2020

Strategies for Reducing the Risk of Data Breach Within the Internet Cloud

Latasha Rivers
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Latasha Rivers

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Yvette Ghormley, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Alexandre Lazo, Committee Member, Doctor of Business Administration Faculty

Dr. Kim Critchlow, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Strategies for Reducing the Risk of Data Breach Within the Internet Cloud

by

Latasha Rivers

MBA, University of Phoenix, 2011

BA, George Mason University, 2010

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2020

Abstract

Businesses are increasingly incorporating cloud computing into their current business models. With this increase, security breach exposure has also increased, causing business leaders to be concerned with financial hardship, operational disruption, customer turnover, and customer confidence loss due to personal data exposure. Grounded in the integrated system theory of information security management, the purpose of this qualitative multiple case study was to explore successful strategies some information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches. The participants were 7 information security leaders from 7 different aerospace and defense contractor companies located in the United States mid-Atlantic region. Data from semistructured interviews were analyzed and compared with 8 publicly available data sources for data triangulation. Emergent themes narrowing this knowledge gap was extracted through an analysis technique such as coding and then triangulated. The recurring themes were (a) strong authentication methods, (b) encryption, and (c) personnel training and awareness. A key recommendation includes information security leaders implementing preventative security measures while improving an organization's ability to protect data lost within the Internet cloud. The implications for positive social change include the potential to increase consumers confidence while protecting confidential consumer data and organizational resources, protecting customers from the costs, lost time, and recovery efforts associated with identity theft.

Strategies for Reducing the Risk of Data Breach Within the Internet Cloud

by

Latasha Rivers

MBA, University of Phoenix, 2011

BA, George Mason University, 2010

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2020

Dedication

First off, I would like to thank God for giving me the strength, courage, and drive to complete and obtain my doctoral degree. Through the good, bad, and challenging times, it was God's grace that brought me through and without him this accomplishment would have not been possible. Again, I thank you. To my parents, Annette Rivers, Eddie and Jennifer Rivers, words cannot explain the continued support, encouragement, and push you all gave me especially when times became rough. On a daily basis, you encouraged me to do better, be better, and always follow my dreams while keeping God first. You consistently reassured me that this journey was not going to be easy because if it was everybody would be doing it, however, you made sure to push me to my best ability because you believed that I could do it. And for that, I want to say thank you and I hope I made you all proud. To my younger brother, Anthony Rivers, thank you for being my rock through the most trying times and reassuring me to go hard for the things I want to achieve and to always move forward. To my love and best friend Tori Sterling, I have never met a person who is as strong and remarkable as you are. Your perseverance and faith made me a stronger person each day. You continue to support me and everything that I set my mind to, you stayed by my side during the times of frustration, you unselfishly remained understanding whenever I needed the times to complete deadlines and research, and most importantly, you encouraged me to stay motivated and prayed up. And for that, I thank and love you. Lastly, to my extended family and friends, thank you for your motivation, understanding, patience and being a listening ear through this whole process.

Acknowledgments

The doctoral process was not an easy journey and at times I felt like I wanted to give up; however, I am grateful for the two chairs that I was fortunate enough to share this experience with; Dr. Krista Laursen and Dr. Yvette Ghromley. Dr. Kirsta Laursen, where do I begin, thank you for reassuring me that I can do this and for turning back on the light I had in my eyes when I first started the program. You took so much of my writing and myself and quickly turned it around within a year and made many things happen. Under your direction, you was able to get my prospectus, proposal, and oral presentation done a little under a year of me being under your instruction. You paid attention, was responsive, and I truly felt like you was going through the process with me. You were the guidance and encouragement I needed for that specific time of my life. Thank you.

Dr. Yvette Ghromley, earning this title would have not been possible without your push, guidance, and constant encouragement. You continued to challenge me in the best way possible and consistently remained professional through all interactions. The commitment you displayed did not go unnoticed and you help me fulfill my dreams of becoming a doctor. I would like to take the time to acknowledge my Second Committee Member, Dr. Alexandre Lazo and URRs, Dr. James Savard and Dr. Kim Critchlow for taking the time out and providing guidance and wisdom in improving my study. Your timely comments and suggestions added great value to my study and I am forever grateful.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

As computer technology continues to advance, both government and private entities have become dependent on computerized information systems that solely carry out all operations and processes, while maintaining and reporting essential information (Wilshusen, 2015). Cloud computing has emerged and evolved due to the many advantages it offers organizations and end users (Saeed & Khan, 2015). The storage of information in the cloud offers significant benefits, including lower data storage costs, enhanced data mobility, and sharing (Bayramusta & Nasir, 2016). Both public and private entities rely on computer systems to transmit proprietary and other sensitive information, conduct operations, process business transactions, and deliver services (Wilshusen, 2015). However, risks associated with cloud computing include threats to the privacy and security of cloud data and a potential for data breaches to occur (Agarkhed & Ashalatha, 2017). Given the increased use of cloud computing, organizations require an understanding of strategies that are necessary for protecting cloud-based data from security breaches.

Background of the Problem

Data breaches affect United States retailers and consumers. The occurrence of data breaches can prompt concerns within the public about the security of personal information stored electronically by corporations and other private entities (Dolan, 2015). Companies should focus on the prevention of data breaches by improving organizational data security standards, protecting customer personal identifiable information (PII), and notifying customers when their data has been compromised once information has fallen into the wrong hands (Weiss & Miller, 2015). Data security is a serious factor to consider in a cloud environment.

Cloud computing offers many advantages over traditional central processing unit (CPU) infrastructures by offering individuals and organizations enhanced data durability, availability, scalability, and flexibility at a lower cost (Luo et al., 2018). The potential risks associated with storing information in the cloud has the potential to overshadow all benefits (Kajiyama et al., 2017). Ineffective protection of data stored in the cloud can result in the loss or theft of assets and funds. Other effects of cloud data breaches include (a) inappropriate access to and disclosure, modification, or destruction of sensitive information such as national security information, PII, and proprietary business information; and (b) disruption of corporate operations (Wilshusen, 2015). The aim of this qualitative multiple case study was to explore the strategies that information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches.

Problem Statement

In 2015, the U.S. Office of Personnel Management (OPM) was the victim of a security breach that resulted in the unauthorized disclosure of sensitive information of 21.5 million government employees, including congressional staff (Christensen, 2015). Security breaches have cost the U.S. economy from $57 to $109 billion annually, with financial losses from these breaches continuing to increase (The Council of Economic Advisors, 2018). The general business problem was that theft of organizational information due to a security breach negatively affects the profitability of some companies. The specific business problem was that some information security leaders in the aerospace and defense contractor industry lack successful strategies to protect cloud-based data from security breaches to improve organizational profitability.

Purpose Statement

The purpose of this qualitative multiple case study was to explore successful strategies that some information security leaders in the aerospace and defense contractor industry used to protect cloud-based data from security breaches to improve organizational profitability. The population consisted of seven information security leaders within seven aerospace and defense contractor companies in Washington, D.C., who have implemented successful strategies to protect their cloud-based data from security breaches to improve the profitability of their organizations. The implications for positive social change may include the potential for information security leaders to learn of strategies to prevent security breaches of personal data that were stored by commercial companies, which may benefit members of the public by helping them avoid the expenses, inconvenience, and disruptions that these breaches may cause.

Nature of the Study

I employed a qualitative methodology for this study. Researchers use the qualitative method to explore the phenomena under investigation in depth (Khan, 2014). The qualitative method was appropriate for this study because the goal of the study was an in-depth exploration of successful strategies that managers used to protect cloud-based data from security breaches. Researchers use the quantitative method to test theories or hypotheses about variables relationships or differences (Barnham, 2015). The quantitative method was not appropriate because, in this study, I did not test theories or hypotheses. Researchers use the mixed methods approach to combine both qualitative and quantitative methods (Steen et al., 2018). The mixed method approach was not appropriate for this study because, in this study, I utilized the qualitative method to explore strategies some information security leaders used to protect cloud-based data from security breaches and therefore did not use the quantitative approach.

The research design for this study was a case study. Case study researchers conduct in-depth explorations of a single person, a group of people, or an organization (Yin, 2017). Researchers use a narrative design to study an individual's life experiences in chronological order through the participant's stories (McAlpine, 2016). A narrative design was not appropriate because I did not focus on individuals' experiences in my study of strategies to protect cloud-based data from security breaches. In a phenomenological model, the researcher seeks to explore the essence of the phenomenon by exploring personal views of the lived experiences (Alase, 2017). A phenomenological design is not appropriate because I did not examine the essence of the phenomenon by exploring personal views of the lived experience. In an ethnographic design, the researcher focuses on studying cultures (Draper, 2015). The ethnographic design is not appropriate because I did not study a group's culture.

Research Question

The research question for this study was: What successful strategies do some information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches to improve organizational profitability?

Interview Questions

1. What successful strategies do you use to protect cloud-based data from security breaches?

2. How do you assess the effectiveness of your organization's strategies for protecting cloud-based data from security breaches?

3. What strategies were not successful for protecting cloud-based data from security breaches?

4. What barriers did you encounter to the implementation of successful strategies for protecting cloud-based data from security breaches?

5. How did you overcome these barriers to the implementation of successful strategies for protecting cloud-based data from security breaches?

6. What additional information would you like to add regarding securing cloud-based data that you have not discussed?

Conceptual Framework

The conceptual framework for this study was the integrated system theory (IST) of information security management. Hong et al. (2003) introduced the IST to help identify unknown gaps and the lack of pertinent information related to information management theories. Hong et al. (2003) applied the IST to help establish controlled systems and security policy. The key constructs or propositions underlying the IST are security policy, internal controls, and contingency management (Hong et al., 2003). Within the workplace, for example, managers use a security policy to protect an organization by setting expectations, establishing appropriate rules for user behavior, and establishing a baseline of employees' responsibilities (Hong et al., 2003). Company managers use internal controls to help prevent, detect, or reduce fraud and theft within their organizations (Hong et al., 2003). Managers use contingency management to identify vulnerabilities or threats and implement countermeasures to prevent an incident or limit the effects should an incident occur (Hong et al., 2003). Therefore, IST could be a relevant lens to understand the effective strategies that some information security leaders use to protect cloud-based data from security breaches.

Operational Definitions

Cloud computing: Cloud computing is a form of technology in which users store and access data on on-demand servers over the Internet (Masrom & Rahimli, 2015).

Cloud data storage: Cloud data storage refers to a technology in which organizations use the Internet and central remote servers to maintain data and allow the sharing of applications (Goyal, 2014).

Data breach: Data breach, commonly known as a security breach, is unauthorized access to sensitive, secured or personal data (e.g. name, social security number (SSN), email address, passwords, debit/credit card information, financial account information, medical records, driver's license numbers, etc.) resulting in privacy being compromised without personal knowledge (Holtfreter & Harrington, 2015).

Hybrid cloud: A hybrid cloud is a cloud solution in which companies maintain control of an internal managed private cloud while relying on the public cloud on an as needed basis (Singh & Singh, 2017).

Identity theft: Identity theft occurs when an unauthorized party uses another person's personal information to commit fraud (Holtfreter & Harrington, 2015).

Infrastructure as a service (*IaaS*): IaaS provides resources that are managed and can easily be scaled up as services to a variety of users (Ouahman, 2014).

Platform as a Service (*PaaS*): Platform as a Service is an infrastructure used by companies to develop, execute and deploy their applications or software in a public or private cloud environment. Examples of PaaS include Google App Engine, Windows Azure, Engine Yard and Force.com (Garg & Goel, 2017).

Private cloud: Private cloud is a computing service offered through a private network to select individuals while providing flexibility, scalability, provisioning, automation, and monitoring (Singh & Singh, 2017).

Public cloud: In a public cloud, the service provider makes resources such as applications (also known as Software-as-a-service) and storage, available to the general public (Singh & Singh, 2017).

Software as a Service (*SaaS*): Software as a Service (SaaS) is an infrastructure that provides a subscription versus an application that an organization must buy, maintain, and upgrade itself. Examples of SaaS include social media sites, office software, and online games (Garg & Goel, 2017).

Assumptions, Limitations, and Delimitations

In the following section, I summarize the assumptions, limitations, and delimitations of this qualitative study. A researcher reveals assumptions during a study that others can perceive as truths or beliefs (Dean, 2014). Limitations are inherent weaknesses throughout the study (Breaux et al., 2014). The researcher imposes delimitations, which involve the design of the study (Dean, 2014).

Assumptions

Assumptions are factors the researcher assumed to be true that may influence conduct of a study (Marshall & Rossman, 2016). First, the researcher assumed all participants possessed the necessary knowledge to respond to the interview questions. Rutberg and Bouikidis (2018) suggested that qualitative researchers consider the participants in qualitative research as experts or have had exposure in the appropriate area of the study. Second, the researcher assumed each participant provided truthful responses and, as a result, the data received reflected the complications that can arise when data breaches occur in a cloud environment. Third, the researcher assumed the chosen research method was the appropriate choice for this study and was effective in providing the information needed to answer the research question.

Limitations

Limitations in a study are potential weaknesses that are out of the researcher’s control and can have an effect on the validity of the study (Leedy & Ormrod, 2015). One limitation may have been unknown factors where the participants work that could have biased their responses. Second, I limited my study to seven companies in the aerospace and defense contractor industry in the Washington, D.C., area, so my study findings may not be applicable to other sectors. The third limitation was that the participants might not have had the appropriate knowledge to make informed responses. Last, I obtained data for this study from information security leaders in a limited geographic area in a particular industry. Accordingly, findings from this study may not represent the views and experiences of information security leaders in other geographic locations.

Delimitations

Delimitations are those factors within the researcher's control that can limit the scope and create boundaries for the study (Rosenberg & Koehler, 2015). The first delimitation was my focus on private industry and not on the government or education sectors. Second, I included only information security leaders from seven aerospace and defense contractor companies in the study. Finally, I focused the study on contractor companies in Washington, D.C.

Significance of the Study

The significance of the study includes the potential for managers to learn successful strategies they can use to help reduce the breach of data within the cloud. Findings from this study could be of value to information security leaders who may learn of strategies to reduce unwanted security breaches, thereby contributing to the financial performance of their organizations. Information security leaders may also gain knowledge about how to implement more secure networks necessary for safeguarding customer and consumer data.

Contribution to Business Practice

Information security leaders may use findings from this study to review and identify successful strategies they can use to help reduce the breach of data within the cloud. Data security breaches and identity theft are becoming a primary concern in today's world (Sen & Borle, 2015). In 2014, a survey of 500 senior-level information technology (IT) and security decision makers showed that 53% of employees expressed a concern about security issues within the cloud (Ksherti, 2014). As organizations continue with IT integrations, there is an increase in risk that could cause harm or disrupt services (Department of Homeland Security, 2015). Business leaders might use findings and conclusions from this study to improve their business practices by identifying problems with security in the cloud and enhancing the knowledge of their managers regarding security-related issues to improve the protection of systems from data breaches.

Implications for Social Change

Recognition of current procedures information technology managers use to mitigate cloud-based data security breaches may assist information security leaders in controlling the effects of breaches on business performance and consumer costs. Data privacy requirements and the need to meet client data privacy expectations with regard to PII require organizations to achieve an appropriate level of control and security of cloud-based data at all stages, from collection, to processing, to destruction (Charlesworth & Pearson, 2013). Because data breaches arising from theft, unauthorized access/disclosures, or hacking incidents continue to increase every year (Wikina, 2014), information security leaders might use findings from this study to design and implement security strategies useful for strengthening the security and resilience of cloud-based data and to protect consumers from the costs, lost time, and recovery efforts associated with identity theft.

A Review of the Professional and Academic Literature

Scholars use literature reviews as a distinctive form of research that creates new awareness about the topic being studied (Torraco, 2016). The design of a literature review involves reviewing, analyzing, and synthesizing literature on a topic in an integrated way such that new frameworks and perspectives on the topic are generated (Torraco, 2016). A researcher can conduct a literature review for different purposes and various audiences. Cooper (1988) categorized the elements of the literature review into the following: focus, goals, perspective, coverage, organization, and audience. In contrast, some scholars assume most literature reviews focus on the research findings of the literature reviewed, research methods, or theories used in the literature (Torraco, 2016). Therefore, a literature review includes substantive findings.

In this literature review, I provide an in-depth analysis of some theories that prior scholars used when conducting research on data breaches. Additionally, the literature review includes information on 15 themes. The themes include (a) history of the cloud; (b) IST; (c) opportunities and challenges for cloud computing; (d) privacy and security; (e) data privacy; (f) latency, reliability, and performance predictability; (g) inoperability and portability; (h) data breach in fiber optic networks; (i) storage of data over internet protocol (IP) networks; (j) attacks in the cloud environment; (k) effective strategies to control security breach in the cloud; (l) security policy; (m) risk management; (n) internal control; and (o) contingency management. The researcher chose the themes to highlight the effects pertaining to risks and the possible effects of data breaches on both individuals and organizations, and security incidents significant to IT professionals.

I provide information regarding some recently published empirical research studies on data breaches. I utilized peer-reviewed articles within the databases found in the Walden Library and searched for relevant articles using the following terms: *cloud computing, cloud services, cloud software, risk, breach, security,* and *privacy*. I also worked with Walden University librarians by scheduling a time to go over any relevant key terms and potential sources to help develop this literature review. Moreover, I used the Google Scholar search engine to locate articles relevant to this literature review.

Majority of databases and electronic means available to the public will be limited to only articles published in 2015 and beyond. Last, to identify articles for this literature review, I selected relevant articles and empirical studies geared towards information privacy and security, reliability, inoperability, risk management, and challenges in the cloud. I included 69 sources in the literature review. Of these sources, 59 (86%) were peer-reviewed and verified through Ulrich (which is offered by Walden University). Additionally, of the 69 sources, 28 (41%) of the sources are within 5 years of my expected chief academic officer (CAO) approval date.

History of the Cloud Environment

The history of cloud computing dates back to the 1960s. Cloud computing has become an emerging technology with dynamic scalability and the use of virtualized resources as a service expanding the Internet, which continues to enable business to surpass their competitors in performance (Catteddu & Hogben, 2009; Ercan, 2010; Goscinski & Brock, 2010; Wu, 2011; Thomas, 2011; Kasemsap, 2015). Cloud computing has become a trend within the past decade. At a more personal level, customers consider that accessing the cloud is an easy and affordable action within their day-to-day social life and business operation (Kouatli, 2014). For example, users can use the cloud to download music files from a mobile device and synchronize with a home computer or vice versa (Kouatli, 2014). This gives users flexibility and convenience to access their electronic information from wherever they might be located.

Cloud computing was first introduced to allow people in different time zones to benefit from the available resources it provides. Sultan (2013) argued that cloud computing delivers a range of IT services remotely through a networked IT environment. Additionally, the cloud continues to manifest and can be classified as external/public cloud, internal/private clouds, and hybrid. External/public clouds are accessible on the internet through web services from an off-site third-party provider on a self-service basis; internal/private clouds handle data and processes that are typically managed within an enterprise without limiting network capacity or security exposures; and hybrid clouds consist of both internal and external cloud computing solutions (Wei-Wen et al., 2013). The cloud offers scalable on-demand services to consumers with greater flexibility, lesser infrastructure investment, and accessibility (Modi et al., 2013). The cloud provides convenience for all personnel and employees.

