts to secure. Non-technical approaches such as improving user behavior can complement technical methods such as cryptography, firewalls and strong authentication methods in ensuring a secured cloud or in-house datacenters.

Again, the more one perceives an innovation as difficult to understand and use, the lower the likelihood that innovation will be adopted. Management is key when it comes to initial awareness, purchase and use of innovative technology of which security is included.

Academic institutions and for that matter Colleges of Education need a more strategic look at security issues and their integrations into core activities that will result in better outcomes in the long run.

Recommendations

On the basis of the findings and the conclusions drawn, the following are the recommendations made:

1. There should be an increased information security awareness and training for users as a means of improving security at the Colleges of Education.
2. Stakeholders should be educated on the benefits and limitations of cloud services and on-premises implantations in terms of vulnerability, threat levels and how to remedy those security challenges
3. Constant promotion of physical controls, procedural controls and technical controls is required to thwart almost all forms of security breaches in cloud services
4. Colleges of education should invest in security technology because they will be able to harness its full potential when they are implemented rather than perceiving how vital it will be without full implementation

5. Security technologies should be built and designed in a user-friendly manner to encourage mass usage at the various colleges of education

6. Top managers should be actively consulted and involved in innovate security technology acquisitions because they contribute to its success through their power of resource allocation.

Suggestions for Further Study

Further studies can be conducted to ascertain the drivers of security innovation at the university and other higher education institutions to provide multiple contexts views due to the vast range of datacenters they deploy in carrying out their core mandate of teaching and research.

Moreover, the factors used as drivers for innovative adoption decisions making can be extended further than the seven factors that were used in this study. This will provide a broader perspective on the innovation adoption whiles offering concrete understanding of the phenomenon.

REFERENCES

Aboagye C. (2018). Breach Alert! *UEW Site Has Been Hacked By Bocah*. 4(6) 2-103) Retrieved from: https://kuulpeeps.com/2018/04/breach-alert-uew-site-has-been-hacked-by-bocah/

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organisational Behavior and Human Decision Processes 50(2),* 179-211

Albrechtsene (2007). A qualitative study of users' view on information security. *Computers & Security 26(4),* 276–289

Amabile, T.M. (1988). A model of creativity and innovation in organizations. In Research in organizational behavior. *Research in Organizational Behavior, 10(12),* 123-167

Amedahe, K. & Asamoah-Gyimah, E. (2003*). Introduction to Educational Research. (CCUCC) 149 –150).*

Andras Cser, (2016). The Forrester Wave: Cloud Security Gateways, *Q4 2016. The Eight Providers That Matter Most And How They Stack Up* retrieved from http://www.forrester.org/cc/news123.html

Armbrust M., Fox A., Grifth R., Joseph A. D., Katz (2010). Above the clouds: A berkeley view of cloud computing. *Electrical Engineering and Computer Sciences Department*, University of California, Berkeley. Tech.Rep. UCB/EECS-2009-28

Armstrong, C. P., V. Sambamurthy. (1999). Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. *Inform. Systems Res, 10(4),* 304–327.

Arsanjani, A. (2004). Service-oriented modeling and architecture. *IBM developer works.*

Avison, D. and Myers, M.D. (2002) A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23(1),* 67-94.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security, 8(2),* 33-56

Bagchi, K and Udo, G. (2003). "An Analysis of the Growth of Computer and Internet Security Breaches", *International Journal of Communications of the Association for Information Systems, 12(1),* 684-700

Blaikie, N. (2009*). Designing Social Research*. Cambridge: Polity Press.

Borgaonkar, R. (2010). An Analysis of the Asprox Botnet. *in Fourth International Conference on Emerging Security Information Systems and Technologies* (SECURWARE), 2010. (pp. 148-153). Rochester, US. ICESIST

Bouchard, L., (1993). Decision Criteria in the Adoption of EDI. Laval, *Association for Information Systems, 21(14),* 365-376.

Briggs, J. & Clukey, C. (2014). Survey of Layered Defense, Defense in Depth and Testing of Network Security. *International Journal of Computer and Information Technology, 3(05),* 101-204

Bryman, A. and Hardy, M.A. (2004). *Handbook of Data Analysis*. SAGE Publications

Brynjolfsson, E., Hofmann, P., & Jordan, J. (2010). Cloud computing and electricity: beyond the utility model. *Commun. ACM, 53(5),* 32-34.

Buyya, R., Ranjan, R., & Calheiros, R. N. (2010). Inter cloud: Utility-oriented federation of cloud computing environments for scaling of application services Algorithms and architectures for parallel processing. *Springer, 27(2),* 13-31

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing andemerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems-the. *International Journal of Grid Computing-Theory Methods and Applications, 25(6),* 599-616.

Carlin, J. (2017). The 'WannaCry' ransomware attack could have been prevented. *Here's what businesses need to know*. CNBC 7(4) 2-13). Retrieved from http://www.cnbc. com/

Carrie, R. (2014). Discovering Security Events of Interest Using Splunk. Retrieved from http://www.sans.org/reading-room/whitepapers /logging /rss/-34272.