The cloud became a centralized stationary system based on current IT convenience such as an increase of capacity or added capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software (Kumar et al., 2012). In contrast, cloud computing offers many benefits to the IT industry by offering unlimited storage and computing capacity (Habiba et al., 2014). Despite the attractive features, the rate of migration to the cloud has been slow mainly due to the inherent security challenges associated with the technology (Habiba et al., 2014). Cloud computing continues to go through many changes as IT continues to evolve leaving more room for vulnerability. As a result, cloud computing emerged from a period in which underlying computing resources were both limited and costly to a period in which the same services were affordable and abundant (Kushida et al., 2015).

Cloud computing services are divided into three categories: Infrastructure as a service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS; Joan, 2014). The delineation by architectural layers illustrates how cloud computing is separate from an outsourcing center. A service that does not differentiate between the architecture layers cannot be considered cloud (Kushida et al., 2015). IaaS can provide access to computing resources in a virtualized environment across the Internet. PaaS offers a framework and environment in which developers can create internet-based applications and services over the Internet that are hosted in the cloud and accessible through a web browser. SaaS is any cloud service that gives consumers access to software applications over the Internet, and both individuals and organizations can use it for a wide range of tasks (Joan, 2014). As a result, the cloud offers flexibility by allowing individuals the capability of document control and working from any location just from moving to the cloud.

Integrated System Theory of Information Security Management

In the contemporary world, cloud computing is a powerful technology that eliminates the need to maintain expensive computing hardware, space, and software

(Hashem et al., 2014). With all the advantages that come with the cloud, issues associated with cloud use become a greater risk to an organization. Measures of intervention are lacking because security issues of cloud data constantly are subject to threats both from within and without. In an attempt to protect confidential and sensitive information, IT security managers are referring to past studies or strategies regarding how to make commercial clouds secure (Ismail et al., 2015).

This study reviews the past strategies in relation to effective intervention methods. Intervention methods are useful in helping IT managers or system administrators to manage cloud security to overcome challenges in their organizations (Ismail et al., 2015). The current research focused on reviewing the literature on IST in addition to cloud security components and associated challenges as well as security strategies to address the threat concerns (Tabrizchi & Kuchaki, 2020). In achieving this, the configuration of literature review content is developed where the IST is built upon components as well as relevant studies, and then customizing it in forming the study's conceptual model that integrates the theory itself with cloud security breach concerns and effective strategies to control or eradicate them.

IST is based on the principles of contingency management and is an integration of information security policy, internal control, information auditing theories, and risk management to establish an information security architecture (Hong et al., 2003), which is in conformity with the objectives of an organization as shown in Figure 1. IST can be associated to three key aspects: (a) information security, which is a function of risk management, information security policy, information auditing, and contingency management; (b) internal control, which consists of the control of physical security, control of personal security, access control, network and systems security control, maintenance control, business continuity management, and system development; (c) and contingency management, which encompasses both internal and external environments of an organization, information techniques, and information management (Sindhuja & Kunnathur, 2015; Yang et al., 2016).

A suitable theory includes a scope, explanation accuracy, prediction precision, and parsimony (Ismail et al., 2015). A theory is capable of making accurate predictions and has the ability of explaining concepts with the use of a few variables (Yang et al., 2016). IST is practical, useful, and comprehensive to this study.

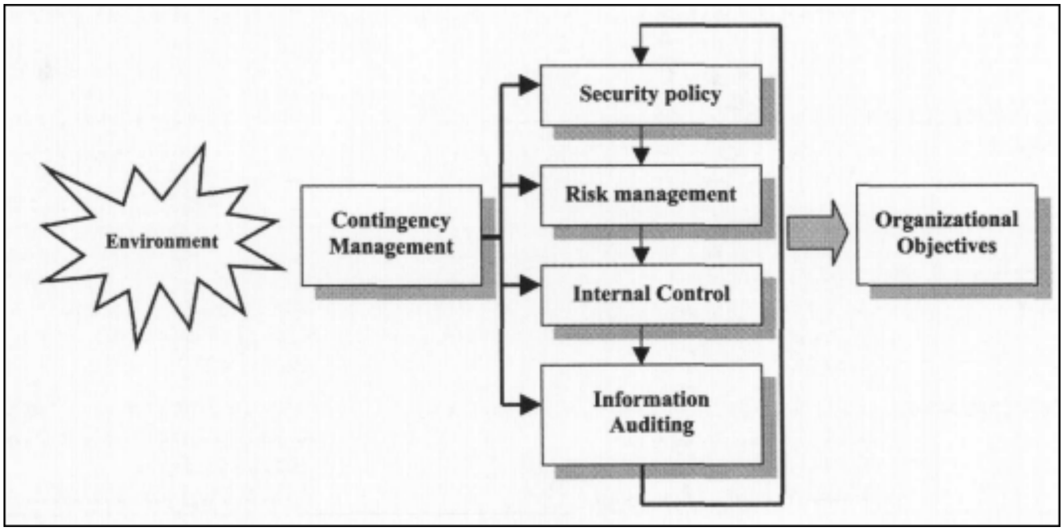

Figure 1. A diagrammatic illustration of Integrated System Theory. Adapted from "An Integrated System Theory of Information Security Management," by K. S. Hong, Y. P. Chi, L. R. Chao, and J. H. Tang, 2003, *Information Management & Computer Security,*11, p. 247. Copyright 2003 by Emerald Publishing Limited.

The integrated system theory of information security management (ISTISM) framework, which is a modification of IST, is relevant to this study as a broad framework that is suitable for examining decisions, actions and behaviors related to information security within an organization (Hong et al., 2003). The adoption of the model is timely because researchers have focused on identifying the security breaches in the cloud and providing effective management strategies for the security threats. Scholars continue to use IST as their foundation within their theoretical framework in security research studies.

Dzazali et al. (2009), Ismail et al. (2014a), Ismail et al. (2015), Järveläinen (2012), and Sindhuja & Kunnathur (2015) all utilized IST within their research involving security. Dzazali et al. (2009) used both IST and social-technical system theory as a framework while taking an exploratory approach in examining the factors involved in the information security management systems of Malaysian public service (MPS) organizations. Based on previous constraints and current challenges faced by most organizations, researchers were motivated to address another issue associated with information security management by figuring out what would be the most cost-effective approach in order to protect information assets and ensure business continuity (Dzazali et al., 2009). Within Dzazali et al. (2009) research, they observed that an effective information security management system should focus on technology, people, processes and business goals.

Dzazali et al. (2009) demonstrated that individuals from the middle and top-level management group personal perception could have a positive influence on implementation of security practices within an organization. Both middle and top-level individuals in the management group are directly or indirectly accountable for either safeguarding or protecting their organizations system assets. As a result, Dzazali and Zolait (2012) conclusions were consistent with the key conceptions of IST where risk management and an organization's environment are a function of information security. In addition, their conclusions disclosed that risk management is a key component of an organization's security framework. Dzazali et.al (2009) findings are similar to those of Ismail et al. (2014a); additional layers to safeguarding information should be required. However, organizational leaders fail to implement appropriately.

According to Ismail et al. (2015), the addition of more layers to the existing theory or model can make it more difficult for unauthorized agents to hack the system as professionals put extra measures in place. The added assurance layer has the ability of immediately notifying the system administrator concerning the problem, hence, prevention of an intrusion (Ismail et al., 2014a). Adding an assurance layer is done with the determination of a strategy, which is capable of boosting the cloud security of an organization, and the researcher is hopeful that the model or framework would play a key role in helping IS security managers to put in place effective security strategies in addressing data breaches in the clouds.

The determination of organizational security requirements necessitates evaluation of the informational sharing approach internally, and a level of informational confidentiality is necessary. To ensure that the security requirements were taken into consideration, the researchers focused on the measurement of organizational security goals based on IST's four main components (security policy, risk management, internal control, and contingency management). Using these four components, the researcher of the study investigates their implementation in 101 organizations that use Supervisory Control and Data Acquisition (SCADA). A characteristic of a SCADA layout consists of SCADA servers, workstations, programmable logic controllers, remote terminal unit, port servers, and communication links that connect SCADA networks to the corporate local-area network (LAN; Hentea, 2008).

SCADA is susceptible to interruptions either in the form of system failure or intentional attacks and are sources of problems for a company. As such, Ismail et al. (2015) sought to measure the goals of information security of organizations using SCADA systems and the extent to which such companies are aware of information security mechanisms implementation. The growing need for SCADA systems to connect the corporate networks equally leads to the creation of risks and the introduction of vulnerabilities (Ismail et al., 2014a). Confidential and private information such as maps, networks, names, and network system configurations are a broad assessment by the public via the Internet. By getting such information, an unauthorized agent is able to access as well as manipulate SCADA networks.

SCADA systems are also susceptible to vulnerabilities. An array of deliberate attacks often targets SCADA systems with the aim of obtaining confidential information and/or have the ability to maneuver through private networks and intentionally curtail the delivery of service (Ismail et al., 2015). The attacks have a high likelihood of resulting in economic, financial, and human loss (Kovaliuk et al., 2018). In using IST, the survey given by Ismail et al. (2014a) revealed that there was a positive relationship between securing SCADA systems and measurement of risk management, security policies, contingency management, and internal controls. Subsequently, from the analysis it is evident that the security policies' availability positively affects the information security goals of organizations (Shahzad et al., 2016). From the survey, majority of individuals were aware of the issue and did implementation of security policies (Shahzad et al., 2016).

The majority of organizations were still utilizing default platform alignments, which led to complexity. Companies were susceptible to future attacks and, therefore, efforts with the aim of increasing available technology and system specific knowledge for the experts in managing SCADA systems were necessary (Kovaliuk et al., 2018). Irrespective of this, some organizations were of the opinion that vital platform configurations should be stored, and backups done accordingly for the purposes of business continuity (Ismail et al., 2014b). Additionally, virtually all the organizations realized the significance of implementing internal security assessment mechanisms and appointing an individual with the expertise to carry out steady security assessments (Bhatia & Malhotra, 2018). Last, a majority of the leaders within the organization trusted that they had sufficient operations continuity and documentation for disaster recovery. In summary, the study by Ismail et al. (2015) analyzes the role of IST in eradicating security breaches of data based on risk management, security policies, contingency management, and internal controls.

Sindhuja (2014) used IST when exploring information security initiatives and supply chain performance and operations that were determined to have an influence on supply chain operations and performance. The researchers highlighted that information security practices are essential in the prevention, detection, and response to security incidents (Hustad et al., 2020). Some organization leaders have a misguided belief that they should consider information security after a disaster takes place (Sindhuja, 2014). The key to organizational success includes understanding and tracking of data generation and processing of data for deriving useful information to operate a condusive supply chain (Biswas & Sen, 2016). Additionally, by implementing common organizational practices such as training programs, policies, procedures, and well-established communication processes, organizational leaders can solve both technological and cultural challenges found within some organization (Sindhuja & Kunnathur, 2015) which remains consisted with Ismail et al.

Ismail et al. (2014a) employed the use of IST in monitoring the critical infrastructure level of the security system. Critical infrastructure systems are vulnerable to disruption, and these disruptions pose a challenge to society as crucial resources such as water, transport, and gas, among other important utilities. The researchers examined critical infrastructure services and the systems that monitored and controlled such critical services (Ismail et al., 2014a). Additionally, the researcher geared the study toward measuring the aspects of information security of those systems using IST with critical examination of the critical components such as policies concerning cyber security, risk assessment and management, process and technical controls, information auditing, and internal control management (lfinedo, 2012).

In achieving the aim of the study, the researchers used preliminary interviews in an attempt to seek the opinions of experts from various countries on significant themes related to IST such as assessments and compliance, awareness, controls, and measures. Consequently, the researchers conducted a pilot study that presented results taken by experts from various countries as well as experts working in different sectors, especially on information security involving critical infrastructure in their respective countries. Based on this, Ismail et al. (2014b) was able to examine the components of prevailing policies and implemented controls by various organizations worldwide. As a result, it was evident that measuring and estimating controls implemented and security awareness at the organizational level were possible through the application of IST.

Ismail et al. (2014b) was able to apply the principles of IST successfully in developing a framework to address security concerns of SCADA. SCADA systems in governing the infrastructure of organizational security data security must have the capability of assuming the following five roles: assuring systems security, reliability emphasis, protection capability, sustainability, and validation of cost-effectiveness (Ismail et al., 2014a). Consequently, if the ascertainment of the following assurances is not possible, then SCADA systems attack categorization is three-fold, namely: attacks on central controller, communication networks, and filed units (Kovaliuk et al., 2018). Such attacks can either be malicious settings, physical, malicious alterations, service denial, sniffing, proofing, or malicious alarms (Abdul-Ghani et al., 2018).

SCADA security systems are of held in a high esteem so that confidential data or organizations can be secure from access by unauthorized agents with detrimental intentions. Subsequently, compartmentalization of security policies is necessary to avoid overlaps, and every policy is efficient and effective in areas of communication, data, personnel, platform and physical security, application and configuration management, audit, and manual operations (Ismail et al., 2014b). For instance, in the case of generating electric power, organizations take into consideration four components, which includes system and device monitoring, extraction and analysis of obtainable data from the devices and instruments, assessment of the potential attack and vulnerability of the systems, and risk mitigation based on last intrusion attempts (Abdul-Ghani et al., 2018). Therefore, the responsibility of developing a SCADA security model to guarantee protection against vulnerability and potential attack by malicious intruders is crucial (Ismail et al., 2014b).

A component of the framework consisted of vulnerability assessment, which identifies security weakness and vulnerability of the system (Ismail et al., 2015). In doing this, organizations security practitioners can determine the security weaknesses of any embedded devices from primary to the advanced level in an attempt to ensure a secured system (Upadhyay et al., 2020). SCADA network vulnerabilities can be grouped by the loss of availability, integrity, and confidentiality, and lack of authentication (Gosh & Sampalli, 2019). In order to maintain within a competitive market, it is critical for organizations to modernize their SCADA network to reduce costs and increase efficiency (Igure et al., 2006). A company conducted a risk assessment for the identification, quantification, and prioritization of risks in the lenses of risk acceptance and organizational relevant objectives in firms using SCADA systems. The risk assessment results determined the corrective and appropriate actions security personnel need to take in managing information security risks by identifying the best security control (Ismail et al., 2014b).

In the risk assessment, the key areas of interest included communication and consultation of SCADA systems, establishment of framework and context, identification of associated risks, analysis and treatment of risks, and monitoring and reviewing of SCADA systems (Ismail et al., 2014b). Eight levels of knowing the identity of the cyber-attacker were designed included advanced information and computer technology (ICT) skills, political motivation, required tools and techniques, assessment of advanced new ICT, advanced SCADA systems knowledge, capability of using internal knowledge and resources, reconnaissance ability, and sufficiency in financial ability to be able to attack SCADA networks or systems (Begs & Warren, 2008). Last, SCADA security controls that included organizational information policy, security policy, environmental and physical security, personnel security, access control, operations and communications management, acquisition of information systems, maintenance and development, SCADA compliance, and the management of SCADA business continuity, were adopted (Ismail et al., 2014b).

Principally, scientist categorized the security controls into three groups: operational, management, and technical controls. All of these have their origin in IST. Yang et al. (2016) adopted the same approach of using IST in developing other frameworks for the purposes of information security management. Accordingly, information security management is essential about drawing the plan for achieving information security necessitating the incorporation of various practical standards and theoretical methodologies into the domain. According to Ismail et al. (2015), though there are many methodologies and standards, majority of them prove to be cumbersome in their adoption by organizations in addition to lack of uniformity to handle systematically the information security management tedious tasks.

In addressing this gap, an integrated system for information security management (ISISM) illustrates the aim of employing the usage of existing methodologies and standards in solving the challenges inherent in them (Yang et al., 2016). The ISISM was targeted to address security issues within the business risk and impact analysis, whereby the security engineering adopted would enable the system to support users in producing risk assessment documentations with relevant polices on information security. Finally, Järveläinen (2012) used IST and theory of business continuity in designing a framework in relation to information systems security by underlining the significance of security components integration within a firm in ensuring that business continuity and information security are effective in the context of inter-organizational IT relationships. Järveläinen (2012) explored the organizational practices that information security and technology leaders used when executing technology solutions for the procurement of products and services. Furthermore, he found that large companies tend to outsource which slows down IT services and has an effect on business continuity (Järveläinen, 2012).

IST application has been useful in other studies. Such studies use the theory in the assessment of information security implementation as well as overall integration of components with the aim of addressing entire organizational security issues (Yang et al., 2016). IST examines management strategies' effectiveness in areas lacking information security management. For instance, IST was used in Malaysian public service organizations' information security architecture in evaluating the maturity level of information security with the aim of providing clear thoughtful information security analysis. Using a sample size of 970 respondents (individual) via self-administered surveys, based on information security landscape, incidents' occurrence, technical safeguard types, and sources of attack, the findings revealed that the high-leveled security incidents by Malaysian public service organizations included spamming (42%) and malicious codes attack (41%). Moreover, 25% of the incidences were from within the organizations, 15% from external sources, and 11% from a combination of internal and external environments, while the remaining 49% were unknown to the study participants (Dzazali et al., 2009).

The most used safeguards in addressing information insecurity were firewalls (95%), anti-virus (92%), and information systems access control (89%). Last, the maturity level indicated that 61% of the study participants were at Level 3 followed by Level 2 (21%), who believed that processes of information security were still regarded to be in the ICT domain (Dzazali et al., 2009). Last, Hong et al. (2006) examined the improvement of Taiwan's information security because of using IST. From the example provided above, IST is the best model of framework for security awareness based on key indicators of measurement both in the public, aerospace and defense contractor organizations.

Opportunities and Challenges for Cloud Computing

Various organization will not commit to using cloud storage because of the security, privacy, and trust issues with subscribers and consumers (Jawad, 2018). The reason for such is attributable to certain loopholes in the cloud's architecture that make it susceptible to various privacy and security threats. There are a number of issues that either present cloud computing as an opportunity to be exploited by organizations in data storage or a challenge to an organization (Ismail et al., 2015).

Privacy and security. The underlying factor, which defines the success of any infrastructure, is the security level it provides to the customer (Ouedraogo et al., 2015). The majority of IT firms believe that the lack of information privacy and security readiness is one of the major reasons for the hesitation of organizations to migrate to the cloud (Bhatia & Malhotra, 2018). Cloud service providers believe organizations should sufficiently protect their servers and the data stored in them from any sort of invasion and theft (Bhadauria et al., 2012). Organizations or individuals can assess the status of personal computer and/or hard drives in a straightforward manner. However, cloud servers can exist anywhere in the world, and any form of Internet disruption can easily deny access to stored data in the cloud (Allen et al., 2014). The providers of cloud service argue that their servers and the stored data are sufficiently secure from any form of theft and invasion. Additionally, such organizations insist that data storage in their servers is intrinsically more secure than the stored information residing in various personal computers as well as laptops.