Chang, I. C., Hwang, H. G., Hung, M. C., Lin, M. H., & Yen, D. C. (2007). Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department. *Decision Support Systems, 44(17),* 350–359.

Chau P. Y. K, Tam K. Y. (1997) Factors affecting the adoption of open systems: an exploratory study. *MIS Q, 21(2),* 1–24

Chau, P.Y.K. & Tam, K.Y. (1997). Factors Affecting the Adoption of Open Systems: An Exploratory Study. *MIS Quarterly, 21(1),* 1-21.

Choi, Young B., Sershon, C., Briggs, J. & Clukey, C. (2014). "Survey of Layered Defense, Defense in Depth and Testing of Network Security", *International Journal of Computer and Information Technology, 3(5),* 73-83

Choudrie, J. and Dwivedi, Y.K. (2005). Investigating the research approaches for examining technology adoption issues. *Journal of Research Practice 1(1),* 1–12

Cooper, R. & Zmud, R. (1990). Information technology implementation research: a technological diffusion approach. *Management Science 36(2),* 123-139.

Creswell, J. W. (2003). *Research methods in education: Qualitative and quantitative and mixed methods approaches.* London: SAGE Publications.

Creswell, J. W. (2007). *Qualitative inquiry& research design: Choosing among five approaches.* Thousand Oaks: SAGE Publications.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approach.* Thousand Oaks, CA: Sage Publications.

Crook, C.W. & Kumar, R.L. (1998). Electronic Data Interchange: A Multi -Industry Investigation Using Grounded Theory. *Information Management 34(2),* 75-89.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20(1),* 79-98.

Dagon, D. Zou, & Lee , W.(2006). "Modeling botnet propagation using time

zones," *in Proceedings of the 13th annual network and distributed system security symposium*.

Damanpour F., Schneider, M. (2006). Phases of the adoption of innovation in organizations: Effects of environment, organization and top Managers. *British Journal of Management,* 17(3), 215-236.

Damanpour, F. & Wischnevsky, D. (2006). Research on innovation in organizations: Distinguishing innovation-generating from innovation -adopting organizations. *Journal of Engineering and Technology Management, 23(4),* 269-291.

Damanpour, F. (1991). Organisational Innovation: A Meta-analysis of Effects of Determinants and Moderators. *Academy of Management Journal, 34(3),* 555-590.

David G. S. S. & Anbuselvi, R. (2015). An architecture for Cloud computing in Higher Education, *in 2015 International Conference on Soft Computing and Networks Security* (ICSNS) London, UK

Dawes, J. G. (2008). Do Data Characteristics Change According to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales. *International Journal of Market Research, 51(1)* 223-342.

Dawson, T. L. (2002). New tools, new insights: Kohlberg's moral reasoning stages revisited. *International Journal of Behavior Development, 2(6),* 154-166.

Daylami, N., Ryan, T., Olfman, L. and Shayo, C. (2005). System sciences , HICSS 05. *Proceedings of the 38th Annual Hawaii International Conference, (p 213-344),* Island of Hawaii. USA

Delmas, M.A. (2002). The Diffusion of Environmental Management Standards in Europe and in the United States: An Institutional Perspective. *Policy Sciences 35(1),* 91-119.

Dhillong & Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11(2),* 127–153.

Dholakia, R.R. & Kshetri, N. (2004). Factors Impacting the Adoption of the Internet among SMEs', *Small Business Economics, 23(4),* 311-322.

Dillon, T., Chen, W., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *Paper presented at the 24th IEEE InternationalConference on Advanced Information Networking and Applications*(AINA). (pp 20-23) London. UK

Drucker, P . (1985). *Innovation and Entrepreneurship*, Harvard Business School

Eder, L.B. & Igbaria, M. (2001). Determinants of intranet diffusion and infusion', *Omega*, 29(3), 233-242

Ercan, T. (2010) .Effective use of cloud computing in educational institutions. *Procedia,- Soc. Behav. Sci., 2(2),* 938–942.

Fichman, R. and Kemerer, C. (1997). Adoption of software engineering process innovations: The case of object orientation. *Sloan Management Review, 34(2),* 7-22.

Fichman, R. G. (2001). The role of aggregation in the measurement of IT-related organizational innovation. *MIS quarterly, 2(4),* 427-455.

Fichman, R. G., (1999). The Diffusion and Assimilation of Information Technology Innovations. In: R. Zmud, ed. *Framing the Domains of IT Management: Projecting the Future Through the Past.* Cincinnati: Pinnaflex Educational Resources, Inc. pp 23-163

Field, A., (2009). *Discovering Statistics Using SPSS. 3rd ed*. London: SAGE Publications

Foster, I., Zhao, Y., Raico, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environments Workshop, 2008. GCE '08,* (pp. 1-10). Texas USA

Fraenkle, J. R., & Wallen, N. E. (1993). *How to design and evaluate research in education (4th ed.).* Boston: McGraw-Hill Companies Inc.

Frambach R.T., & Schillewaert N. (2002). Organizational innovation adoption: A multi-level framework of determinants and opportunities for future research. *Journal of Business Research, 55 (2),* 163-176.

Frihati J., Moldoveanu F., & Moldoveanu A. (2009). General Guidelines for the Security of a Large Scale Data Centre Design. *University Politehnica of Bucharest Sci. Bull., Series* C, *71(3),* 26-433

Gallivan, M. (2001). Organizational adoption and assimilation of complex technological innovations: development and application of a new framework. *SIGMIS Database, 32(3),* 51-85.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16(2),* 186-208.

Ghosh, B.N. and Chopra, P.K. (2003) *A Dictionary of Research Methods*. Wisdom House.

Gibbs & K. L. Kraemer, (2004). A Cross-Country Investigation of the Determinants of Scope of E-commerce Use: An Institutional Approach. *Electronic Markets, 14 (2),* 124-137

Gill, J. and Johnson, P. (2002) *Research Methods for Managers*. Sage Publications

Glatthorn, A. A. (1998). *Writing the winning dissertation step by step*. California: Saga Publications

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of innovations in service organizations: systematic review and recommendations. *The Milbank Quarterly, 82 (4),* 581-629

Grover, V. (1993) . An Empirically Derived Model for the Adoption of Customer-based Interorganizational Systems. *Decision Sciences, 24(3),* 603-640

Grover, V. (1993). An Empirically Derived Model for the Adoption of Customer-based Inter-organizational Systems. *Decision Sciences, 24(3),* 603-640

Gunasekaran A., Sandhu M., 2010. Handbook on business information systems. *World Scientific Publishing Co. Pte*. Ltd. ISBN-13 978-981-283-605-2

Hagel, J., & Brown, J. S. (2001). Your next IT strategy. Harvard Business Review, 79(9), 105-115. *International Conference on Information Technology Interfaces*. (pp. 31—40), Delhi. India

Hagen, J.M, Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16(4),* 377 -397.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate data analysis, (6th ed.),* New Jersey: Upper Saddle River, Pearson Education, Inc.

Halpert, B. (2011). *Auditing Cloud Computing: A Security and Privacy Guide*. Wiley, 2011.

Hameed, S., Butt, A. J., & Tariq, M. J. (2012). The factors causing failure of foreign enterprises resource planning (ERP) systems in Pakistan. *African Journal of Business Management, 6(3),* 946-955.

Hashem, I.A.T., (2014). The rise of "Big Data" on cloud computing: *Review and open research issues. Information Systems, 47(3),* 98–115.

He, S., Lee, G. M., Quarterman, J. S., & Whinston, A. B. (2016). Cybersecurity Policies Design and Evaluation: Evidence from a Large-Scale Randomised Field Experiment. *Proceedings of Workshop on the Economics of Information Security*. (pp. 1-50). Vancouver, Canada

Iacovou, C., Benbasat, I & Dexter, A. (1995). Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *Management Information Systems Quarterly, 19(4),* 465-485.

Igbariam & IivariJ (1995). The effects of self-efficacy on computer usage. *International Journal of Management Science 23(6),* 587–605

Jeon, B. N., Han, K. S. & Lee, M. J., 2006. Determining factors for the adoption of e-business: the case of SMEs in Korea. *Applied Economics, 38(5),* 105-116.

Jones, C.M., McCarthy, R.V., Halawi, L., and Mujtaba, B. (2010). Utilizing the Technology Acceptance Model to Access the Employee Adoption of Information System Security Measures. *Issues in Information System 11(1),* 9-16

kajal, R., Saini, D. & Grewal, K. (2012). Virtual Private Network. International *Journal of Advanced Research in Computer Science and Software Engineering, 2(10),* 428-432

Kankanhalli, A., Teo, H-H., Tan, B.C. & Wei, K-K. (2003). An integrativestudy of information systems security effectiveness. *International Journal of Information Management, 23(4),* 321-412

Kant, K., Le, M. & Jajodia, S. (2001). Security Considerations in Data Center Configuration Management. *In Configuration Analytics and Automation (SAFECONFIG), 4th Symposium*, (pp 1-9), Rochester, USA

Kanter, R. M. (1983). When a thousand flowers bloom: Structural, collective, and social conditions for innovation in organization. *Research in Organizational Behavior, 10(3),* 169 -211.

Kendall, J. (2001).Receptivity of Singapore's SMEs to electronic commerce adoption', *The Journal of Strategic Information Systems, 10(3),* 223 -242.

Kim, W., Kim, S. D., Lee, E. & Lee, S. (2009). Adoption Issues for Cloud Computing. *Proceedings of the 7th International Conference on Mobile Computing and Multimedia*, pp. 2—5. Boston, USA

Kline, P. (1999). The handbook of psychological testing.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy', *Information Management & Computer Security, 14(1),* 24-36.