Privacy and security shapes sections of the cloud architecture. In many cases, there are instances of insecurity and slow systems due to such activities (Allen et al., 2014). In 2013, half of security breaches occurred exposing the fundamental limitations of main cloud service providers' (SP) security model. Within the environment of cloud computing, privacy refers to an entity having control over what information is stored or revealed in the cloud and the entity has the ability to control who can access certain information (Bhadauria & Sanyal, 2012). As such, information on privacy and the various challenges to privacy require leaders to put particular steps into place to assure cloud privacy.

There are various daunting security concerns in comparison to private cloud because a public computing cloud encompasses a plethora of virtual machines, supporting middleware, and machine monitors among others. Consequently, cloud security is dependent on these objects' behaviors and the interactions happening between them. In addition, the public cloud enables the sharing by multi-tenants, and the number of users is directly proportional to the diversity and intensity of security concerns (Bhadauria et al., 2014). In a multi-tenant environment, providers must account for issues such as access policies, application deployment, and data protection (Tianfield, 2012). Therefore, by avoiding unauthorized access putting measures and mechanisms in place, organizations can achieve greater confidence in data integrity and protection (Sun et al., 2014).

There is a preference in favor of private clouds because public clouds are part of multifarious security concerns, which is a threat to the stored data. Because cloud computing assumes a major proportion of data storage, a mashup center can integrate multi-cloud servers and deliver a new service (Yang et al., 2013). By definition, a mashup is an application with the capability of combining functionality or data from various web sources and creating new services (Bhadauria et al., 2014). The usage of such applications, as technology evolves, targets the intensity and diversity of security challenges. Premised on mashup solution, the development of multiple security architectures involving a secure constituent model, which is capable of addressing security framework based on entropy for cloud-configured services suffices.

Data privacy. Big data is a new phenomenon where large volumes of data is generated by end hosts even though the data brings additional security challenges in terms of privacy and security associated with cloud computing (Lu, 2014; Dincer & Zeydan, 2017). When migrated into the cloud, data becomes transparent and stored by service participants; however, once stored, the user loses control of personal data, which may easily lead to a disclosure of private data (Ke et al., 2017). Camron and Marcum (2019) believed all important information that is shared and stored becomes vulnerable to cyberattacks, system infiltration and shutdowns, and hacker demands. Therefore, IT needs to be mindful about protecting user's personal information to ensure privacy and security.

Due to recent technological advances, the quantity of data produced by the Internet, social networking sites, sensor networks, healthcare applications, and other companies continue to increase every day (Jain et al., 2016). Generating large amounts of data on a daily basis causes a higher risk of compromise. If leaders cannot ensure privacy of dat within the cloud systems, users will refuse to utilize these beneficial systems (Sajid & Abbas, 2016). The primary factors in gaining a user's trust and making the cloud successful is the privacy and security of data (Sun et al., 2014).

In the cloud computing environment, data privacy becomes particularly serious because data is spread around different machines and storage devices such as servers, PCs, and various mobile devices (Sun et al., 2014). Information security policies shall play a role within an organizations practice. Policies should be in place to ensure user confidentiality. The compromising of data can be exceptionally destructive as users' personal information can be disclosed (Jain et al., 2016).

Data privacy contributes to the achievement of cloud computing; however, it could also be the most challenging issue (Chidambaram et al., 2016). Majority of the time, users immediately move their information over into the cloud without thinking about security. The cloud tends to become an issue to users when a breach of information becomes present. Today, more and more people worry about personal data breaches and businesses often acknowledge the importance of transferring confidential data in the cloud without understanding the correct security controls put in place (Ngnie et al., 2017). Due to the multi-tenant nature of cloud computing, organizations must put controls in place to compensate for the additional security risks inherent to the commingling of data (Singh & Singh, 2017). All these can become factors that help network administrators manage the data in the cloud more effectively. Users' data stored in the cloud are sensitive and private; and organizations could apply access control mechanisms to ensure only authorized users can have access to their data (Ouahman, 2014). Therefore, it is important to make sure authorized users only have the proper control of sensitive data.

Latency, Reliability, and Performance Predictability

Latency has been a matter of significant concern in cloud computing, in which data flows through different clouds. The primary drawback of cloud computing is the latency induced into the intercommunication between an Internet of things (IoT) device and the cloud (Moysiadis et al., 2018). Additional factors that contribute to latency are data encryption and decryption, which are helpful when data circulates around unreliable public networks with characteristics such as congestion, windowing and packet loss (Bhadauria et al., 2014). Congestion contributes to latency when the flow of traffic via the network is high and, thus, may generate many requests necessitating execution. Consequently, windowing, as a message conveyance technique, adds to the prevailing latency because the receiver has to send back the message to the sender. Indeed, the latency plays a key in determining the performance of a cloud. Occasionally, the cloud system is devoid of capacity by either permitting access to virtual machines or achieving the thresholds of upper throughput on the Internet links due to the high demand emanating from clients (Eloff & Solms, 2000). This, in truth, affects the network performance of the cloud.

Interoperability and Portability

Interoperability within the cloud refers to the ease of migration and integration of applications or data among different cloud providers (Kaur et al., 2017). Organizations that experience security breaches may opt to change the cloud service provider and seek the services of another one; however, there are cases where this is a project in futility as impossibilities make it difficult to move data and applications from the existing one (Bhadauria et al., 2014). In this instance, companies refers to this phenomenon as *Lock-in*. *Lock-in* refers to the difficulty in joining data and applications from one cloud platform to another (Silva et al., 2013). More often, this phenomenon associates with risks, which have a high likelihood of breaking the whole system, and importantly, lock-in is dependent on the type of cloud in use. For instance, SaaS application may be challenging when the format of the migrated data is not congruent to the destination specification (Eloff & Solms, 2014). Organizations should apply SaaS when applicable

Additional steps are necessary like data back up and execution of regular data extraction in conformity to SaaS usable format. Generally, PaaS lock-in normally occurs in instances whereby the language of use while developing the application is not in conformity to the platform of migration (Eloff & Solms, 2014). To remedy the situation, elimination of PaaS lock-in is possible by carrying out the following procedures: first, understanding cloud offering, which supports a standard syntax and open architecture; second, understanding the components of the application as well as modules particular to the providers of PaaS and performing primary services like logging and monitoring; and last, understanding the control functions, which are specific to the public cloud providers and their colleagues in an open forum (Bhadauria & Sanyal, 2012). PaaS data security should be securitized as information becomes stored.

Data Breach in Fiber Optic Networks

Security risks for information in transit are a matter of serious concern. The transitioning of data is rampant in today's ICT environment, including multiple data centers as well as deployment models of private and public clouds (Panah et al., 2014; Bhadauria et al., 2012). The transitioning of data from one center to another raises concerns in relation to breaching within the cloud. In most cases, data transfer is done through fiber-optic cables, which are no longer safe from attacks (Bhadauria et al., 2014). There are special devices that have the capability of tapping data while in the flowing process with minimal disturbances if any. While fiber-optic cables run through the underground, it becomes very difficult to change any anomaly, hence, a need to assure maximum data security to such tensioning networks.

Optical networks can become vulnerable to different types of security breaches or attacks, which may disrupt service or allow unauthorized access of data . Within the fiber optic network, a breach can induce financial losses against clients and cause service disruptions (Furdek et al., 2014). Vulnerability to breaches can also include jamming, physical infrastructure attacks, interception, and eavesdropping (Fok et al., 2011). Although it can be impossible to protect networks from breaches, organizations should consider placing robust encryptions in place to protect data.

Storage of Data over Internet Protocol Networks

Data storage online is becoming the norm and will require data security mechanisms, which can prevent leakage and loss of user information (Rejin & Paul, 2019). Virtually all enterprises will be maintaining big data chunks without establishing the requisite architecture. There are quite a number of benefits to online data storage; however, threats to security that can cause data unavailability or data leakage exist (Eloff & Solms, 2014). These instances manifest on a frequent basis when dealing with dynamic data, which has a tendency of flowing in the cloud as compared to static data. Depending on various operational levels and provision of storage, the networked devices in close proximity with the dynamic data fall into network-attached storage (NAS) and storage area network (SAN), which are operational in different servers (Bhadauria & Sanyal, 2012). Thus, they are prone to multiple security threats. Besides cloud computing, mobile cloud computing can have more challenges.

With the evolution of the Internet, data accessibility by nonauthorized agents with malicious intentions becomes one of the challenges for network accessibility. Because the invention of non-continuous and non-consistent wireless network, data latency is more robust (Bhadauria & Sanyal, 2012). Consequently, such inconsistency is responsible for longer time interludes for data transfer, hence, causing traffic among the components of intermediate network (Eloff & Solms, 2014). Moreover, dynamic scalability and network monitoring that is typical of mobile cloud computing may result in challenges with non-compatibility when migrating data from one device to another, which also increases the chances of attack by criminals. Security challenges are of high magnitude as compared to the normal cloud computing.

Attacks in the Cloud Environment

Attackers of the cloud environment can be internal or external (Sun et al, 2014). These attackers make the cloud vulnerable as confidential and sensitive data becomes exposed without permission. An internal attacker can be a current or former employee, contactor, or any other business associate with the mandate to access the network system or data of an organization, abusing the privilege by engaging in malicious acts. According to Yusop and Abawajy (2014), an insider is a person who is or was a trusted employee of an organization and who formerly or currently has knowledge and the opportunity to oversee network systems in an organization, abuses the responsibility bestowed upon him/her to access and interfere with confidentiality, integrity, or availability of the data in a negative manner. Alternatively, insiders can violate the security policy by exerting legal access. In the sphere of cloud computing, insiders, to begin with, have the ability of inviting rogue administrators to the system. Rogue system administrators exploit cloud weaknesses leading to illegal access within an organization (Claycomb & Nicholl, 2014). Additionally, rogue system administrators utilizing cloud systems to carry out attacks on the local resources of an organization. The main intention of a rogue administrator is to render weak the cloud infrastructure with the intention of stealing sensitive data, and such attacks culminate into confidentiality and integrity loss of information/data.

The various groups of rogue administrators in relation to cloud computing include system, application, hosting firm, and virtual image administrators. Such an array of rogue administrators can carry out different attacks on the cloud system. For example, application administrators have the capability of targeting vulnerabilities existing within the drivers of virtual machines (Claycomb & Nicholl, 2014). Additionally, they can assume the control of the system whereby the cloud services' execution or they can exert malicious actions to the applications that host cloud services.

Within the cloud, administrators maintain certain activities and processes for the entire system (Lazarova, 2016). According to Mallaiah and Ramachandram (2014), systems administrators have the capability of executing attacks on conventional operations such as root compromises and Trojan horses. In the meantime, administrators of virtual image may copy machines or virtual disks, which in the process create alternating images that are not congruent with the established baseline in spite of reports indicating the contrary; they have the capability of also modifying virtual machine's individual cases in the cloud culminating into incorrect functioning of the cloud. Last, hosting firm administrators may create network taps on the systems by implementing engineering techniques in monitoring the software used in hosting (Fernandes et al., 2014).

Another category of inside attackers involves such individuals who capitalize on the cloud system's vulnerabilities in acquiring unauthorized access to the system/data of an organization. According to Claycomb and Nicholl (2014), attacks of this caliber are either malicious or intentional with access control or security polices variations between the cloud system and the client. The individual attacker gains access to the confidential and sensitive information fraudulently. The final insider in terms of threat provision to cloud information is the attacker who utilizes the cloud information by assuming control of a user's computer to execute nefarious activities around the world (Becking, 2016). Accordingly, the insider uses cloud services like email and file sharing to steal data.

These insiders use their legalized access in violating the security policy. Additionally, the insiders overpass their boundaries by sidestepping the policies related security and access control to the clouds. Such excessive privileges urge insiders to act without restraint; therefore, they do not uphold accountability and restriction.

The attack of insiders is more intense and vigorous in comparison to external hackers to the cloud system. Internal attackers pose more security threats because they can conveniently extract a user's data from the hard drive managed by the cloud storage (Lal et al, 2017). For example, inside attackers are immensely successful in their malicious activities becasue they are very familiar and conversant with the security control internally. Moreover, the organization configures security tools where the external threat is prioritized as compared to the internal one. In addition, insiders' activities are worse to the point of including deletion of vital data, tampering with very sensitive data, duplication of data, and illegal data extraction. Further, inside attackers actively engage in blackmail, sabotage, theft, fraud, and espionage, which may be costly to the organization concerning cloud system security (Nurse et al., 2014). In general, the attack of the cloud system from within presents severe security challenges to IT security managers or system administrators, and their diligence can play a critical role in effectively securing the cloud against unwarranted breaches.

The external attackers have limited access to the cloud system to manipulate data; they are dependent on internal security mistakes to make the cloud vulnerable to attack (Camron & Marcum, 2019). In summary, both internal and external attacks to the cloud system are detrimental to data integrity and confidentiality. Against this backdrop, ISTISM framework argues in favor of security policy, risk management, internal control, and contingency management to effectively achieve organizational information security goals and assure a secure cloud (Garg & Goel, 2017).

Effective Strategies to Control Security Breach in the Cloud

There are three categories of strategies used in preventing cloud breaches, and they include informal, formal, and technical strategies. Organizations regard such strategies as security mechanisms having the capability of addressing the challenges inherent in the complex nature of the cloud system. Informal strategies offer education on data security, and the concerns towards the development of organizational security culture and environment (Toma & Leuca, 2018). Formal strategies are geared toward necessitating compliance to information security related processes, procedures and regulations (Granneman, 2018). Last, technical controls are in place to prevent unauthorized access management. These strategies are only useful when a guardian is available to implement such controls.

Guardians play a key role in the cloud security process. An organization often refer to guardians as individuals mandated with the responsibility of preventing crimes (Weisburd, Groff, & Yang, 2014). These individuals are capable of preventing crime because they have the ability of maintaining vigilance and implementing necessary interventions to eliminate potential offenders. The unavailability of able guardians, possible offenders, and appropriate targets may culminate into predatory breaches (Pyrooz et al., 2015). These aspects lead to crime commissioning due to the possibility of spatial or temporary converging that provides opportunities for criminal activities.

Information security leaders can regroup the various strategies into the aspects of the conceptual framework including security policy, risk management, internal control, and contingency management.

Security Policy

Formal strategies form part of the security policy. Besides, such strategies ensure regulation and compliance to policies on information security. There are three categories of strategies: informal, formal, and technical. Ambre and Shekokar (2015) argued that organizations ought to consistently communicate and enforce policies regarding information security in an attempt to make employees understand the ways of preventing the outside or inside attacks. There should be clear, specific policies, which an organization can effectively recognize, analyze, and respond to an incident, will affect the damage and lower recovery costs (Ruefle et al., 2014). Additionally, security policies must highlight the consequences for neglecting the expected standards. Extensive service-level agreements between the cloud-service provider and customer should provide direction on how to deal with risks associated with information security by both the insider and outsider threat.

The security policy ought to demarcate the monitoring capabilities, the supervision of employees' activities, and determination of the restriction levels of accessing the sensitive data of the client in the cloud. According to Soomro et al. (2016), agreements are vital in guaranteeing that the providers of cloud service either meet or exceed the requisite standards for information security management. In addition, incident reporting policies and procedures are necessary, as these would enable workers to report any unscrupulous activity by rogue colleagues. Incident-reporting undertaking is capable of addressing committed episodes by either outsiders or insiders through an escalation chain (Ruefle et al., 2014). Such is only possible when relevant authorities are in place to make critical decisions on security-based problems. To this end, either an insider or outsider provides an outline on the right mechanism for reporting attacks, which in the process provides IT managers with many opportunities to initiate the recommended remedies.

Risk Management

Several legal frameworks can be used in implementing the security policy in an organization. To begin with, leaders should first pursue enterprise then governance risk management. Governance is concerned with the supervision and control of the operational and procedural activities involved in cloud services. According to Villaronga and Millard (2019), issues like regulatory issues, legal concerns, monitoring and service testing, applications' development standards, policies, and procedures are key for governing the cloud system. Consequently, the cloud needs an examination of policies, legal issues, ethical and security challenges (Soomro et al., 2016). Information security leaders must identify and handle threats to address sensitive and confidential data protection, cloud-service provider's transparency, and service-level agreement breaches.

Organizations, indeed, must have the ability to govern, measure, and manage enterprise risks, which are part of the information in the cloud. To this effect, organizations should ensure and guarantee sensible data security through the supply chain, which encompasses cloud service providers, clients, and third-party sellers (Liu et al., 2015). Procedures of data security governance, consists of management commitment and leadership, organizational structures processes, technologies and compliance mechanisms that work together to ensure the confidentiality, integrity, and availability of an organizations assets (Solms, 2005; Liu et al., 2015).

The second approach to ensure security policy is data regulation and compliance management. Arguably, conforming to legal issues, especially those related to information within the cloud, is quite challenging. Thus, cloud service providers ought to evaluate requirements to compliance emanating from the service deployment because cloud computing is ubiquitous and has various service models. According to Elifoglu et al. (2014), legal and regulatory trajectory introduced by cloud service providers varies in terms of cloud service location. Hence, clients have a bearing on different operational functions inclusive of security and privacy responsibility, data lifecycle management, electronic discovery, and violation of client's data security and privacy. The providers of cloud service must be accustomed to complying with laws and regulations that assure protection of confidential and sensitive data of clients (Sookhak et al., 2015). Additionally, cloud providers should carry out both internal and external security audits in an attempt to ensure that information security risk management is apparent.

In the United States, major states are equipped with established data breach statutes that make it mandatory for organizations to provide notification to customers in the event security breaches happen. These laws or statutes facilitate sensitive data identification with the aim of preventing identity theft (Smith, 2016). Moreover, such regulations are important as they protect clients from harmful practices and data breaches because businesses or cloud service providers should utilize appropriate security mechanisms. Organizations that fail to comply with privacy laws on security breach have a high likelihood of facing legal risks to the point of facing criminal penalties as well as civil proceedings (Elifoglu et al., 2014). Subsequently, tort laws, provide further information security protection by compensating consumers or clients in the event an organization is involved in sensitive data misuse.

There is an uncertainty on the application of tort laws for organizational failure in an attempt to secure the client's confidential data (Congressional Research Service, 2019). To this end, a portion of consumers resorts to civil proceedings in dealing with organizations or service providers of cloud that fail to offer protection for their personal data (King & Raja, 2012). Majority of people regard tort laws as ineffective in protecting sensitive data because economic harm is difficult to prove.

Businesses using cloud services have to ensure that their clients are "armed" with remedies pegged on consumer protection laws. For example, Lee et al. (2016) hints that a company may be guilty of violating the Federal Trade Commission Act through failure to protect stored personal data from illegitimate or unauthorized access or from accidental access, processing, erasure, loss or use while in the cloud, hence, enabling unauthorized access by unscrupulous agents. Consumer data is a foundation on which firms build their business models and may potentially become unable to embrace appropriate security policy on information in protecting sensitive data (Bleier et al., 2020). The consumer can then be justified in holding the cloud service provider responsible and bringing the issue to the hearing of the Federal Trade Commission, purposely for the agency to enforce action against the organization as guided by relevant laws and regulations. In addition, there is inadequate comprehensive legislation related to consumer sensitive data protection in the cloud sphere; therefore, cloud service providers have the opportunity to decide on the architecture of privacy protection.