Kotulic, A. & Clark, J., (2004). Why there aren't more information security research studies, *Information & Management, 41(5),* 597-607

Koutsopoulos D. & Papoutsis F. (2016). School on Cloud: Transforming Education Educational Policy. *Analysis and Strategic Research, 11(1),* 216-432

Krutz,R. Vines,R. (2010). Cloud Security: A Comprehensive Guide to Secure cloud computing, pp 125-216

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30(15),* 607-610.

Kuan, K.K.Y. & Chau, P.Y.K. (2001). A perception-based model for edi adoption in small businesses using a technology-organization-environment framework, *Information & Management, 38(8),* 507-521

Kwon, T. & Zmud, R. (1987). *Unifying the fragmented models of information systems implementation, in Boland, R. and Hirschheim, R.A. (Eds), Critical Issues in Information Systems Research*, John Wiley & Sons Inc, New York, NY

lacovou, C.L., Benbasat, I., & Dexter, A.S. (1995). Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *MIS Quarterly 19(2),* 465-485.

Lam, H.Y., Zhao, S., Xi, K. & Chao H.J. (2012). Hybrid Security Architecture for Data Center Networks. *IEEE International Conference in Communications* (ICC), (pp. 10-15), Washington DC, USA

Lance, C. (2013). Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *International Journal of Information Security, 4(3),* 144-149.

Lanman, J., Linos, P., Barry, L. and Alston, (2012). A Modernizing the U.S. Army's Live Training Product Line using a Cloud Migration Strategy: Early Experiences, Current Challenges and Future Roadmap. *In Proceedings of the 18th International Conference on Enterprise Information Systems,* (p 12-214). Boston, US. ICEIS

Lee, Y., and Kozar, K.A. (2005). Investigating Factors Affecting Adoption of Anti –Spyware Systems. *Communications of the ACM , 48(8),* 72-77.

Lee. J. (2004). Discriminant Analysis of Technology Adoption Behavior: a case of internet technologies in small business. *Journal of Computer Information System, 12(6),* 57-66

Leibenstein, H. (1976). *Beyond Economic Man: A New Foundation for Microeconomics*, Harvard University Press, Cambridge, MA

Lertwongsatien, C. and Wongpinunwatana, N. (2003). E-commerce Adoption in Thailand: An Empirical Study of Small and Medium Enterprises (SMEs). *Journal of Global Information Technology Management, 6(3),* 67-83.

Li, Q., Wang, C., Wu, J., Li, J., & Wang, Z.-Y. (2011). Towards the business information technology alignment in cloud computing environment: An approach based on collaboration points and agents. *International Journal of Computer Integrated Manufacturing, 24(11),* 1038–1057.

Lohr, S. L. (1999). *Sampling: Design and Analysis*. New York: Duxbury Press. Google Scholar

Low, C., Chen, Y. and Wu, M. (2011), "Understanding the determinants of cloud computing adoption". *Industrial Management & Data Systems, 111(7),* 1006-1023.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2012). Construct Measurement and Validation Procedures in MIS and Behavioral

Research: Integrating New and Existing Techniques. *MIS Quarterly 35(2)*, 293-334.

Majumdar, S.K., Venkataraman, S. & Snider Entrepreneurial, C. (1992). *New technology adoption in U.S. telecommunications: the role of competitive pressures and firm-level inducements.* Wharton School of the University of Pennsylvania, Snider Entrepreneurial Center.

Marston, S., Z. Li, et al. (2010). Cloud Computing - The Business Perspective. *Elsevier B.V. 34(7)*, 212-343.

Martin, M. C., Livshits, B., Andlam, M. S. (2005). Finding Application Errors and Security Flaws using PQL: a Program Query Language. *In Proceedings of the ACM Conference on Object Oriented Programming, Systems, Languages, and Applications* (OOPSLA), (pp. 365–383) Delhi India, UD

Masiyev, K. H., Qasymov, I., Bakhishova, V., & Bahri, M. (2012). Cloud computing for business .In Application of Information and Communication Technologies (AICT), 2012 *6th International Conference on* (pp. 1-4). Florida, USA IEEE

Mata, F., W. Fuerst, J. Barney. (1995). Information technology and sustained competitive advantage: A resource-based analysis. *MIS Quart*erly, *19(4)* 487-505.

Mathisen. E. (2011). Security challenges and solutions in cloud computing. *Proceedings of the 5th IEEE International Conference*. (pp. 208-21). Vancouver, Canada *IEEE*

Maughan, D., Schertler, M., Schneider, M., & Turner, J. (1998). RFC2408 - Internet Security Association and Key Management Protocol(ISAKMP). Rertrived on 22/11/2018 from http://www.ietf.org/rfc/rfc2408.txt

McFarlane, R. (2005). *Let's Add an Air Conditioner, Search Data Center news article*, retrieved from http://searchdatacenter.techtarget.com/ columnItem/ 0,294698, sid80_gciZ 1148906,00.html

McKinnie, M. (2016). *Cloud Computing: TOE Adoption Factors By Service Model In Manufacturing.* Atlanta: Georgia State University

Mell, P., & Grance, T. (2012). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication, 32(3),* 800- 145.

Mendel, P., C. L. Damberg, M. E. S., Sorbero, D. M. Varda, & Farley D. O. (2008). The Growth of Partnerships to Support Patient Safety Practice Adoption. *Health Services Research*, Accessed 01/03/15 from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2677037/

Mezias, S.J. & Glynn, M.A. (1993). The Three Faces of Corporate Renewal: Institution, Revolution, and Evolution. *Strategic Management Journal, 14(2),* 77-101.

Mircea M. & Andreescu A. I. (2011). Using cloud computing in higher education: A strategy to improve agility in the current financial crisis, *Communications of the IBIMA, 17(8),* 251-458

Mouratidis, H, Jahankhani, H & Nikhoma, MZ (2008). Management versus security specialists: an empirical study on security related perceptions. *Information Management & Computer Security, 16(2),* 187 -205

Nadji, Y., & Song, D. (2008). *Document Structure Integrity : A Robust Basis for Cross-site Scripting Defense* retrieved from www.oxit.it/ptest/v433/hit.html

Namjoo C, Dan K, Jahyun G, & Andy W (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Inform. Manage. Comput. Secur, 16(5),* 484–501.

Naone, E. (2009). Technology Overview: Conjuring Clouds – How Engineers are making on-demand Computing a reality. *MIT Technology Review, 15(3),* 254-465

Nguyen-Tuong, A., Guarnieri, S., Greene, D.,Shirley, J., Andevans, D. (2005). Automatically Hardening Web Applications Using Precise Tainting. *In Proceedings of the 20th IFIP International Information Security Conference* (SEC), (pp. 295–308) Manchester, UK. IFIP

Oliveira, T. and Martins, M.F. (2011). Firms patterns of e-business adoption: Evidence for the European union-27. *The Electronic Journal Information Systems Evaluation, 13(1),* pp 47-56.

Pallant, J. (2007) *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using SPSS*. Allen & Unwin.

Parisot, A. (1995). *Technology and Teaching: The Adoption and Diffusion of Technological Innovations by a Community College Faculty*, Montana State University, Bozeman, MT

Parsad, B., & Jones, J. (2005).*Internet access in U.S. public schools and classrooms: 1994-2003* (No. NCES 2005-015). U.S. Department of Education. Washington, D.C.: National Center for Education Statistics

Paulson, L., C. (2002) Proving Properties of Security Protocols by Induction. *In Proc. of the IEEE Computer Security Foundations Workshop, pages* 70–83. Montana, USA. IEEE Computer Society

Pedhazur, E.J. and Schmelkin, L.P. (1991) . *Measurement, Design, and Analysis: An Integrated Approach*. Taylor & Francis.

Perrin C., (2014). *Understanding Layered Security and Defense in Depth,* Retrieved from: http://www.techrepublic.com/blog/it-security/ understanding-layered-security-and-defensein-depth/

Porter, M. & Millar, V. (1985). How Information Gives You Competitive Advantage', *Harvard Business Review, 63(4),* 149–60.

Porter, M. (1990). *The Competitive Advantage of Nations*, Macmillan, London.

Prakash, P. G., & Sadhana, P, 2013. Virtual Local Area Network (VLAN). *International Journal of Scientific Research Engineering and Technology (IJSRET), 1(10),* 006-010

Premkumar, G. and Ramamurthy, K. (1995) . The Role of Interorganizational and Organizational Factors on the Decision Mode for Adoption of Inter-organizational Systems. *Decision Sciences, 26(3),* 303-336.

Premkumar, G. & Roberts, M. (1999). Adoption of new information technologies in rural small businesses. *Omega, 27(4),* 467-484.

Premkumar, G. & King, W.R. (1994). Organizational Characteristics and Information Systems Planning: An Empirical Study. *Information Systems Research, 5(2),* 75-109.

Premkumar, G. & Michael, P. (1995). Adoption of computer aided software engineering (CASE) technology: an innovation adoption perspective. *SIGMIS Database, 26 (3),* 105-124.

Premkumar, G. and Michael, P. (1995). Adoption of computer aided software engineering (CASE) technology: an innovation adoption perspective. *SIGMIS Database, 26(2-3),* 105-124.

Rai, A., Brown, P. & Tang, X., (2009). Organizational Assimilation of Electronic Procurement Innovations. *Journal of Management Information Systems, 26(1),* 257-296.

Ramdani, B. (2008) .*Technological, organizational & environmental factors influencing SMEs adoption of enterprise systems: a study in the northwest of England Manchester University*. University of Manchester, UK

Ramdani, B. and Kawaiek, P. (2007). SME Adoption of Enterprise Systems in the Northwest of England: An Environmental, Technological and Organizational Perspective', *in IFIP WG 8.6 - Organizational Dynamics of Technology-Based Innovation: Diversifying the Research Agenda*. Springer. *16(3),* 127-321)

Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Knowledge management and enterprise systems adoption by SMEs: Predicting SMEs' adoption of enterprise systems. *Journal of Enterprise Information Management, 1(2),* 10-24.