In the absence of an all-inclusive regulatory establishment for cloud computing in most countries, primarily the developing nations, service providers have a high likelihood of developing low data security boundaries. In addition, they have the tendency of manipulating the service-level agreements with the purpose of leveraging the legal burden if they fail to offer adequate security to the client's confidential information (Bacon et al., 2014). A typical example is when the service-level agreements fail to put under consideration mechanisms set aside to deal with inside security threats as they only focused on the outsiders. Thus, security policy gives a guideline that the clients of cloud service providers must be cognizant of the binding service-level agreements in the context of being comprehensive enough to ensure maximum security to their personal data and the legal responsibilities (Wheatley, 2014).

Internal Control

In information security management, incident response is mandatory, as it is the underlying factor within the cloud system. The incident management as an internal control process functions well when tools, programs, and processes of the cloud system are intact. In the event of a threat to security management of information, guardians have the responsibility of undertaking suitable actions in discovering the circumstances that culminated into the unfortunate tragedy. As a result, contributions to cloud forensics can be models, systems, frameworks, and solutions relating to the security incident that triggers the forensic investigation (Manral et al., 2019). The cloud systems robust forensic architectures ought to be capable of performing verification of security incidents, analysis of the attack (either internal or external), and restoration of secure service (Kalloniatis et al., 2014). As such, it is imperative that an effective response framework remains in place for efficient detection and rejoinder to incidents of security threats to personal information.

Technical strategies are available for a robust and effective incident response. Such technical strategies amicably deal with matters related to information access management. Various preventive technical control measures are available for incident response. Key and encryption management includes the significance of encrypting data with the aim of minimizing possible data breach in the cloud system. According to Renwick and Martin (2017), encrypting data ensures no meaningful information becomes leaked or compromised in an event of a compromise. Data encryption is necessary in environments encompassing various people. Accordingly, the multi-tenancy nature of the cloud system requires data encryption so a myriad of users involved in the process do not interfere with the stored data in the case of a serious threat to security (Wheeler & Winburn, 2015). Therefore, IT professionals have diversified the data encryption process to ensure information security management.

A technique such as private information retrieval, a process that hides performed queries from un-authorized agents, ensures data security in the clouds. Although this technique is costly in relation to computation cost, it is effective in preventing failure of data processing support in the encrypted platform (Riad & Ke, 2018). Additionally, role-based access control is also effective in facilitating superior technical stratagem as far as data security is concerned. Fun and Samsudin (2016) suggests homomorphic encryption, a solution with the capability of securing confidential data within the cloud system, while allowing corresponding third parties to perform computation on encrypted data without having to decrypt.

In order for encryption to meet the intended purpose, a privacy manager plays an integral part in the process. A privacy manager operates in the capacity of a data encryption processing security mechanism by serving as the first line of defense by helping the user manage the privacy of their data within the cloud (Pearson et al., 2009). In this vein, the privacy manager has to use obfuscation methods in reducing the sensitive personal data stored in the cloud while minimizing data leakage as much as possible. The principle behind this data shrinkage is to store the client's data in an encrypted form. However, privacy managers must take care and be willing to execute this activity with utmost carefulness to secure sensitive information. Moreover, the architecture operates with a proposed protocol based on trust and encryption concepts to ensure cloud data integrity without compromising confidentiality and without overloading storage services (Pinheiro et al., 2018).

Healthcare providers will be implementing privacy methods by successfully shifting their client's confidential data to a commercial cloud service provider with no security threats. The healthcare organizations believes they must implement security measures and approaches such as encryption standards in order to protect the privacy and confidentiality of customer's data over the cloud (Abouelmehdi et al., 2018). Similarly, Kazim and Ying (2015) contended by stating that techniques of encryption preserve data format and context of data utilization within the cloud environment. Nevertheless, the key management is a challenging process given the multi-tenancy nature of the cloud environment and it resources (Kalloniatis et al., 2014).

Contingency Management

Information security management forms the core of contingency management. In the cloud environment, data is vital when it comes to security and consequential protection within the multi-tenancy platform. Information protection is possible by safeguarding virtual and physical networks, data backup, data cryptography, and data integrity and segregation (Kalloniatis et al., 2014). Personnel involved in IT security management must take into consideration robust sanitization, cryptography, hardware suitable maintenance, and effective methods of computation while managing the cloud data life cycle. Such an approach is sufficient in dealing with various threats to information security involving data breaches by insiders and through insecure interfaces. A domain pinpoints the information management relevance within the cloud through processes such as storing, creating, sharing, using, destroying and archiving of information. Roy et al. (2015) stated the cloud is used as a data storage, hence leading to threats of data leakage and confidentiality and integrity threats to data. Therefore, it important for access to be controlled.

Another aspect of contingency management in dealing with data breaches in the cloud is the entitlement, identity, and access to information management. Entitlement, identity, and access management of consumer personal data enable information security leaders to incorporate relevant technical strategies. In the cloud system, identity management transformation includes entitlement in the information managing access process (Kalloniatis et al., 2014). Kazim and Ying (2015) give a suggestion of cloud services and applications that use various sources to identify users as the entitlement management to provide a decision process in authorizing access to the data, system and processes of the cloud. Such emphasis on types of identity is necessary for cloud environment inclusive of agents, code, organization, users, and device. The two most significant elements used in ascertaining identity types are the attributes' strengths and the expected identity that provides higher flexibility in the cloud system (Brandas et al., 2015). Most importantly, the access to data entails many things such as the application, process, network, and system facets. In this regard, the entitlement process should ensure that links exist between the needs of the business and those of the user's security based on governing rules to access different cloud entities.

The business continuity, conventional security, and disaster recovery are also components of the contingency management. Cloud computing offers infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, as well as threaten business continuity and corporate reputation (Arianyan et al., 2016). For the continuity to thrive, a requirement that appropriate safety measures crucial in the management of security risks, and assuring information integrity, availability, and confidentiality, must be available. Kazim and Ying (2015) conformed to this line of thought and argue that cloud services have to be persistently available to clients, and in the event of an interruption, the service provider of the cloud must put in place a vigorous recovery system ensuring that normal business undertakings are continuous.

Service availability is very significant, and the breakdown in cloud service provision may lead to closure of businesses owned by the cloud users (clients). Breakdown of such caliber results from either a failure or attack in the cloud hardware (Roy et al., 2015). Consequently, data backup and disaster recovery are helps support data protection and transition reliability (Kazim & Ying, 2015). Hence, entire virtualization of data scalability in terms of file systems and recovery applications as well as data storage becomes useful for business continuity in using cloud and disaster recovery.

Contingency management is tending to be more of an informal strategy than a formal strategy. Informal strategies primarily focus on information provision. The strategies offer education on information security in creating an organizational security culture. On this basis, managers have a responsibility to make sure employees are aware of the possibilities of technology vulnerability by offering their employees training on how to keep their intellectual property and company information protected throughout the use of cloud computing (Kahle-Piasecki et al., 2017). Indeed, awareness of threats that put information security in jeopardy by employees makes it easy for them to identify suspects with suspicious behaviors amongst them, hence, helping in thwarting the plans by internal attackers. Further, subjecting employees to training creates vigilant workers in the firm, and this plays a key role in reinforcing opposition against insider and outsider unscrupulous activities. Training programs may lead to an establishment of an organizational security culture that is inhibitory to security threats to sensitive information of clients (Ruefle et al., 2014).

Information security management, in most organizations, has viewed data security from a technical point of view (Bernsmed et al., 2014); however, the crux of the matter is that the implementation of data/information security with success is more of a management concern than a technical issue (Dzazali, 2009). Individuals are very critical in managing successful implementation of security. The reason being that security is part of everyone's activities on a daily basis from the lowest worker to the senior managers in an organization (Kazim & Ying, 2015). Information security, for majority of people, is not an intuitive or obvious process; training programs and awareness, when established in an organization, are cultivated into an organizational security culture (Ruefle et al., 2014). People may possess direct access to personal information of others without restraint; however, guidelines, polices, procedures, and controls have been demarcated in guiding the behavior of accessing other people's data without their knowledge and authority.

The cloud service security strategy should be able to segregate data from various users. Malicious agents are opportunities and maximize on application vulnerabilities with the intention of developing parameters that are capable of bypassing security checks and ultimately grant authorization to user's data without permission (Hemalatha, Jenis, Cecil, & Arockiam, 2014). Due to this, security managers get an opportunity to validate and test data segregation within the cloud system using techniques such as structured query language (SQL) injection, data validation, and insecure storage (Zineddine, 2015). Additionally, these tests may identify vulnerabilities, which grant attackers the opportunity of accessing personal information with no authorization whatsoever. For example, Chang et al. (2016) demonstrated how security has become a highly important attribute based on the development of online-based applications such as Google products and Google Docs, which could potentially expose personal data to other users due to session allocation flaws.

Data segregation is useful in eradicating a security problem resulting from session allocation flaws, and this is possible with proper functioning data centers. Various strategies like assessment of operational procedures of cloud service provider, data center architecture, and security strategies dissemination are vital for successful functioning of data centers (Kalloniatis et al., 2014). A data center is vital for cloud system operations because it holds the applications required in the cloud environment. Therefore, clients are in dire need of continuous and lasting stability data centers for continuous cloud system services provision. Service management, security standards, regulatory requirements, and location of the data center are important considerations when it comes to their intended operations (Tankard, 2015).

Data confidentiality in the cloud needs user authentication. Electronic authentication is a determinant of electronic user identity authentication as presented in the data/information system. Privacy breaches happen when electronic authentication is missing culminating into an unauthorized user account access (Dawson, 2015). Moreover, the security of the cloud system encompasses software confidentiality that relates to the notion that certain processes as well as applications must handle and maintain the sensitive information of the client. Consequently, within the cloud environment, clients deem the applications of the cloud system are effective in protecting their personal information as agreed. Hence, an organization must certify the applications that are in contact with the client's confidential information to avoid further risks associated with confidentiality and privacy (Elhaida & Frueh, 2015). In the end, unauthorized access to client's sensitive information by malicious users with the sole purpose of exploiting the software vulnerabilities becomes curtailed.

Potential directions can be pursued in preventing concerns related to data control and in the long run, establish various auditing categories in the cloud system. From the onset, there is a need for a monitoring system that can be trusted within the server of cloud, and this mechanism ought to facilitate the server's actions auditing while providing verifiable security-auditing conformance proof to the customer. Additionally, cloud service providers should have their data stored in the clouds, self-protected within a secure and safe environment (Hong & Rong, 2014). In line with this, Lin et al. (2014) proposed a policy that the security auditing ought to be done at the virtual cloud environment's software level with the systems in place offering monitoring of events and logs within the server as the bare minimum.

Summary

The ISTIM model, as shown in the discourse above, has presented every element involved in security breach in the cloud. From the one end, the model has discussed the inherent factors within the cloud system that lead to security threats, either internally or externally to the client's sensitive data (Ismail et al., 2015). Such concerns include privacy and security issues, latency, reliability, performance predictability, interoperability and portability, data breach within the fiber optic networks, data storage over IP networks, and attacks in the cloud environment by either insiders or outsiders (Ismail et al., 2014a). An organization has a mandate to fulfil their information security goals in light of these challenges inherent in the cloud system, effective strategies is necessary with the aim of securing the sensitive data of their clients.

The first strategy as adopted from IST is the security policy, in which an organization sets rules and regulations in tandem with the existing legal frameworks in a country to deal with both internal and external security threats and ways of compensating clients in the case of data manipulation (Ismail et al., 2014b). The second strategy entails the internal control. Internal controls ensure a secure cloud system for the client's confidential information (Ismail et al., 2014a). The third strategy is contingency management that largely consists of informal strategies, whereby organizations train and educate their employees to effectively deal with the client's personal information. The last strategy is risk management, which involves governance and enterprise risk management in dealing with inherent cloud environment's data security threats.

Transition

In Section 1, I highlighted the need for information security leaders to implement best practices when developing strategies and policies that protect and address data security concerns within the cloud environment. Additionally, I included a discussion of the background of the study, the problem and purpose statements, the nature of the study, assumptions, limitations, delimitations, the research question, conceptual framework, and a definition of key terms and review of the literature. In the literature review, I summarized the importance of internal controls that involve security standards, security awareness, current information security laws and regulations, contingency management, breaches and risk management.

Section 2 will include an overview of the research project, including restatement of the purpose statement and discussion of the role of the researcher, participants, the research method and design, population and sampling, ethical research, data collection instruments and techniques, data organization techniques, data analysis, and the reliability and validity of the study. Section 3 will include a presentation of (a) study findings, (b) implications for social change, (c) recommendations for action and future research, (d) a reflection of my experiences conducting this study, and (e) my research conclusions.

Section 2: The Project

In this section, I present the overall goal of the study by providing specific details that will contribute to the findings of the proposed research plan. I go into further depth by discussing the different roles a researcher exhibits, various research methods, and design approaches as well as highlighting the importance of ethics within the doctoral study. Also included in this section is an explanation of the data analysis procedures chosen for this study. I also discuss the data collection techniques used for the design of the study and describe the steps that I performed to help ensure that research results and observations are scientifically thorough, valid, and dependable.

Purpose Statement

The purpose of this qualitative multiple case study was to explore successful strategies that some information security leaders in the aerospace and defense contractor industry used to protect cloud-based data from security breaches to improve organizational profitability. The population consisted of seven information security leaders within seven aerospace and defense contractor companies, two organizations in Washington, D.C., and four publicly available sources who have implemented successful strategies to protect their cloud-based data from security breaches to improve the profitability of their organizations. The implications for positive social change may include the potential for information security leaders to learn of strategies to prevent security breaches of personal data that were stored by commercial companies, which may benefit members of the public by helping them avoid the expenses, inconvenience, and disruptions that these breaches may cause.

Role of the Researcher

Some of the significant role’s researchers are required to fulfill include collecting, processing, and transcribing data. Yin (2017) observed that when conducting a qualitative study, a researcher might gather information from a variety of sources to include interviews, observations, documentation, and current records. For this qualitative multiple case study, I served as the primary data collection instrument. Cronin (2014) concluded a researcher’s responsibility within a case study is to design the study, develop interview questions, confirm participant responses, and eliminate personal bias from the study. My role in this qualitative multiple case study was to design the study, develop interview questions, choose the participants, collect the data, organize the data, and evaluate the data. Fusch and Ness (2015) noted that the researcher should take the necessary steps to mitigate any potential bias that could affect the information being collected. As the primary data collector, I asked open-ended interview questions and did not share my personal experience or give my personal insight on the topic to avoid influencing the participants in the study.

Concerning my past and present personal relationship with the subject, I did not work with the participants in this study nor do I work in the IT job industry. In 2015, I became a victim of the OPM breach of personally identifiable information (PII). My experience led me to becoming interested in the cloud environment, and my interest has continued to grow as more organizations are adopting the cloud service even though security issues remain common, which in turn prompted me to dive deeper. My experience did not have an effect on my study during the collection of data.

The Belmont Report was published in 1979 and includes discussion of three principles that are the foundations for the protection of human research subjects: respect for persons and their autonomy, beneficence, and justice (Gabriele, 2003). Respect for persons suggests individuals who participate in research studies remain autonomous and only participate in a study if they freely consent after being informed of all known risks and benefits. Beneficence allows participants to strive to maximize benefits and minimize risks and justice highlights fairness (Adams & Miles, 2013). In addition to the three principles, the report also outlines ethical guidelines, research principles, and considerations researchers should be aware of when conducting their studies (Lainie, 2006). I followed the guidelines and principles outlined within the Belmont Report. In addition, I received approval from the Walden University Institutional Review Board (IRB) before proceeding with data collection for my study.

The protection of participants in clinical trials or research studies is critical to the success of a study (Sims, 2010). Ethics, from the Greek word *ethos*, refers to a set of regulations or standards against which behaviors can be measured (Gabriele, 2003). Researchers may have the potential to influence factors within their study. In order to avoid unethical challenges, I conducted my research in a fair and trustworthy manner.

The primary data source was the interview process. Interviewing provides researchers with detailed data to better understand the participant's description and meaning of those experiences (Castillo-Montoya, 2016). While conducting interviews, I could have introduced potential biases. Researchers can introduce bias due to their personal experiences, personal values, and viewpoints during data analysis (Young, 2009). To avoid bias, I was open to new approaches and ideas when it came to the protection of information within the cloud. I made sure I appropriately transcribed and recorded all information provided in the interview and reduced bias by conducting the study in a neutral place to avoid other factors that could have an influence on the respondent's answers.

Additionally, I utilized an interview protocol (see Appendix A). Interviews provide researchers with rich and detailed qualitative data for understanding participants' experiences, description of their experiences, and the meaning they make of those experiences (Castillo-Montoya, 2016). A researcher's interview protocol is an instrument that consists of asking questions for specific information related to the aims of a study (Patton, 2015). The interview protocol helps the interviewer prepare for the interview by making sure the researcher knows what to ask overall and determine what information is important to obtain (Castillo-Montoya, 2016). I utilized an interview protocol to help make sure I did not forget key points, ensure I asked the right questions in the appropriate order, and to make sure I knew how to ask questions.

Participants

The participants in this study included seven information security leaders who have experience with security breaches of cloud-based data. I selected information security leaders who work at different companies within the aerospace and defense contractor industry in this multiple case study, which was centralized in the Washington, D.C., area, and included managers who have experience in hosting confidential/personal data in the cloud (Elo et al., 2014). Draper (2015) presupposed those individuals partaking in a research study should have some type of experience with the research topic. The eligibility criteria for the information security leaders are as follows: (a) experience developing and implementing security policies, protocols, and procedures; (b) familiarity with cloud security frameworks, principles, and functions; (c) familiarity with security controls relevant to compliance and regulatory requirements for cloud environments; and (d) experience migrating data to a cloud platform. The participants had a minimum of 5 years of work experience in the IT industry and have worked for their current employer for a minimum of 3 years while having a comprehensive understanding of cloud and cloud security (Wara & Singh, 2015). I expected the participants to provide information on how to protect data from a data breach within the cloud. The collection of data supported the guiding research question for this study and supported the conceptual framework of this study.

According to Cacari-Stone et al. (2014), participants will participate in a study if the research problem is relevant to their field of study and could result in helping implement effective policies and procedures within their organization. Before moving forward with the interviews, I established a rapport by contacting the eligible participants that I found on LinkedIn, emailed and had a phone conversation detailing the requirements of the study. I then contacted the participants through email to set-up a time that would accommodate each individual (Gioia et al., 2013). Researchers conducting interviews may experience challenges such as the participants being uncertain of their answers or failing to respond in a timely manner (Alshenqeet, 2014). To mitigate the possible challenges, I delivered each interview question with clarity to avoid misunderstanding, made sure all participants understood the research question, and made sure I obtained the necessary permission to record the interviews.

Additionally, some issues may arise while attempting to get the necessary participants and relying on them on to answer their phones, and showing up to follow up appointments (Alshenqeet, 2014). These participants will be responsible for either implementing, reinforcing, or reviewing current security incidents within their current organization (Wara & Singh, 2015). Hurmerinta and Nummela (2016) observed that participants might need assistance while conducting research. I conducted my research by specifying the purpose and the problem that led to my study, and I created questions that narrowed the purpose of my research.

A method of building a strong rapport with the participants is starting the interview with general conversation. Patton (2015) surmised that a general conversation with each participant could help ease nerves and establish comfort prior to the onset of the interview. Comfortability within an environment or with another individual (i.e., interviewer) can result in more in-depth responses (Yin, 2017). In addition to beginning the interview with general conversation, I conducted the interview in a comfortable and familiar environment such as a private conference room at a public library. Last, establishing a rapport by showing and displaying trust and respect through continuous open communication can create confidence (Holloway & Wheeler, 2013).

Research Method and Design

In a research study, there are three types of prominent methods: qualitative, quantitative, and mixed methods. The most appropriate research method and design for this study is a qualitative multiple case study to explore the strategies of information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches. In this section, I expand on both the research method and design I adopted for this study. Accordingly, I provide further explanation of why the other methods and designs were not suitable for the study.

Research Method

Researchers use the qualitative research method to explore the relationship between the research and the source of the research data (Pratt & Loizos, 2015). I chose the qualitative method to gain an in-depth and holistic understanding of the causes and effects of data breach within the Internet cloud. Researchers use the qualitative method to gain a better understanding through first-hand experience, truthful reporting, and quotations from conversations (Pandve, 2016). Flexibility during the interview process is the key to qualitative research, which adds an in-depth analysis from a small sample size (Young et al., 2017). Researchers look for patterns within the data rather than a statistical analysis claimed by quantitative method (Ranney et al., 2015). The use of qualitative research techniques such as open ended semistructured interviews with probing questions and observation provided a descriptive and elaborative rich data from each participants rather than than statistical data obtained from the simple questioning (Boz & Dagli, 2017).

Researchers using the quantitative method to apply statistical tests to draw conclusions about collected data to test a hypothesis or theory (Trafimow, 2014). This approach includes the gathering of statistical data (such as numbers) and focuses on variables, with the goal of generalizing and confirming research hypotheses and relationships (Hesse-biber, 2016). In quantitiave research a variable is a statistical term, meaning a quantity that can take on different possible values which is expressed in numbers to indicate amount, degree, quantity or magnitude of a variable (Onen, 2016). Therefore, I did not choose quantitative method because my objective is to gain insight into data breaches without quantifying any data.

While quantitative and qualitative research approaches each have their individual strengths and weaknesses, combining qualitative and quantitative approaches within a single study can yield results that have both breadth and depth in terms of rich meaning (Hesse-biber, 2016). A mixed method study includes a combination of both quantitative and qualitative approaches and methods either concurrently or sequentially, which is not suitable for this study (Hesse-biber, 2016). A researcher using the mixed method may find both contradictory and complementary conclusions from the quantitative and qualitative data collection method (Venkatesh et al., 2013). Morever, this approach leverages the complementary strengths and nonoverlapping weaknesses of qualitative and quantitative methods, and offer greater insights on a phenomenon that each of these methods individually cannot offer (Venkatesh et al., 2013). I did not choose the mixed method because my objective is to explore my area of interest and gain an in-depth understanding of data breaches within the Internet cloud.

Research Design

Researchers use a case study design to explore issues that apply to the real world, which requires the collection of data from multiple sources (Ridder, 2017). A case study can be useful when identifying features that can get lost in the data and those aspects may hold information needed for the situation. Focusing on small samples helps to direct the researchers' attention to the cross-level interactions and the deductive studies that sometimes are ignored (Creswell & Clark, 2011). Researchers conducting case studies typically explore all factors to provide an understanding of the event and situation. The purpose of a case study is to understand one situation or event being studied in great depth for a defined period of time while the researcher collects rich details through observations, interviews, documents, or past record (Pacho, 2015). The case study design is appropriate for this study because I will explore all factors and circumstances of the phenomenon and the characteristics of the individuals who are involved.

The narrative research design involves the description of the lives of individuals. This design focuses on collecting stories about the lives of people and provides a narrative of the individuals' experiences (Dwyer et al., 2017). The method may be used to explore the experience of a group and how the institutional, social, and cultural environment within the individuals' experiences influence and shape their practices within the world (Haydon et al., 2018). Additionally, the researchers gather individual stories from the participants through data collection methods such as interviews, memory boxes, letters, informal observations, conversations and journals among others (Leedy & Ormrod, 2015). I did not choose this design because my research is centered on the socioeconomic data breach within the Internet cloud and will not involve the exploration of people's lives.

Researchers use an ethnographic design to observe and interact with study participants in their real-life environment (Creswell & Poth, 2018). The major objective of this research design within a suitability project is to provide a further analysis into a design problem (Chan et al., 2018). This research design is most applicable when the researcher wants to have a better understanding of the experiences of the participants of the research (Leavy, 2017). I did not choose ethnographic design because I am not going to interact with the study's participants in their real-life environment. I am interested in obtaining relevant information from them; hence, understanding the participants' entire culture is of less importance to my study.

Phenomenological design is a form of study in which the researcher examines the lived experiences of the participants and attempt to discover the similarties with their shared experiences (Percy et al., 2015). The focus is on what and how the individuals experienced the phenomenon. Researchers using this design seek to collect data from a group of individuals who have all had the same experience and develop from those findings the essence of the phenomenon (Chan et al., 2018). In phenomenological research, the essence of a thing refers to exposing the implicit structure and meaning of the experience. The goal of phenomenological study is to explore a concept filled with social and cultural nuances and reduce those characteristics into one universal experience (Creswell & Poth, 2018). Because the data breach within the cloud is not a concept filled with cultural and social nuances, I did not choose the phenomenological design.

Population and Sampling

The population for this study consisted of seven information security leaders within seven aerospace and defense contractor companies located in Washington, D.C. A population consists of individuals who belong to the same group or live in the same geographical area (Malterud et al., 2016). A population should be fully defined so that those to be included are clearly identified (Banerjee & Chaudhury, 2010), and it will allow me to gather as much of information as possible with the least number of participants. Based on the defined eligibility criteria of the information security leaders, they must have the knowledge and experience with implementing strategies to minimize security breaches within the Internet cloud. The ideal sample size of participants in a case study research ranges anywhere from 3 to 10 participants (Duxbury, 2012). Therefore, I identified a targeted sample size of five information security leaders among the targeted organizations to be appropriate for this study.

The sampling method that I employed in this study was purposeful sampling. Purposeful sampling is a technique that involves identifying and selecting individuals or a group of individuals that are knowledgeable or experienced with the phenomenon of the study (Creswell & Clark, 2011; Palinkas et al., 2015). Furthermore, purposeful sampling is appropriate when it comes to case study research (Ishak & Bakar, 2014). Employing purposeful sampling enabled me to select participants with the knowledge of the research subject area (Benoot et al., 2016). Combining sampling strategies is appropriate and consistent with current developments within research (Palinkas et al., 2015). Therefore, I employed snowball and criterion sampling, which are considered different types of purposeful sampling strategies.

Snowball sampling is a referral method where individuals with specific characteristics recruit others from within their network or community (Valerio et.al, 2016). The use of snowball sampling allowed me to gain access to individuals and groups that may otherwise remain inaccessible (Woodley & Lockard, 2016). Once I observed the participants, I did not request their assistance in identifying people with the same knowledge. Snowball sampling can include participants nominating potential individuals with the same interest as the subject where they might be hard to locate (Siddiqui et al., 2016). Therefore, snowball sampling will be suitable for this study. A recruitment letter is provided in Appendix B.

Criterion sampling is another kind of purposeful sampling that entails preconceived criteria (Sandelowski, 2000). Criterion sampling involves the inclusion of a particular group of participants who meet some type of predetermined criterion of importance (Palinkas et al., 2015). This form of sampling allows the researcher to set criteria and pick all cases that meet those criteria (Patton, 1990). In criterion sampling, the researcher must select the criteria carefully in order to obtain detailed and rich data relevant to the particular research problem (Ormona, 2013). For example, my criteria for participants in this study included each participant having a minimum of 5 years of work experience within the IT industry and having worked for their current employer for a minimum of 3 years. Therefore, criterion sampling will be suitable for this study.

Data saturation is the point in data collection at which no new data is introduced within the interview process (Saunders et al., 2017). Failure to reach data saturation can affect the quality of the research conducted and hinders content validity (Fusch & Ness, 2015). Data saturation can be achieved through collecting data from multiple sources, which will include interviews and publicly available data. The publicly available data will focus on current policies and strategies on preventing data breaches, which in turn will verify no new themes emerging from the study (Guetterman, 2015). The researcher achieved data saturation by the third interview. Additionally, member checking with each participant verified data saturation was reached by clearing up any misrepresentation of the data.

I conducted a semistructured interview with each eligible participant at their location of choice that was free of distractions (Scheibe et al., 2015). When going through the interview process, the researcher obtained better results by choosing a quiet and comforting environment where it was easier for the participants to be open (Anyan, 2013). Additionally, I followed the interview protocol (see Appendix A) and included the same interview questions for all participants. Researchers can perform consistent interviews to reach data saturation (Archambault et al., 2015).

Ethical Research

Informed consent refers to the disclosure of pertinent details by the researcher to the participant (Chiumento et al., 2015). The disclosure should entail how the participant's information as well as the data collected through the study will be used. With this disclosure, the ethical responsibility of the researcher to the privacy of the participant has been fulfilled and it is in the hands of the participant to consent to these actions or decline to participate (Dranseika et al., 2017). This concept regarding the fulfillment of the ethical requirement through informed consent is analogous to the ideas presented by Cahana and Hurst (2015). Cahana and Hurst (2015) described informed consent as permissions to include participants' personal information and not to use this access to exploit all points along the way. This approach viewed informed consent as the first step in ethical protection of participants, not the singular, overarching solution.

During the initial meeting, I furnished each participant with a copy of an informed consent form (see Appendix C), interview questions, and my point of contact. The researcher designed the informed consent process to ensure the rights of all participants are not violated during the data collection process (Chiumento et al., 2015). The researcher must ensure that all participants are familiar with the process and that they understand the study is voluntary (Crockett et al., 2013). The consent form details (a) the purpose of the study, (b) procedures, (c) the researcher's role in the study, (d) statement of confidentiality, (e) withdrawing from the study, (f) description of incentives/compensation, (g) risks and benefits of being in the study, (h) contact information, and (i) consent. I required each participant to read and sign the consent form prior to being interviewed. Prior to member checking, each participant received a copy of the fully executed consent form.

At any time, the participants were able to withdraw from the study. I informed each participant that participation in this study is voluntary and that they may withdraw at any time with no consequences or penalties. Any participant planning to withdraw from the study should inform the point of contact at the earliest opportunity (Zang & Creswell, 2013). Prior to moving on within the form, I continued to express the importance of each participant's rights in withdrawing from the study. Furthermore, I informed each participant that there would be no incentives offered before, during, or after the study. Researchers who offer incentives risk the chance of having adverse effects on the data (Robinson, 2014). Instead, I continued to encourage voluntary participation, and I informed each participant that their involvement in the study could benefit other security managers in protecting their data from breaches within the cloud (Crockett et al., 2013).

To assure that the ethical protection of participants was adequate, I followed all legal and ethical requirements established by Walden University in conjunction with the Belmont Report. The identities and organizations of participants of a study should remain confidential (Cooper et al., 2016). Insurance of anonymity and personal data protection is of paramount importance to those who volunteer for studies in today's information age. Lohle and Terrell (2014) detailed different methods to protect the identities of participants by disguising their identities. I ensured the confidentiality of each participant, organization, and secondary data (SD) by assigning them a unique study ID (i.e. Organizations 001, 002, and so on; Participants 001A, 002A, and so on; and Secondary Data SD01A, SD01B and so on). Cooper et al. (2016) noted the use of study codes is a sufficent measure for maintaining the confidentiality and protecting the privacy by providing additional safeguards of each participant or organization involved. The researched assured privacy and confidentiallity of the data that was provided to prevent people from determining the participant's identity and organization (Khan, 2014). The

Walden University Institutional Review Board (IRB) number for this study is 03-05-19-0542898.

I will store the data securely for 5 years to protect the confidentiality of each participant and their organization. All the paper documents collected during the research are stored in a locked safe. The data created or collected electronically is password protected and stored in a separate file on the computer. At the end of the 5 year period, I will destroy all hard copy documents by shredding, and all electronic data and recordings will be permanently destroyed.

Data Collection Instruments

I was the primary data collection instrument in this study. Yin (2013) stated the main instrument in the data collection process is the researcher. As research continued to evolve, Yin (2017) later concluded that data collection should include a minimum of two sources to include direct observation, documents, artifacts, interviews, archived records, and participant observation. I used semistructured interviews with audio recordings and direct observation to include journal notes and the current analysis of publicly available data.

Interviewing is a way of collecting data to help direct the participant in responding to a specific research question (Stuckey, 2013). I collected data using a semistructured interview protocol. Winbaum & Onwuegbuzie (2016) concluded a semistructured interview allows the use of an interview guide, with the order of the questions altered based on the direction of the interview and additional questions asked for the purpose of prompting and probing. I used semistructured interviews to ask open-ended questions and support the collection of rich data. Additionally, I followed an interview protocol (see Appendix A). White (2017) observed that researchers should ask each participant the same questions throughout the interview. By following the protocol, I maintained consistency of my semistructured interviews.

In addition to the conduct of semistructured interviews, I collected and reviewed publicly available data related to data breach and the security of the Internet cloud. Yin (2013) stated that a secondary source in relation to the interview could help expand and confirm the data collected from each interviewee; therefore, the publicly available data was used to verify the findings of the data I collected during the interview process. A researcher should take the time to observe each data collection instrument carefully because evidence may have the tendency to arise verses listening (Hunt, 2014). Minimizing the amount of talk time with each participant and during the recording of the interviews will allow the observation of participants' verbal and physical behavior in a neutral setting (Houghton et al., 2013).

I used member checking and triangulation to verify the accuracy, reliability and credibility of my study. Birt et al. (2016) believed member checking involves returning and reviewing the results of the study with the participants. Additionally, member checking and data triangulation are used to ensure the authenticity of data (Carter et al., 2014). The member checking process allowed each participant to revisit his or her words and provide further clarification. Additionally, it also allowed the participants to double check and make sure their answers were recorded correctly during the transcribing process (Widodo, 2014). The advantage of completing member checking is to understand the issue at hand better (Doody & Noonan, 2013). In the interview, I allowed each participant to speak on the current strategies that work for their organization as well as allowed them to provide information on what they thought might work out better. The disadvantage of member checking can be the amount of time the researcher must put into transcribing and going back with follow-up interviews (Jamshed, 2014). Once the member checking process was completed, I had each participant confirm my interpretation by providing a transcript review and using member checking. I used member checking because it allowed me to verify participants' responses to the interview questions appropriately.

Data Collection Technique

The purpose of this study was to find out what strategies some information security leaders in the aerospace and defense contractor industry used to protect cloud-based data from security breaches. Yin (2017) described six sources of collecting data in case study to include documentation, archival records, interviews, direct observation, researcher or participant observation, and physical artifacts. The data collection technique that I utilized in this study was a semistructured interview protocol (see appendix A) and additional documentation to help guide me in gathering data from each participant. Cachia and Millward (2011) deemed a semistructured interview is practical when collecting qualitative research data. Conducting a face-to-face semistructured interview allowed me to focus on the topic being observed and decrease the chances of the interviewee not answering. Another key aspect in using the semistructured technique is obtaining in-depth responses to each of the questions highlighted in the interview protocol (Qu & Dumay, 2011).

I utilized technology tools such as Freeconference, Microsoft Outlook, and email. Further, I obtained data from emails, face-to-face meetings and interviews. Technology tools such as SKYPE and Video Conferencing were not necessary because all of my potential participants are local. The target was to find a convenient atmosphere that is accessible, comfortable, and relaxed. An interview transcript was emailed to participants for their review, feedback, and confirmation to make sure the collected data was filtered to improve the reliability and relevance of the study.

A researcher's interview protocol works as an instrument that asks questions related to the aims of a study, as well as serving as a conversation on a particular topic (Patton, 2015). The interview protocol contained instructions on how to conduct an interview properly that should take no more than two hours. I decided on this time because it takes time, careful listening, and intentional follow up for participants to explain their experiences (Castillo-Montoya, 2016). The instructions I developed for the interview protocol included open-ended questions and prompted me to watch for nonverbal cues. Additionally, I collected data through other documentation such as publicly available data to get a better understanding of securing data within the cloud. Anderson et al. (2014) suggested a researcher who uses organizational policies as a source of data collection is better able to recognize, record, and transmit organizational practices.

One advantage to using semistructured interviewing is that the researcher can prepare the questions in advance (Doody & Noonan, 2013). This allowed me the opportunity to be well prepared and knowledgeable during the interview process. Secondly, semistructured interviews is an efficent and effective method that produces rich and detailed information during the qualitative data collection process (O'Keeffe et al., 2016). Interviewees had the opportunity to ask me any questions they may have had or seek further clarification about any question they wanted to revisit during the interview process. Another advantage of a semistructured interview is the opportunity for the interviewer to observe nonverbal communication from the participants (Irvine et al., 2013). While carrying out the interviews, the process was recorded which afforded me the ability to conduct direct observation with each participant.

The disadvantage to semistructured interviewing is the presence of potential biases due to the degree of subjectivity (Baskarada, 2014). This could have a skew on the results of the study, so it is important to verify there is no bias during member checking. Another disadvantage included the interviewer giving out unconscious cues that may persuade the participant to give expected answers (Jamshed, 2014). Last, another disadvantage included the participants not being available or the feeling that their privacy will not be protected (Stuckey et al., 2014). The researcher managed disadvantages by contacting all participants a few days before their scheduled interview to make sure they were still available for their allotted time, reiterating the ethics and importance of privacy prior to the start of the interview, and continuing to maintain the rapport that was established.

Utilizing publicly available data as a data source is in alignment with current recommendations for case study data collection (Rule & John, 2015). The advantages of using secondary data such as publicly available data include a saving in time and cost-effectiveness, easy accessibility, and information being collected from another person rather than the researcher. Researchers look for efficient ways that can save time and are cost effective (Church, 2001). In some cases, secondary data are more accessible and can generate common patterns (Johnston, 2014). The disadvantages of secondary data may include the available data not being collected to address the particular research question (Cheng & Phillips, 2014).