Riccardi, Oro, D., Cremonini, M. and Vilanova, M. (2010). A framework for financial botnet analysis in Crime. *Researchers Summit (eCrime)*, 15(2) 1-7.

Ristenpart T., Tromer E., Shacham H., and Savage S. (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *In Proceedings of the 16th ACM conference on Computer and communications security*, 2009, (pp. 199-212), New York USA. *ACM*

Rogers, E. (2003) *Diffusion of Innovations 5th edn*. New York: Free Press

Rogers, E. M. (1983). *Diffusion of InnovationsThird Ed.* The Free Press, New York, 1983

Rogers, E.M. (1995) *Diffusion of innovations, Fourth Edition ed*., New York, Free Press.

Sabnis, S., Verbruggen, M., Hickey, J., & McBride, A. J. (2012). Intrinsically Secure Next Generation Networks. *Bell Labs Technical Journal, 17(3),* 17-36.

Safa, N.S., Sookhak, M., Solms, R.V., Furnell, S., Abdul-Ghani, N., and Herawam, T. (2015). Information Security Conscious Care Behaviour Formation in Organisations. *Computers and Security, 53(6),* 65-78.

Sahin, I. (2006). Detailed Review of Rogers' Diffusion of Innovations Theory and Educational Technology-Related Studies Based on Rogers' Theory'. *The Turkish Online Journal of Educational Technology, 5(2),* 14-23.

Sarantakos, S. (1998) Social Research. Palgrave

Saunders M, Lewis P, Thornhill A (2007). *Research Methods for Business Students. 4th ed*. Harlow: Financial Times/ Prentice Hall.

Saunders, M., Thornhill, A. and Lewis, P. (2009) *Research Methods for Business Students. 5th edn.* Harlow: Financial Times/ Prentice Hall.

Savu, L. (2011).*Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges*. Tirunelveli, IEEE.

Scupola, A. (2003). The Adoption of Internet Commerce by SMEs in the South of Italy: An Environmental, Technological and Organisational Perspective. *Journal of Global Information Technology Management, 6(1),* 52-71.

Sinclaire, J. (2005). Current research in information security and privacy, *Proceedings of the 2005 Southern Association of Information Systems Conference.(p 22-61) LA, US. AISC*

Siponen, M., Mahmood, M., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies. *Communications of the ACM, 52(12),* 145-147

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34(2),* 503-522.

Stantonjm, Stamk, Guzmani & Calderac (2003). Examining the linkages between organizational commitment and information security. *In IEEE Systems, Man, and Cybernetics Conference*, (p 15-321), Washington DC. USA.

Stuart, W.D. (2000). Influence of Sources of Communication, User Characteristics and Innovation Characteristics on Adoption of a

Communication Technology, *University of Kansas, Communication Studies, Kansas 14(2),* 303-432

Swamy, N., Corcoran, B., Hicks, M. & Fable M. (2008). A language for enforcing user-defined security policies. *In the Proceedings of the IEEE Symposium on Security and Privacy.* Boston, USA

Tan, & Felix, T., C. (2010). A perception based model for technological innovation in small and medium enterprises. *Paper presented at 18th European Conference on Information Systems* (ECIS), (p.32-354) Vancouver, Canada

Tang, Q., Linden, L., Quarterman, J. S., & Whinston, A. B. (2013). Improving Internet Security through Social Information and Social Comparison: A Field Quasi-Experiment. *Workshop on Economics of Information Security, Texas USA*

Teo, T.S.H., Lin, S., and Lai, K. (2009). Adopters and Non-adopters of E Procurement in Singapore: An Empirical Study. Omega, *International Journal of Management Science, 37(5),* 972-987.

Thong, J. (1999). An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems, 15(4),* 187 -214.

Thorsteinsson, G., Page, T. & Niculescu, A. (2010). Using virtual reality for developing design communication. *Stud. Inform. Control, 19(1),* 93–106

Tipton, Harold F. & Krause, (2004). *Information Security Management Handbook, 5th Edition*. Tngton Books

Tiwana, A. and Bush, A. (2007). A comparison of transaction cost, agency, and knowledgebased predictors of IT outsourcing decisions: a US-Japan cross

-cultural field study. *Journal of Management Information Systems*, 24(1), 259-300

Tornatzky, L. G., & Fleischer, M. (1990). *The Process of Technological Innovation*. Lexington, Mass: Lexington Books.

Tornatzky, L.G. & Klein, K. (1982). Innovation characteristics and innovation adoption- implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management, 29(1),* 28-43.