When the interview process was completed, I performed member checking within 10 days of the original interview. Member checking played a significant role in validating information (Andrasik et al., 2014). Member checking allowed participants the opportunity to check or approve the aspects of the interpretation of the data they provided (Carlson, 2010). The interview protocol provided instructions for member checking. During the follow-up, I shared a concise summary of the responses from all open-ended questions and allowed the participants to respond by agreeing or disagreeing with the information transcribed. I also took the opportunity to clarify and go back to any unanswered questions in order to collect the right data.

Data Organization Technique

Data tracking systems can be helpful in data collection and allow sequential analysis (Meinecke et al., 2017). For instance, I deem it prudent to make use of file names for purposes of consistency and reduce inconsistency. Therefore, I will keep track of data through research logs and records that will be stored in a folder named for each case study. Tracking systems help researchers achieve effective data collection and structure (Anney, 2014). A researcher uses a research log for record keeping purposes and secretly identifies each participant (Yin, 2017). I utilized a research log within this study and will store all hard copy data and recordings in a fire protected locked safe located within my home for 5 years. After the conclusion of 5 years, I will destroy all data. Assigning generic codes to all participants allows the researcher to maintain confidentially and allows for organization (Yin, 2017).

Additionally, once I analyzed all the data from the interviews, observation field notes, and publicly available documents, I recorded the themes and encrypted the information with NVivo®, and stored the confidential documents into Dropbox. I created a backup of the data on a universal serial bus (USB) drive, encrypted the information, and stored the drive in a locked file cabinet in my home. I will keep all data, both hardcopy and electronic, for 5 years before deleting or destroying it. After 5 years, I will remove all data I store in the Dropbox and shred any hard copy documents kept in the locked file cabinet.

Data Analysis

The best way to organize data is to go back to the interview guide and identify and differentiate between questions and topics that were derived (O’Connor & Gibson, 2003). Triangulation utilizes more than one particular approach in order to obtain richer and fuller data by confirmong the results of the phenomenon being studied (Wilson, 2014).

Carter et al. (2014) identified four types of triangulation; (a) method triangulation, (b) investigator triangulation, (c) theory triangulation, and (d) data triangulation. Data triangulation is the most suitable data analysis for this qualitative case study. Data triangulation involves the collection of data from different sources such as people, groups, families, and communities, etc. to gain multiple perspectives and increase the validity of a study (Carter et al., 2014). In addition to conducting interviews, I collected data through different sources such as publicly available data and through direct observation. I confirmed the data through member checking.

Principally, there are four fundamental aspects of qualitative data analysis; coding, classifying, categorizing, and labelling of primary patterns (Elliott, 2018). Coding is an important part of data analysis that involves discovering of themes that encompass abstract constructs that investigators identify before, during and after the process of data collection (Theron, 2015). Classification enables researchers to complete the task of data collection successfully (Maylor & Blackmon, 2015). The categorization process involves scanning data to develop a phenome that share common characteristics and relationships (Elliott, 2018). Labelling is the final stage of qualitative data analysis. It entails indexing or assigning data codes to phenomena that are used to distinguish them based on their similarities and differences (Anney, 2014). In this stage, the researcher put data in meaningful analytical units to reduce technicality and complexity to enhance understanding.

In qualitative research, data collection and data analysis are integral tasks that usually complement each other (Anney, 2014). This means that they equally depend on one another if the objectives of a qualitative research are to be addressed satisfactorily. Hence, data analysis and data collection will always overlap (Sutton & Austin, 2015). Before data collection tasks are completed, a substantial period is spent on data analysis particularly when pilot tests must be conducted at the beginning of a qualitative research (Mancini et al., 2017). As time goes on, the researcher dedicates more time to data analysis, and less time is spent on data collection.

Themes and patterns emerged as I transferred interview transcripts and external information using NVivo®, a qualitative data management software used for data analysis (Zamawe, 2015). NVivo® empowers researchers to include information and recognize topics and patterns, data organization, and coding (Houghton et al., 2013). Gibson, Webb, and Lehn, (2014) showed that analysts use programming to help with monitoring and to sort out information. Meyers and Lampropoulou (2013) noticed that researchers utilize PC programs for arranging and sorting interview responses and information from different sources. Researchers use PC programming to aid interpretation, data organization, journaling, and data analysis (Wilerson et al., 2014). I focused on the key themes and correlated the key themes by conducting the literature review and the conceptual framework. Last, I compared key themes that I identified within the literature review and conceptual framework with new studies that were published during the start of my proposal.

Reliability and Validity

Reliability

Barry et al. (2014) viewed research as reliable if the outcomes are repeatable and the foundation of information legitimacy alludes to the precision of the information. A research study is reliable when another researcher can rehash the study and get comparative or the correct results (Cope, 2014). A reliable study should be able to show dependability (Elo et al., 2014).

Dependability refers to the consistency of the research data over similar conditions (Cope, 2014). Dependability enhances the trustworthiness of the study because the results of the study are repeatable as well as consistent (Elo et al., 2014). According to Liu et al. (2015), researchers ensure consistency through the data they collect for the study to make sure if a different researcher uses the same data, they would arrive at same findings, interpretations, and conclusions. This is also crucial because it ensures that there was nothing missed while conducting the study especially in analyzing the collected data. The researcher applied the same practice for this study. I ensured dependability by utilizing member checking and providing participants with their transcript responses. Once I received and verified their responses, I began to analyze the data.

Validity

Validity may refer to the accuracy or correctness of the findings in a research study (Lueng, 2015). Validity in research helps enhance the trustworthiness of the study (Golafshani, 2003). The four aspects that ensure validity are credibility, transferability, confirmability, and data saturation (Sandelowski, 2014).

Credibility. According to Resnik (2014), credibility is crucial in a study or research because it enhances the dependability of data. For instance, if the people to be interviewed can trust the interviewer, then they are likely to give helpful information to the study. The opposite will happen if the interviewer does not have traits of credibility. According to Cooper and Schindler (2014), for a study to be credible, it has to prove that it has shown what the participants intended. To ensure credibility of this study, the researcher will use member checking where the researcher will double-check all the data for errors. If the findings of the study show clearly the meanings described by the participants, then the research can be said to be trustworthy, hence, credible (Cooper & Schindler, 2014).

As Cope (2014) argued, member checking enhances the accuracy of the data used, which is important because it means that the results will be accurate as well. Member checking was done for this study, and each member participated to ensure that the results are not biased. If a study passes the right procedures, it is considered trustworthy and credible (Liu et al., 2015). It is important to account for all the information that may have an effect on the research during the collection and analysis of data (Cooper & Schindler, 2014). These could include participants' attitudes, which may interfere unconsciously with the findings.

Transferability. It is important that a study is transferable. Transferability is important because the results of a study can be significant to another group not necessarily involved in the study (Elo et al., 2014). To ensure that a study is transferable, it is important to give all the detailed information that may be helpful to other groups of people in conducting research (Cooper & Schindler, 2014). This is achieved through ensuring that this study explores as much information as possible (Maylor & Blackmon, 2015).

Transferability becomes apparent in this study through describing and documenting all the procedures so that anyone interested in conducting a similar research can use. Other than research findings being useful to other researchers, they can also be useful to certain times, or a particular population (Cooper & Schindler, 2014). As Cope (2014) argued, the researcher cannot prove that the findings of the research are transferable. Additionally, it relies on the reasoning that findings can be generalized or transferred to other settings or groups (Elo et al., 2014).

Confirmability. Cope (2014) indicated that confirmability ensures that the researcher represents participants' responses and not the researcher's bias. According to Houghton et al. (2013), a researcher normally conducts confirmability to make sure that the results provided, or the data used, is not biased. Confirmability is usually conducted by various means. Cooper and Schindler (2014) affirmed all the procedures used when collecting and analyzing data will be documented for this case and will be presented to confirm that they are done in the right way. A data audit can also be conducted to ensure that the right data was used (Nowell et al., 2017).

For the purpose of confirmability, Mehmood et al. (2016) stated that it is important that the researcher also document all the negative instances in the study. These instances are normally useful in determining what may have caused bias in the study (Houghton et al., 2013). For this study, the researcher will properly document all negative instances to enhance confirmability of the study. That way it is possible to tell what caused bias in the study. As Maylor and Blackmon (2015) stated, an audit trail is one of the best and most common means of establishing conformity in a study. An audit trail was established through making sure the data collection, analysis, and interpretation were correctly detailed.

Data Saturation. Data saturation is accomplished in research when no new themes occur, and there is enough information to replicate the study (Marshall et al., 2013). Failure to reach data saturation affects the quality of the research being conducted and hampers content validity (Fusch & Ness, 2015). I ensured data saturation by (a) conducting in-depth semistructured interviews, (b) member checking all interview transcripts and recordings, and (c) implementing data triangulation by reviewing current and past company policy and procedures. By implementing these methods, I ensured that I collected rich and thick data for this qualitative multiple-case study. Additionally, data saturation was reached by the third interview.

Transition and Summary

In Section 2 of this study, I restated the main purpose of the study and defined the role of the researcher, the targeted participants, the research method and design, and population and sampling. Additionally, I also further explained the importance of ethical research, data collection instruments and techniques, data organization techniques, and data analysis plans, and the reliability and validity of the study. By identifying the qualitative multiple case study design, this methodology supported the collection of data from information security leaders in order to discover the strategies being used to protect data from the breaches within the Internet cloud. In Section 3, I presented the findings of the study and discussed how the findings from this study might have a positive or adverse effect on current strategies being implemented by information security leaders. Last, I closed out the research by providing the study’s conclusion.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the successful strategies that some information security leaders use to protect cloud-based data from security breaches to improve organizational profitability. I interviewed seven information security leaders within seven aerospace and defense contractor companies in Washington, D.C. The interview responses and eight publicly available sources (inclusive of organizational information) related to data breach and the security of the Internet cloud provided me with the information to address the research question that guided this study. The interviews took place in a quiet and comfortable location where participants were free to respond to six semistructured questions (see Appendix B). Based on the research question and analysis of the data, I identified three emergent themes from the research: (a) authentication methods, (b) encryption, and (c) personnel training and awareness. The conceptual framework that guided this study was IST.

Presentation of the Findings

The research question that guided this study was: What successful strategies did some information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches to improve organizational profitability? The findings may assist information security or IT professionals in developing an effective risk management approach that reduces data breaches. I conducted semistructured interviews to gain an in-depth understanding. In addition to semistructured interviews, I reviewed publicly available organizational data and recently published documents to collect data for this study. Access to publicly available documents allowed for validation of the information obtained during the interview. I conducted all interviews in a distraction-free conference room, and each interview lasted 45 minutes.

The interviewees answered six semistructured questions that were centralized around the research questions. The interviews were recorded and transcribed using software such as Temi^{TM} and Trint^{TM} . Once the transcription process was complete, I performed member checking by asking participants to verify their transcripts. Member checking continues to be an important quality control process in qualitative research (Harper & Cole, 2012). After member checking was verified, I then imported the transcripts, organizational data, and published documents into NVivo ® 12 software and began analyzing and coding the data in search of common themes. By using the NVivo ® 12 software, I was able to identify three core emergent themes. The three themes were (a) strong authentication methods, (b) encryption, and (c) personnel training and awareness. The following sections present the summary of each theme.

Theme 1: Strong Authentication Methods

Strong authentication methods emerged as a theme from the interviews and supporting documents. A strong authentication method involves implementing both two- and multifactor authentications, which aligns with internal controls within the IST and privacy and security within the literature review. If the cloud becomes compromised by intruders, all of an organization’s resources will be at risk (Ahmad et al., 2018). Managing authentication and access control within the cloud is a major challenge that the participants addressed (Naik & Jenkins, 2016). Authentication is the procedure by which an individual that is attempting to access a secured domain is vetted by utilizing the appropriate accreditations. Authenticating a person by password continues to be the main power of information security and must be effective to serve as the preferred method for securing the cloud (Rajamanickam et al., 2020). The objective of the authentication process is to increase the security level of authorized users and to hinder unauthorized access (Kaur & Mustafa, 2019). Therefore, passwords should be long and convoluted.

Strong authentication methods were a theme that was common amongst five (71%) participants and six (75%) of the secondary data documentation. The participants and secondary data demonstrated that having solid authentication techniques expands security. Participant 001D stated, “Administrative identity should require strong authentication across the board and should also have one-time-use credentials that are generated based on the user and their role.” Participants 001F expressed, “The way to having solid confirmation is having the option to affirm who is attempting to access the system (through username and password) and one of the techniques for accomplishing that is system authentication.” Participant 001G specified, “Privileged users requesting access will be checked to confirm all security is refreshed before allowing full access to the secured domain.” Meanwhile, participants 001B and 001E suggested, “Having a strong factor authorization and authentication process in place will safeguard sensitive information that is stored in the Internet cloud.”

Multifactor authentication. Participant 001D expressed, “Multifactor authentication should be mandatory and utilized across all users and accounts. Using this strategy requires a password as well as an extra technique for the client to confirm their identity." Participant 001F conveyed, "When access is given to standard clients, they will utilize their client ID and their password, which must satisfy the appropriate standards." Participant 001G stated,

> Multifactor authentication gives an additional type of security by creating layers of defense which makes it more difficult for intruders to access target areas. If one of the factors become compromised, the intruder has at least one more barrier to breach before getting to the intended target. By that time an intrusion detection should take place.

Archival document analysis on multifactor authentication. SD01C stated,

> Multifactor authentication or use of at least two separate identifiers of authentication instead of using just an ID and password helps increase security access by adding multiple barriers to inbound user access before actual entry is allowed. In doing so, this reduces the likelihood of an attacker break-in and makes it harder for anyone with a stolen password to gain entry to the system by accessing critical data.

SD01A, in turn, stated,

> Multifactor authentication is necessary. Organization 001GG considers, "identity and authentication services integrate with public key infrastructure (PKI) to support smart card and multifactor authentication for hosted applications and management functions. This method implements best practices for identity and access management (IAM), account management, and role structure."

Information in the secondary and organizational publicly available documents served as confirmation of leaders' expressed assent that multifactor authentication is necessary and results in the application of best practices for validating each user access as described in the interviews. Moreover, as conveyed in the literature, to maintain data confidentiality in the cloud, users need to implement authentication to minimize data breaches. Further, the same participants indicated that multifactor authentication (sometimes referred to two-factor authentication or 2FA) serves as an enhancement to security by providing two different barriers.

Two-factor authentication. Participant 001B expressed,

> Two-factor authentications are important because passwords are antiquated. For example, single-use passwords as you have seen in the news from Target to Amazon to Google is hackable. Passwords are the number one easiest thing to break. In turn, we try to go with a two-factor authentication code."

Participant 001F encouraged, "Going with a two-factor authentication method to add an extra layer of security designed to ensure that you're the only person who can access your account and prevent the potential of hacking."

Archival document analysis on two-factor authentication. SD01E stated, "Two-factor authentication can be applied for restricting unauthorized access. Moreover, role-based access control mechanism can be implemented which is an important method to restrain the availability of information needed to perform a certain task." SD01F conveyed, "Authentication must be implemented at various levels in the system." SD01A stated, "It is also important for organizations to invest in the infrastructure to support and making sure all personnel understand the importance of two-factor authentication." Organization 001FF stated,

> Other password security measures to include when it comes to two-factor authentication is not using the same passwords across multiple accounts, making sure your user passwords are at least eight characters long and consist of a unique combination. It is encouraged that passwords include uppercase and lowercase letters, symbols, and numbers, and do not include identifiable words such as birthdates, addresses or phone numbers in your passwords.

A strong authentication method was a frequent theme amongst the participants and secondary data, which also aligned with the conceptual framework that guided this study. Hong et al. (2003) used IST to assist in identifying unknown gaps and the lack of pertinent information related to information security risk. Users' being able to implement proper authentication methods reduces the perceived risks from improper authentication. Additionally, Hong et al. (2003) applied the IST to assist in establishing control systems and security policies, which in turn is enforced by proper authentication methods in securing networks.

There is additional literature that supports the reasons for a strong authentication method. Many organizations are trying to increase account security by stressing the importance of authentication to include both two-factor and multifactor authentication (Albayram et al., 2017). Some information security individuals trust the authentication practices that implement public-key cryptography and stonger mutual athentication as the right approach (Ghazizadeh et al., 2014). Cloud systems require protection mechanisms that will continuously monitor network activity and detect intrusions (Ahmad et al., 2018). Individuals tend to underestimate the risk involved when it comes to the importance of cloud security. Huang et al. (2011) and Albayram et al. (2017) found risk awareness to be a substantial factor in increasing users' willingness to follow security advice (e.g., choosing secure passwords), hence, the relation to the IST.

The collected data from the participant's response and the publicly available data on authentication methods support the conceptual framework and the relation to the importance of authentication. Adding an extra layer of verification such as multi-factor authentication to the cloud adds an additional form of security (Abdellaoui et al., 2016). Multifactor authentication serves as a centralized access control mechanism to secure data in the cloud (Anakath et al., 2019). When talking about security, user responsibility and accountability are mechanisms to help achieve security goals such as keeping data private (Duncan & Whittington, 2015). Chanda (2016) stated users tend to set short and easy to remember passwords, which are highly vulnerable to attacks. Therefore, a computer-generated password generally possess a higher degree of randomness and security.

Table 1

Strong Authentication Methods (Frequency)

Source of data	Data collected from	Total number of references
Participants	5	10
Secondary data	6	7

Theme 2: Encryption

Cloud computing is a version of an IT service model where cloud customers can remotely store any type of data into the cloud to enjoy the benefit of on-demand high-quality applications and services from a shared pool of configurable computing resources (Marston et al., 2011; Mell & Grance, 2011; Marchisotti et al., 2019). Systems under cloud computing distribute and nest many resources and private information, therefore the cloud environment is an easy target for intruders looking for possible vulnerabilities to exploit (Ahmad et al., 2018). Suguma and Raja (2018) stated to protect data privacy, sensitive data, which may include e-mails, personal health records, photo albums, tax documents, financial transactions, and other data, organizations should encrypt the information before outsourcing to the commercial public cloud or other users.

Encryption was an item that was common among four (57%) participants and seven (88%) of the secondary data (see Table 2). Many leaders have reported privacy and security breaches due to lost or stolen assets. In response, Participants 001B, 001D, 001E, and 001F stated, “Organizations now use encryption to mitigate the risks of unencrypted data assets throughout the entire data lifecycle.” Participant 001F concluded, “Encryption enables secure data sharing with suppliers and customers and integration of encryption solutions with existing infrastructure is highly recommended to enhance data security.”

Archival document analysis on encryption. Organization 001FF stated, “Many organizations have reported privacy and security breaches due to lost or stolen assets. In response, many leaders within an organization use encryption to mitigate risks of unencrypted data assets throughout the entire data lifecycle. This also enables secure data sharing with suppliers and customers. Integration of encryption solutions with existing infrastructure is highly recommended to enhance data security." Additionally, SD01C stated, "Encryption is the conversion of data into seemingly random, incomprehensible data which ensures that data remains jumbled to everyone for whom it is not intended, even if the intended user has access to the encrypted data."

Data at rest encryption is a method to protect data at rest within the cloud server. Participant 001E stated,

> When it comes to data at rest, they incorporate different things such as encryption methods like S3, which is where you store all your files. Individuals can encrypt a service by enabling encryption on buckets. Securing data at rest and migrating data from one source to another while it is there in storage capacity involves encryption. Leaders should make sure, depending on the circumstance with the data, that the data remains secure. Again, this secures data at rest while it is sitting there and not in transit.

Participant 001B stated, "Their organization stresses multifactor authentication at this state for the added layer of protection."

Collectively, Participants 001B, 001D, 001E, and 001F stated,

> The most critical part for the implementation of any of these methods is key management for data encryption and decryption. The most common way to protect data in motion is to utilize encryption with authentication, which can safely pass data to or from the server within the cloud.

Organization 001GG believed, “Encryption of data at rest should utilize built-in cloud and third-party solutions and full volume encryption of cloud storage to protect data from unintentional disclosure and malicious activity.”

Data in transit involves the flow of information over a public or unsecured network. Participant 001B shared,

> In terms of securing the data their organization does encryption in transit and at rest. We set up transport layer security (TLS) protocols and Internet protocol security (IP SEC) tunnels just to make sure the data being transcribed between their infrastructure and client cloud service provider is encrypted.

SD01B stated, “This process makes the other major security aspect difficult. Also, while this process is taking place, they apply the aspect of monitoring and two-factor authentication.” Participant 001E added,

> While the data is in transit, they assure that the data is secure from any breaches or any type of leak by implementing https, or any type of SSL encryption which will secure the data while transferring from one source to the other, or any location while it’s moving.

Archival document analysis on data in transit. Reflective of the interview findings, SD01D stated, “All these mechanisms involved with data in transit is intended to make sure that organizational data remains safe.” Organization 001GG stated,

> When it comes to the data itself, like accessing the data, they make sure that there are no breaches from whenever there is an end-user or someone who is trying to access the data or whenever we provide the data to them, they also want to make

> sure that while providing that data, there's no breach or any type of mishandling with the data from one user to another. Therefore, they incorporate factoring authentication.

Information in the secondary and organizational publicly available documents served as confirmation of leaders expressed assertion that encryption is necessary because it allows the user to protect data securely as described in the interviews. Moreover, as conveyed in the literature, to maintain data in the cloud, organizational leaders should ensure that only legal users have the authority to access certain data to minimize data breaches. Further, participants 001B, 001D, 001E, and 001F indicated that encryption securely protects files and other sensitive information when file sharing as well as mitigating risks of spillage.

The use of cloud computing is snowballing into one of the most promising platforms which has increased rapidly in many organizations (Miyan, 2017). According to Gaidhani et al. (2017), cloud computing poses confidentiality concerns where data might be leaked either accidentally or intentionally, or by an external attacker who succeeds in gaining unauthorized access and the solution is data encryption. In order to improve the security and confidentiality of the data stored in the cloud, users must encrypt before uploading into the cloud (Lakshmi, 2017). Additional literature shows that data confidentiality is achieved through proper encryption methods within the cloud (Miyan, 2017). Therefore, encryption is one of the best ways to make data in the cloud secured (Sharma, 2017).

Data privacy is an increasing concern for business leaders today and privacy issues effects all types of stakeholders within the cloud (David & Dhillon, 2019). To protect data privacy it requires encrypting and decrypting the data files while in transmission over the cloud (Agarkhed & Ashalatha, 2017). Various encryption techniques and valuable mechanisms are used to ensure that data is shared between valid users (Kaur & Kaur, 2018).When it comes to cloud computing, this technology enables organizations to expand IT limits without putting into a new framework and authorizes new programming (Khan, 2019). This offers flexibility, economic saving, availability, and efficency by being available remotely (De Donno et al., 2019). Data protection is one of the most important security element because organizations will not be able to transfer their data to the remote machine because of the lack of guarantee of data protection (Shaik et al., 2017). Without the proper encryption technique, information travelling through computer networks may be vulnerable to being intercepted, modified, fabricated or even interrupted by an unauthorized user (Mehran & Khayyambashi, 2017).

Not only was encryption a common theme between the participants, but it also aligns with the IST when it comes to the component of control and auditing. When it comes to control and auditing, Hong et al. (2003) suggest that an organization should establish information security controls to maintain access controls and organizational security. Encryption is aligned with the IST under the component of information security. Security policies are important for ensuring compliance with security practices in an organization (Ismail et al., 2015). IST provides the basis for the research framework concerning information systems security and highlights the importance of integrating effective security components within an organization to ensure that any type of data is properly classified and protected.

Table 2

Encryption (Frequency)

Source of data	Data collected from	Total number of references
Participants	4	9
Secondary data	7	13

Theme 3: Personnel Training and Awareness

A third major theme that emerged from the analysis of the data is the training and awareness of personnel. Awareness is the first line of defense for the security of information systems and networks (Tasevski, 2016). All seven (100%) participants and four (50%) secondary documents indicated that the lack of training or training to stay updated with the transition to the cloud prevents the successful implementation of cloud security strategies. The findings showed that information security leaders need to align the personnel of their organization and repurpose them to focus on more business effective solutions. Providing adequate training builds the personnel's knowledge of how important a part they play in securing proprietary data and how much of a benefit cloud computing can be to the organization. By not providing the proper awareness and training to personnel, an organization can become exposed to a variety of security risks for which people, rather than system or application vulnerabilities, are the threats and points of entry (Piplode & Singh, 2012). Olusegun and Ithnin (2013) stated educating users on the criticality of information security is vital and important to the mission of establishing sustainable information security in any organization.

Participant 001A stated, “Old-timers like me, like to do things the way we like to do things and training seasoned individuals can be a struggle. However, training is necessary for making people understand the risk associated with securing data within the cloud.” Participant 001B highly suggested, “Security awareness training for all personnel and staff.” Participant 001C indicated,

> That the breach analysis they read recently points to a lack of competent administration when looking at root cause analysis of cloud data breaches. It would appear from the data that the press to move vast amounts of data to cloud-based solutions has outpaced our training and education process. Many root cause analyses simply point to the fact that administration personnel did not know what they were doing when it came to configuring or services they were enabling. The lack of training, poor use of tools, lack of understanding of the organization’s business functions all have led to significant data breaches.

Additionally, participant 001C recommended,

> Organizations should accelerate the pace of training so it can better match the pace at which an organization migrates or establishes its services and data using cloud-based solutions. This is not unique to cloud solutions. Before cloud-based breaches, system administration personnel remained the root cause of data loss/compromise.

Participant 001D stated, “Organizations should want to train people. Organizations should want to embed the importance of security in their security training and train their users on things like phishing and spam and other types of attempts.” Participant 001F said, “Organizations should also want to make sure users are aware of any acts such as trying to gain unauthorized access into the system. Building this continuously will help.” Participant 001E continued, “To encourage the use of personnel and customer awareness and identified different avenues to gain appropriate training.”

Archival document analysis on personnel training and awareness. SD01A stated, “Raising awareness among cloud actors about different aspects of security and privacy, regularly, is necessary. Cloud application developers must be trained on and encouraged to use a security development life cycle.” SD01E indicated,

> A cloud system must be dynamic and flexible. Seminars, workshops, and conferences should be organized for the training and education of personnel on a regular basis after a certain period. Education and training programs perform a significant role in achieving information privacy and security in the cloud. After t he workshop or seminar, skills of the technical personnel should be tested for understanding.

SD01F specified, “Employee resistance can be expected when the introduction of new technology gets adopted by an organization. Organization 001GG assumed, “Personnel training is an effective tool for managers to prepare employees for the change. Personnel training also furthers the knowledge and helps facilitate learning amongst all personnel involved.”

Information in the secondary and organizational publicly available documents served as confirmation of leaders expressed assentation that personnel training and awareness is necessary because it teaches all personnel to understand the risks and threats involved when it comes to the data in the cloud as described in the interviews. Moreover, as conveyed in the literature, to maintain data in the cloud, organizations should ensure that all personnel are aware of the consequences of failing to protect data from outside intruders. Further, the same participants indicated that proper personnel training and awareness helps prevent breaches.

Personnel training and awareness relates to both the IST and literature review. This theme relates by instilling a detailed and thorough security policy and relates to managers setting expectations, establishing appropriate rules for user behavior, and establishing a baseline of employees' responsibilities (Hong et al., 2003). The IST offers a fresh perspective on approaching employee enterprises. A part of IST focuses on the importance of security guidelines and policies to remain effective; it is ideal that all personnel are trained and aware. Continuing to regulate consumer privacy and security also challenges government enforcement of data protection laws (King & Raja, 2012). Lafuente (2015) stated that before any big data project begins organizations should have the right mechanisms in place to protect that data which is acquired through awareness and training. Security awareness is a crucial part of any information security program either at a personal or organizational level (Alruwaili, 2019).

Table 3

Personnel Training and Awareness (Frequency)

Source of data	Data collected from	Total number of references
Participants	6	14
Secondary data	4	8

Applications to Professional Practice

The most significant contribution from the study findings may be the identification of the best practices aerospace and defense contractor organizations use to protect cloud-based data within the cloud. Information security leaders are gradually finding it difficult to determine the best solution to protect cloud-based data. However, the findings obtained from this study resulted in key themes that may be useful and used by organizations and companies in their practices to encourage organizational improvement. The most significant contribution may be the potential to minimize data breaches, which could increase business performance and profitability. Without proper controls, data breaches within the cloud will continue to rise and cause harm to customers and organizations. The findings will be beneficial to information security leaders, business leaders, and IT professionals to strengthen security protocols and privacy defense mechanisms within the cloud which promotes the migration of data into the cloud.

Intrusions with the theft of data can cause organizations harm by the intruder gaining access to systems and consumer data (Barona & Anita, 2017). This results in grave damage to an organization’s reputation and the loss of consumer and customer confidence. With the increase in cloud computing, personnel training and awareness is a requirement in enhancing security awareness to minimize data breaches. The findings of this study may help information security leaders in reducing the costs incurred in the efforts to respond quickly to cases of breach of data within the cloud. By implementing these security strategies, other organizations and industries may adopt successful strategies, increase customer’s confidence, and sustain the reputation of the organization.

The strategies demonstrated by the findings from this study are critical to IT professionals by aligning cloud computing with business models and successful strategies to address the effects of data breaches on the performance of businesses (Joia & Marchisotti, 2018). The characteristic of cloud adoption have an effect on an organizations privacy as well as security (Tyagi et.al, 2019). The findings of this study identified successful authentication methods, encryption, and personnel training and awareness requirements to minimize a breach within the cloud. By providing successful security strategies, organizations are equipped with the tools to mitigate risks of breaches efficiently.

The cloud is evolving into a reliable storage; however, there are substantial security issues such as ensuring confidentiality, integrity and privacy (Udendhran, 2017). The findings of this study can be used to provide additional resources for information security managers to use in their efforts to protect data within the cloud environment.

Business, Governments, and private organizations make extensive use of information and the most current technologies, and as a result security is of utmost importance (Alruwaili, 2019). Implementing the best practices identified in the study findings can assist in the mitigation of the data security threats. Moreover, the findings may also help information security leaders reduce the cost incurred while protecting confidential data by forcing organizations to adopt security best practices, and efficiently training employees to respond to growing security threats (Manworren et.al, 2016). Data breaches pose a significant security and privacy risk on stakeholders, stockholders, and affected consumers of an organization (Zou & Schaub, 2019). Therefore, information security managers and business leaders should implement successful strategies that protect consumer data and other types of information that are confidential. These best practices may lead to the improvement of the current security presence within the organization and used as a guideline by the business and organizational leaders to ensure the protection of such kinds of confidential information.

The internet cloud is used in a range of organizations in different industries. Therefore, data is an asset that is critical and has to be protected against breaches and threats. One of the most critical challenges related to cloud computing is earning consumers trust by ensuring adequate privacy and security for sensitive date (King & Raja, 2012). The difficulty is how to ensure consumer’s data is safe in the cloud (Zhang, 2011). Data leakage can be caused by internal or external breaches, either intentional or inadvertently (Cheng et al., 2017). The study findings can assist security leaders in implementing strategies that control the varying and growing risks and vulnerabilities to the cloud infrastructure.

Large numbers of industries have adopted or developed cloud services and stored sensitive data over the cloud (Alam, 2018). Therefore, data as an asset is critical and must be protected against breaches and threats. Data protection includes fostering protective countermeasures against criminal threats. The exposure of data may lead to severe consequences and cause customers and organizations to lose their money and reputation due to data breaches (Basheer, 2020). One of the greatest concerns within an organization is unauthorized access to data (Yisa, 2018). The study findings can assist security leaders in implementing strategies that protect from the potential loss of data from unauthorized access within the cloud infrastructure.

One of the outcomes from the study is a clear understanding that when successfully implementing data breach strategies within the cloud infrastructure, it helps control the compromise of data. Implementing data breach strategies could help organizations in detecting, identifying, and analyzing potential threats so that future occurrences of data breaches can be minimal. Additionally, the results from the study may provide information security leaders with an in-depth understanding of data breaches, to include strategies used to decrease the possibility of security occurrences.

Implications for Social Change

A vital implication of this study was to find effective ways to reduce breaches within the cloud. Developing effective strategies used in protecting sensitive information within the cloud could assist the aerospace and defense contractor industry in achieving their organizational goals. With the increase in cloud adoption, the incidence of cybercrimes has also increased (Alruwali, 2019). Consumer data is considered valuable assets to an organization. Allowing the consumer and customer to understand that their sensitive information will be properly stored in a secured cloud will reflect a positive change. Therefore, organizations should implement best practices to minimize the threat at which data becomes exposed during a security breach. From a social change standpoint, the findings of this study may be useful to organizations because it helps build trust, confidence, and assurance between their customers and consumers. An organization may result in continuing to uphold its reputation by maintaining a decrease in compromised data.

Furthermore, the findings explained that when information security leaders implement distinct security strategies, this encourages a confident cloud environment knowing that sensitive data will be secured, which promotes cloud usage and consumer satisfaction. The study findings identified key tools necessary for securing data within the cloud, which will protect both the consumer and customer from loss or theft of assets and funds. Additionally, the study findings provided a detailed analysis of the effective security strategies used by information security leaders that may affect social change by protecting its consumers and customers’ PII. Effective security strategies, when implemented, will keep a handle on inappropriate access or destruction of sensitive information, PII, and proprietary business information.

As the volume of data continues to grow exponentially and data breaches are becoming more frequent, detection, and prevention of data loss has become one of the most pressing security concerns to an enterprise (Cheng et.al, 2017). Data breaches have proven to be costly for both public and private organaizations (Carre et al., 2018). This not only affects the organizations downtime but loss of customers, loyalty, and trust all become a great concern (Choong et al., 2017). The findings of this study can affect social and behavioral change in various institutions, organizations, and businesses. Although the advancement of the cloud is starting to become common, few studies have explained its implication on everyday social life. The results from this study may contribute to positive social change in the sense of implementing more networks for safeguarding customer and consumer data.

Recommendations for Action

The research findings generated data to assist information security leaders in avoiding security breaches within the cloud. The objective of this study was to explore successful strategies that some information security leaders in the aerospace and defense contractor industry used to protect cloud-based data from security breaches. If organizations are starting to move towards adopting cloud computing, information security leaders should assess their current strategies against effective strategies or if no strategies exist within their corporate structure, then information security leaders should adopt effective strategies (Mohlameane & Ruxwana, 2014). Based on the research findings, I recommend the following actions:

- Information security leaders should mandate formal training programs for all staff and personnel to increase security awareness.

- Information security leaders should educate personnel by implementing quarterly security training that focuses on the need to protect sensitive data through strong authentication and encryption in hopes to minimize the threat to sensitive data within the cloud.
- Information security leaders should perform a frequent assessment of current authentication methods.

I will distribute my research findings to all interested participants and other interested individuals within IT throughout the country. Lafuente (2015) stated that people across an organization must understand the consequences of not treating customer and employee data with proper consideration after exposure of sensitive information could result in fraud or identity theft. Information security leaders might utilize the results of this study to design and implement security strategies useful for strengthening the security and resilience of cloud-based data and to protect consumers from the costs, lost time, and recovery efforts associated with identity theft. Once the study is approved, a version of the study will be available to access through ProQuest journal to help other researchers within the IT field.

Recommendations for Further Research

The limitations of this study included unknown factors such as where the participants work, limiting the study to seven companies in the aerospace and defense contractor industry within the Washington D.C. area, participants not having the appropriate knowledge to make informed responses, and obtaining data from information security leaders in a limited geographic area in a particular industry. The participants that were involved in the study collectively provided strategies used to protect data within the internet cloud from data breaches. Data breaches are becoming more common and will continue to pose a threat not only to aerospace and defense contractor companies but to other industries. Additionally, this study design was appropriate because the focus centered on both a small geographic area and a limited number of individuals were chosen as subjects to this study. Therefore, there is a need to expand on this research.

The major limitation of the study was that I focused on a small sample size within a small geographical area. I recommend that future researchers might consider a larger sample size on different industries from different geographical areas and regions in the United States. The other limitation is that the participants might not have had the appropriate knowledge to make informed responses. Further studies might involve participants with experience from diverse backgrounds to ensure reliability in the responses made.

The findings of my study showed that there is a need for leaders or managers in technology to promote a positive outlook on data and security. Additionally, future researchers might expand on the findings of my study by examining the effect of the culture of organizations on the governance of information security. By developing policies that are in line with the culture of the organization and promoting security awareness, technology leaders can develop further strategies to minimize data security breaches to increase the performance of businesses and consumer data protection.

After the findings of this study, a multiple case study might be designed to explore a bigger sample area, which will show a more accurate assessment of the proper protocols to protect cloud-based data from security breaches within a different geographic location. In addition, it will be of interest to future researchers to explore protocols and frameworks different Government agencies or private companies outside of the aerospace and defense industry implement. By studying the outcomes of my research, leaders within the aerospace defense contractor organizations might develop proper protocols to protect cloud-based data from security breaches in order to improve organizational profitability.

I would recommend that future researchers conduct preliminary research on the organizations where they will choose their participants. This will help reduce the cases of biased responses and improve the accuracy of the study findings. Future researchers might also have to conduct the study on other departments within the organization. The researcher might have to consider the composition of the study sample based on other factors such as gender or race. Overall, when choosing the participants in future research, researchers might have to consider all factors applicable.

Future researchers should not have to limit their study on only a few companies in a single industry. Although it might be a challenge in terms of the costs incurred while traveling from one geographic area, it is important to consider several industries as factors for, and issues of data security breaches from industry to industry. This will help in the attainment of reliable results. Once completed, the findings of future research will represent the views and experiences of information security leaders and research participants in different geographic areas.

Reflections

By utilizing a qualitative multiple case study, I explored best practices technology managers use to minimize data security breaches within the cloud to improve organizational profitability. Reflecting on my experiences throughout this process, I found that best practices were similar from company to company. Each participant in this study elaborated on the role they played within the organization and how their role had an effect on the organization's profitability and capability to adapt to the appropriate security measures. One of the common themes that the researcher heard from each organization was how managers continue to play a critical role in leading data security and awareness.