Udeze, C., C., Okafor K.,C., Inyiama H.C., & Okezie C.C. (2012). Effective Security Architecture for Virtualized Data Center Networks. *International Journal of Advanced Computer Science Application, 3(1)* 196-200

Upadhyaya, D. & Jain, S. (2012). Model for Intrusion Detection System with Data Mining. *International Journal of Advanced Research in Computer Engineering and Technology, 1(3),* 145-148

Van de Ven, A.H. (1986). Central Problems in the Management of Innovation. *Management Science, 32(8),* 590-607

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49(3),* 190-198

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A Break in the Clouds: Towards a Cloud Definition. *Computer Communication Review, 39(1),* 50-55

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27(3),* 425-478

Von Solms, R. (2004). Towards Information Security Behavioural Compliance.

Computers & Security, 23(4), 191-198.

von Solms , B. (2001). Information Security - A multidimensional discipline. *Computers & Security, 20(6),* 504-508.

Vouk, M. A. (2008). Cloud computing: Issues, research and implementations. *Proceedings of 30th International Conference on Information Technology Interfaces*, (pp. 31—40), Delhi India. ICFTI

Wang, Y., Wang, Y. S., & Yang, Y. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. Technological Forecasting and Social Change. *Omega 3(5),* 211-451

Webster, J., Watson, R. (2002). Analysing the Past to Prepare for the Future: Writing a Literature Review. *MIS Q. 26(10),* 232–541

Weimer, J. (1995). *Research techniques in human engineering.* Englewood Cliffs, NJ: Prentice Hall.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stosser, J.(2009). Cloud Computing - A Classification, Business Models, and Research Directions. *Business & Information Systems Engineering, 1(5),* 391-399.

West, M. A., & Farr, J. L. (1990). *Innovation and Creativity at Work: Psychological and Organizational Strategies* Wiley, Chichester

Williams, M., Dwivedi, Y., Lal, B. & Schwarz, A. (2009) .Contemporary trends and issues in IT adoption and diffusion research. *Journal of Information Technology, 24(1),* 1-10.

Worthington, R. L. & Whittaker, T. A., (2006). Scale Development Research: A content Analysis and Recommendations for Best Practices. The Counseling Psychologist, *34(6)*, 806-838.

Yadav C. (n.d.). An Application of Security Threats on Electronic Business, (18710213).

Yeo, AC, Rahim, M & Miri L (2007). Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution. In *Proceedings of the Pacific Asia Conference on Information Systems 2007*, Auckland Australia. University of Australia

Youssef, A. & Emam, A. (2012). Network Intrusion Detection Using Data Mining and Network Behaviour Analysis. *International Journal of Computer Science and Information Technology, 3(2),* 87-98

Zaltman, Gary, Robert Duncan, & Jonny Holbek. (1973). *Innovations and organizations*. NewYork: Wiley.

Klein, K.J., Conn, A.B. & Sorra, J S. (2001). Implementing computerized technology: An organization analysis. *Journal of Applied Psychology, 86(5),* 811-824.

Zeller, W., & Felten, E. W. (2008). *Cross-Site Request Forgeries : Exploitation and Prevention. The New York Times*, 1–13. Retrieved from http://from.bz/public/ documents /publications/csrf.pdf

Zhang, Q., L. Cheng & R. Boutaba (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications, 1(7),* 1-18.

Zhu, K. & Kraemer, K.L. (2005) Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry, *Information Systems Research, 16(1),* 61-84.

Zhu, K., Dong, S.T., Xu, S.X. and Kraemer, K.L. (2006) Innovation diffusion in global contexts: Determinants of post-adoption digital transformation of European companies, *European Journal of Information* Systems, *15(6),* 601-616

APPENDICES A

QUESTIONNAIRE ON CLOUD AND IN-HOUSE DATACENTERS; DETERMINANTS OF SECURITY INNOVATIONS AT THE COLLEGES OF EDUCATION, GHANA

Dear Respondant,

You have been randomly chosen as a respondent in the above titled survey which is being undertaken as part of an educational research in partial fulfillment of Master of Education (Info Tech.) at University of Cape Coast. Your cooperation in filling this questionnaire will ensure
success of the study. Thank you

Demographic Data

Please provide information regarding yourself by ticking the appropriate box es

1. Your Sex: Male ☐ Female ☐

2. Please specify your age range:

18-25 ☐ 26-35 ☐ 36-50 ☐ 51-60 ☐ 60+ ☐

3. How many years of work experience do you have in the teaching profession?

Less than 2 years ☐ 3 to 5 years ☐

11-20 years ☐ 6-10 years ☐ More than 21 years ☐

4. Name of your institution ……..

5. Role at the institution

Management ☐ Lecturer ☐ Other ☐

6. Is your institution currently using any type of cloud computing services for its operations? (For example Dropbox, Google drive, Gmail)

Yes ☐ **No** ☐

7. If Yes, are you satisfied with the service you receive from the cloud provider?

Extremely Satisfied ☐ Very Satisfied ☐

Somewhat Satisfied ☐ Very Unsatisfied ☐ Extremely Unsatisfied ☐

If No, please answer question Q8:

Q8. Intention to use	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
a. I intend to use cloud computing in the next 12 months					
b. I predict I would use cloud computing in the next 12 months					
c. I plan to use cloud computing in the next 12 months					

9. Do you have controls against the following system vulnerabilities (Tick to signify Yes or leave blank to signify No)

DDoS/DoS ☐ Code execution ☐ Buffer Overflow ☐

Memory corruption ☐ Directory Traversal ☐ XSS ☐

Improper Access Control (Authorization) ☐

SQL Injection ☐ Man-In-The middle attack ☐

10. Do you have controls against the following Threat actors (Tick to signify Yes or leave blank to signify No)

Bot-Network ☐ Malicious Insider ☐ Data corruption ☐

Insecure APIs ☐ Insecure Web Applications ☐

We-based Attack ☐ Phishing ☐ Spyware ☐

Spammers ☐ Malware (Virus, Trojan Horse, Worms) ☐

11. Which of the following technical control measures do you have in place (Tick all that apply)?

Firewalls, IDS/IPS ☐ Secure Remote Access (VPN) ☐

Anti-Virus ☐

Data Encryption Systems ☐ Vulnerability scanning tools ☐

Code Analysis Tools ☐ Secure Access-Control Measure ☐

Enterprise Baseline Security Analyzers ☐

Network/Remote Control Monitoring Systems ☐

Secure Network Transmission Control Systems ☐

Behavioral Profiling and Monitoring (Background Checks) ☐

Security innovation is the possession of ideas, systems, practice, products or technologies that are new to the adopting organization which is aimed at improving the confidentiality, integrity and availability of Information System assets

12. Please tick on stages that are applicable to your institution

Innovation	Stage
1. My institution is not familiar with security technology	
2. My institution is familiar with security technology and /or has considered using it	
3. My institution is planning to use security technology within the next 24 months	
4. My institution has launched pilot projects or initiatives for evaluating and/or trailing security technology	

12. Please tick on stages that are applicable to your institution (Cont'd)

5. The acquisition of specific security technology are planned, in progress, implemented or cancelled	
6. My institution has security technology but we have yet to establish a program of regular use	
7. My institution has security technology and we have established a program of regular use	

To what extent do you agree or disagree with the following statements?

13. Relative Advantage	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
RA1: Using innovative security technology would makes it easier for us to do our job					
RA2: Using innovative security technology would improve our job performance					
RA3: Using innovative security technology would enable us to accomplish tasks more quickly					
RA4: Using innovative security technology would enhance our effectiveness on the job					
RA5: Innovation allows us to use the latest version of security technology					

14. Complexity	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
CY1: Working with security technology is complicated, it is difficult to understand operational procedures					
CY2: It takes too long to learn how to use security mechanisms to maintain audit logs to make it worth the effort					
CY3: Learning to operate innovative security technology is easy for me					
CY4: It takes too much time for me if I want to use secured connection to do my normal duties					
CY5: In general innovative security technology is very complex to use					

15. Compatibility	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
CM1: I think using innovative security technology fits well with the way our institution usually performs					
CM2: Using innovative security fits into our institution's work style					
CM3: Using innovative security technology is compatible with our					

institution's norms and culture					
CM4: Innovative security technology can easily be integrated into our existing IT infrastructure					
CM5: Innovative Security technology is NOT compatible with other systems that we are using					

16. Top Management Support	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
TM1: Top management provides resources for adopting security innovations					
TM2: Top management supports the implementation of security innovations					
TM3: My top management is likely to consider the adoption of security technology as strategically important					
TM4: The Institution's top management provides strong leadership and engages in the process when it comes to information security technologies					
TM5: Our top management exhibits a culture of enterprise wide information sharing.					

17. Technological Readiness	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
TR1: My institution hires highly specialized or knowledgeable personnel for security technology services.					
TR2: We have sufficient technological resources to implement innovative security systems – unrestricted access to computer.					
TR3: We have sufficient technological resources to implement security systems – high bandwidth connectivity to the internet.					
TR4: We allocate a percent of total revenue for security technology implementation in the institution.					
TR5: Our organization has the in-house expertise to implement security systems					

18. Competitive Pressure	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
CP1: Our institution thinks that innovative security technology has an influence on competition in their industry					
CP2: Our institution is under pressure from competitors to adopt security systems					

CP3: Some of our competitors have already started using innovative security technologies					
CP4: It is easy for our customers/students to switch to another institution due to secure security systems in place					
CP5: We believe that our competitors get many advantages from using security systems					

19. Regulatory Compliance	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
RP1: Ghanaian laws and regulations are sufficient to protect and facilitate the use of security systems					
RP2: Specific and individual controls to meet security systems policies are well documented in my institution					
RP3: Our institution has an implemented procedure to ensure compliance with legal restriction and intellectual property					
RP4: Ghanaian universities and colleges will be adopting security innovations in the near future					
RP5: My institution conducts					

regular review to ensure compliance with security policies					