My doctoral study experience improved my knowledge regarding the importance of data security within my current organization. The understanding I gained when interacting with each participant will affect my current and future data security views. Utilizing open-ended questions in this study provided an opportunity for in-depth discussions with each participant. This research aligned with recent data security breaches that occur within the United States, whether reported to the public or not and further enhanced my awareness of the need for effective protocols. I particularly gained knowledge on how these breaches have the potential to affect any organization regardless of the industry and location. I gained more of an in-depth understanding towards the importance of security from when I first began writing my dissertation.

The most challenging portion of the proposal was identifying participants during the collection of data. When selecting my participants, I utilized LinkedIn, which provided me with each participant's description, location, and current job status. I compared the information to those participants that met the criteria to participate and implemented successful strategies to protect their cloud-based data from security breaches within their organization. Based on that criterion, I messaged 36 potential candidates. Out of the 36 potential candidates, I only received responses from seven individuals who were willing to participate in the study because they were intrigued with the study during the initial contact and after receiving the informed consent. Once I started receiving responses, the data collection started to become more exciting versus a stressful situation. Data saturation was reached by the third interview.

Conclusion

The purpose of this qualitative multiple case study was to explore successful strategies that some information security leaders in the aerospace and defense contractor industry used to protect cloud-based data from security breaches to improve organizational profitability. The focus of this study was organizations located in Washington, D.C. By using open-ended questions and reviewing publicly available security and privacy policy documents, the researcher collected and triangulated data to address the research question. During the data triangulation process, three themes emerged during data analysis which identified the best practices information security leaders use to minimize data security breaches to improve organizational profitability. The themes identified were (a) strong authentication, (b) encryption, and (c) training personnel. My findings indicate a need for technology managers to initiate security awareness and annual security training programs to illustrate the serious nature of information security responsibilities. Managers need to become active in their efforts to adopt and implement industry best practices within their organizations, as well as ensure that staff receives added functionalities by deploying effective cloud tools such as authentication and encryption. In addition, information security managers should ensure their staff remain current on security trends and threats.

References

Abdellaoui, A., Khamlicki, Y.I., & Chaoui, H. (2016). A robust authentication scheme for telecare medicine information system. *Procedia Computer Science, 98*, 584-589. doi:10.1016/j.procs.2016.09.091

Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications (IJACSA), 9*(3), 355-373. doi:10.14569/IJACSA.2018.090349

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data, 5*(1), 1-18. doi:10.1186/s40537-017-0110-7

AbuSaad, B., Saeed, F. A., Alghathbar, K., & Khan, B. (2011, December 5-7). *Implementation of ISO 27001 in Saudi Arabia – Obstacles, motivations, outcomes, and lessons learned*. Paper presented at the Security Research Institute Conference, Australia. doi:10.4225/75/57b52709cd8b2

Adams, D. P., & Miles, T. P. (2013). The application of Belmont Report principles to policy development. *Journal of Gerontological Nursing, 39*(12), 16-21. doi:10.3928/00989134-20131028-07

Adashi, E. Y., Walters, L. B., & Menikoff, J. A., (2018). The Belmont Report at 40: Reckoning with time. *American Journal of Public Health, 108*, 1345-1348. doi:10.2105/AJPH.2018.304580

Agarkhed, J., & Ashalatha, R. (2017). Security and privacy for data storage service scheme in cloud computing. *International Journal of Information Engineering and Electronic Business, 9*(4), 7-12. doi:10.5815/ijieeb.2017.04.02

Ahmad, A., Zainudin, W. S., Kama, M. N., Idris, N. B., Saudi, M. M., & Zakaria, N. H. (2018). State of the art intrusion detection system for cloud computing. *International Journal of Communication Networks and Information Security, 10*(3), 480-495. Retrieved from www.ijcnis.org

Alam, S., Muqeem, M., & Suhel, A. K. (2018). Review on security aspects for cloud architecture. *International Journal of Electrical and Computer Engineering, 8*(5), 3129-3139. doi:10.11591/ijece.v8i5.pp.3129-3139

Alase, A. (2017). The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education & Literacy Studies, 5*(2), 9-19. doi:10.7575/aiac.ijels.v.5n.2p.9

Albayram, Y., Khan, M.M., & Fagan, M. (2017). A study on designing video tutorial for promoting security features: A case study in the context of two-factor authentication. International Journal of Human-Computer Interaction, *33*(11). 927-942. doi:10.1080/10447318.2017.1306765

Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. *International Journal of Advanced Research in Computer Science, 10*(5), 1-4. doi:10.26483/ijarcs.v10i5.6476

Alshenqeet, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research, 3*(1), 39-45. doi:10.5430/elr.v3n1p39

Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science, 45*, 436-445. doi:10.1016/j.procs.2015.03.175

Anakath, A. S., Rajakumar, S., & Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing, 22*(5), 10817-10823. doi:10.1007/s10586-017-1181-0

Anderson, C. A., Leahy, M. J., DelValle, R., Sherman, S., & Tansey, T. N. (2014). Methodological application of multiple case study design using modified consensual qualitative research (CQR) analysis to identify best practices and organizational factors in the public rehabilitation program. *Journal of Vocational Rehabilitation, 41*, 87-98. doi:10.3233/JVR-14070

Andrasik, M. P., Chandler, C., Powell, B., Humes, D., Wakefield, S., Kripke, K., & Eckstein, D. (2014). Bridging the divide: HIV prevention research and black men who have sex with men. *American Journal of Public Health, 104*, 708-714. doi:10.2105/ajph.2013.301653

Anney, V. N. (2014). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies, 5*(2), 272-281. Retrieved from jeteraps.scholarlinkresearch.org

Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A focus on qualitative research interview. *Qualitative Report, 18*(18), 130-136. Retrieved from http://www.nova.edu/ssss/QR/index.html

Archambault, P. M., Thanh, J., Blouin, D., Gagnon, S., Poitras, J., Fountain, R., & Légaré, F. (2015). Emergency medicine residents' beliefs about contributing to an online collaborative slideshow. *CJEM:* J*ournal of the Canadian Association of Emergency Physicians, 17*(4), 374-386. doi: 10.1017/cem.2014.49

Ardagna, C. A., Asal, R., Damiani, E., & Vu, Q. H. (2015). From security to assurance in the cloud: A survey. *ACM Computing Surveys, 48*(1), 2-50. doi:10.1145/2767005

Arianyan, E., Ahmadi, M. R., & Maleki, D. (2016). A novel taxonomy and comparison method for ranking cloud computing software products. *International of Grid and Ditributed Computing, 9*(3), 173-190. doi:10.14257/ijgdc.2016.9.3.19

Banerjee, A., & Chaudhury, S. (2010). Statistics without tears: Population and samples. *Industrial Psychiatry Journal, 19*(1), 60-65. doi:10.4103/0972-6748.77642

Barnham, C. (2015). Quantitative and qualitative research. *International Journal of Market Research*, *57*(6), 837-854. doi:10.2501/IJMR-2015-070

Barona, R., & Anita, E. M. (2017, April 20-21). *A survey on data breach challenges in cloud computing security: Issues and threats*. Paper presented at International Conference on Circuit, Power and Computing Technologies (ICCPCT*)*. doi:10.1109/ICCPCT.2017.8074287

Barry, A. E., Chaney, B., Piazza-Gardner, A. K., & Chavarria, E. A. (2014). Validity and reliability reporting practices in the field of health education and behavior: A review of seven journals. *Health Education Behavior, 41*(1), 12-8. doi:10.1177/1090198113483139

Basheer, H. A., Ahmed, A. J., & Wasseem N Ibrahem Al-Obaydy Al-Obaydy. (2020). Data loss prevention (DLP) by using MRSH-v2 algorithm. *International Journal of Electrical and Computer Engineering, 10*(4), 3615-3622. doi:10.11591/ijece.v10i4.pp3615-3622

Baskarada, S. (2014). Qualitative case study guidelines. *The Qualitative Report, 19(40),* 1-25. Retrieved from https://tqr.nova.edu/

Baur, S., & Boche, H. (2018). Robust secure authentication and data storage with perfect secrecy. *Cryptography, 2*(2), 1-29. doi:10.3390/cryptography2020008

Bayramusta, M., & Nasir, V. A. (2016). A fad or future of IT?: A comprehensive literature review on the cloud computing research. *International Journal of Information Management, 36*(4), 635-644. doi:10.1016/j.ijinfomgt.2016.04.006

Becking, J. C. (2016). The future of violence: Robots and germs, hackers and drones-confronting a new age of threat. *Parameters, 46*(3), 117-118. Retrieved https://go.gale.com

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology, 16*(21), 1-12. doi:10.1186/s12874-016-0114-6

Bernsmed, K., Cruzes, D. S., Jaatun, M. G., Haugset, B., & Gjaere, E. A. (2014 Sept 8-14). *Healthcare services in the cloud – Obstacles to adoption , and a way forward*. Paper presented at 2014 Ninth International Conference on Availability, Reliability and Security, Switzerland. doi:10.1109/ARES.2014.28

Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. *International Journal of Computer Applications, 47*(18), 47-66. doi:10.5120/7292-0578

Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2014). Security issues in cloud computing. *Acta Technica Corviniensis - Bulletin of Engineering, 7*(4), 159-177. Retrieved from https://www.ebsco.com

Bhatia, S., & Malhotra, J. (2018). CSPCR: Cloud security, privacy and compliance readiness - A trustworthy framework. *International Journal of Electrical and Computer Engineering, 8*(5), 3756-3766. doi:10.11591/ijece.v8i5.pp3756-3766

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*(13), 1802-1811. doi:10.1177/1049732316654870

Biswas, S., & Sen, J. (2016). A proposed architecture for big data driven supply chain analytics. Journal of Supply Chain Management, XIII(3), 7-34. doi:10.2139/ssrn.2795906

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Reseaerch in Marketing, 01356*, 1-15, doi:10.1016/j.ijresmar.2020.03.006

Bowie, B. H., & Wojnar, D. (2016). Using phenomenology as a research method in community-based research. *Nursing Research Using Phenomenology*. doi:10.1891/9780826126870.0007

Boz, H., & Dagli, Y. (2017). The contribution of qualitative methods for identifying the educational needs of adults. *Cypriot Journal of Educational Science, 12*(4), 167–176. doi:10.18844/cjes.v12i4.2901

Brandas, C., Megan, O., & Didraga, O. (2015). Global perspectives on accounting information systems: Mobile and cloud approach. *Procedia Economics and Finance, 20*, 88–93. doi:10.1016/s2212-5671(15)00051-9

Breaux, R. W., Black, E. W., & Newman, T. (2014). A guide to data protection and breach response: Part 1. *Intellectual Property & Technology Law Journal, 26*, 3-10. Retrieved from https://home.heinonline.org

Cacari-Stone, L., Wallerstein, N. G., & Minkler, M. (2014). The promise of community based participatory research for health equity: A conceptual model for bridging evidence with policy. *American Journal of Public Health, 104*, 1615-1623. doi:10.2105/AJPH.2014.301961

Cachia, M., & Millward, L. (2011). The telephone medium and semistructured interviews: A complementary fit. *Qualitative Research in Organizations and Management: An International Journal, 6*, 265-277. doi:10.1108/17465641111188420

Cahana, A., & Hurst, S. A. (2015). Voluntary informed consent in research and clinical care: An update. *Pain Practice, 8*, 446-451. doi:10.1111/j.1533-2500.2008.00241.x

Cameron, E. A., & Marcum, T. M. (2019). Why business schools must incorporate cybersecurity into the business curriculum: Preparing the next generation for success. *Journal of Higher Education Theory and Practice, 19*(4), 25-33. doi:10.33423/jhetp.v19i4.2199

Carlson, J. A. (2010). Avoiding traps in member checking. *The Qualitative Report, 15*, 1102-1113. Retrieved from https://tqr.nova.edu/

Carre, J. R., Curtis, S. R., & Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal, 33*, 436-446. doi:10/1108/MAJ-11-2017-1693.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*(5), 545-547. doi:10.1188/14.ONF.545-547

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*(5), 811-831. Retrieved from https://tqr.nova.edu/

Catteddu, D. and Hogben, G. (2009), Cloud computing: Benefits, risks and recommendations for information security. *European Network and Information Security Agency (ENISA), 72*(1), 1-125. Retrieved from http://www.springerlink.com

Chanda, K. (2016). Password security: An analysis of password strengths and vulnerabilities. *International Journal of Computer Network and Information Security, 8*(7), 23. doi: 10.5815/ijcnis.2016.07.04

Chan, Z. C. Y., Fung, Y., & Chien, W. (2018). Bracketing in phenomenology: Only undertaken in the data collection and analysis process? *The Qualitative Report, 18*(30), 1-9. Retrieved from https://tqr.nova.edu/

Chang, V., Ramachandran, M., Yao, Y., Kuo, Y., & Li, C. (2016). A resiliency framework for an enterprise cloud. *International Journal of Information Management*, *36*(1), 155–166. doi:10.1016/j.ijinfomgt.2015.09.008

Charlesworth, A., & Pearson, S. (2013). Developing accountability-based solutions for data privacy in the cloud. *Innovation: The European Journal of Social Sciences, 26*(1-2), 7-35. doi:10.1080/13511610.2013.732753

Cheng, H. G., & Phillips, M. R. (2014). Secondary analysis of existing data: Opportunities and implementation. *Shanghai Arch Psychiatry, 26*(6), 371-375. doi:10.11919/j.issn.1002-0829.214171

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIRESs Data Mining and Knowledge Discovery*, *7*(5). 1-14. doi:10.1002/widm.1211

Chidambaram, N., Raj, P., Thenmozhi, K., & Amirtharajan, R. (2016). Enhancing the security of customer data in cloud environments using a novel digital fingerprinting technique. *International Journal of Digital Multimedia Broadcasting, 2016,* 1-6. doi:10.1155/2016/8789397

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2015). Managing ethical challenges to mental health research in post conflict settings. *Developing World Bioethics,16*(1)*,* 15-28. doi:10.1111/dewb.12076

Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *Journal of Marketing Development and Competitiveness, 11*(1), 59-68. Retrieved from https://articlegateway.com

Christensen, M. D. (2015). *OPM data breach: Personnel security background investigation data* (Report No. CRS Insight, IN10327). Library of Congress: Congressional Research Service Reports. Retrieved from www.hsdl.org

Church, R. M. (2001). The effective use of secondary data. *Learning and Motivation, 33*(1), 32-45. doi:10.1006/lmot.2001.1098

Claycomb, W., & Nicholl, A. (2014). Insider threats to cloud computing: Directions for new research challenges. *IEEE 36th Annual Computer Software and Applications Conference, Izmir, Turkey, 2012*. doi:10.1109/compsac.2012.113

Congressional Research Service. (2019). *Data protection law:An overview.* Retrieved from https//www.fas.org

Cooper, D. R., & Schindler, P. S. (2014). *Business research methods* (12th ed.). New York, NY: The McGraw-Hills Companies, Inc.

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society, 1*, 104-126. doi:10.1007/BF03177550

Cooper, J., Borasky, D., Rosenfeld, S., & Sugarman, J. (2016). Challenges in the ethical review of research involving complementary and integrative medicine. *Therapeutic Innovation & Regulatory Science, 50*(3), 337-341. doi:10.1177/2168479015620246

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*(1), 89-91. doi:10.1188/14.ONF.89-91

Creswell, J. W., & Clark, P. (2011). *Designing and conducting mixed method research* (2nd ed). Thousand Oaks, CA: Sage Publishing, Inc.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4thed.). Thousand Oaks, CA: Sage Publishing, Inc.

Crockett, D., Downey, H., Firat, A., Ozanne, J., & Pettigrew, S. (2013). Conceptualizing a transformative research agenda. *Journal of Business Research, 66*(8), 1171-1178. doi:10.1016/j.jbusres.2012.08.009

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *US National Library of Medicine National Institutes of Health, 21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Dahbur, K., Bashabsheh, Z., & Bashabshe, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Mangement Review, 13*(1*),* 37-58. Retrieved from https://www.proquest.com

David, L. C., & Dhillon, G. (2019). Cloud privacy objectives a value based approach. *Information and Computer Security, 27*(2), 189-220. doi:10.1108/ICS-05-2017-0034

Dean, J. (2014). Personal protective equipment: An antecedent to safe behavior. Retrieved from http://www.asse.org

De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. *Future Internet, 11*(6), 1-30. doi:10.3390/fi11060127

Department of Homeland Security. (2015). *Privacy response to potential PII incident*. Retrieved from https://www.dhs.gov/pii

Dincer, C. & Zeydan, E. (2017, June 5-8) *Big data security: Requirements, challenges and preservation of private data inside mobile operators*. Paper presented at 2017 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Turkey. doi:10.1109/BlackSeaCom.2017.8277711

Dolan, A. M. (2015). *Data security and breach notification legislation: Selected legal issues* (CRS Report No. R44326). Retrieved from https://www.crs.gov

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher, 20*(5), 28-32. doi:10.7748/nr2013.05.20.5.28.e327

Dranseika, V., Piasecki, J., & Waligora, M. (2017). Relevant information and informed consent in research: In defense of the subjective standard of disclosure. *Science and Engineering Ethics, 23*, 215-225. doi:10.1007/s11948-016-9755-4

Draper, J. (2015). Ethnography: Principles, practice and potential. *Nursing Standard, 29* (36), 36-41. doi:10.7748/ns.29.36.36.e8937

Duncan, B., & Whittington, M. (2015, 30 Nov – 3 Dec). *The Importance of Proper Measurement for a Cloud Security Assurance Model*. Paper presented at 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*,* Canada. doi:10.1109/CloudCom.2015.91.

Duxbury, T. (2012). Towards more case study research in entrepreneurship. *Technology Innovation Management Review, 2*, 9-17. Retrieved from www.timereview.ca

Dwyer, R., Davis, I., & Emerald, E. (2017). *Narrative research in practice: Stories from the Field*. [Adobe Digital Editions version]. doi:10.1007/978-981-10-1579-3

Dzazali, S., Sulaiman, A., & Zolait, A. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, *26*(4), 584–593. doi:10.1016/j.giq.2009.04.004

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity: An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology, 14*(1), 23-57. doi:10.1108/13287261211221128

Elhaida, J. D., & Frueh, B. C. (2015). Security of electronic mental health communication and record-keeping in the digital age. *The Journal of Clinical Psychiatry,77*(2), 478. doi:10.4088/jcp.14r09506

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. *The Qualitative Report, 23*(11), 2850-2861. Retrieved from https://tqr.nova.edu/

Elo, S., Kääriäinen, M., Kanste, O., Pokka, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open, 4*(1), 1-10. doi:10.1177/2158244014522633

Eloff, M. M., & Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers and Security, 19*(3), 243−256. doi:10.1016/S0167-4048(00)88613-7

Ercan, T. (2010). Effective use of cloud computing in educational institutions. *Procedia – Social and Behavioral Sciences*, 2(2), 938- 942. doi:10.1016/j.sbspro.2010.03.130

Ferng, H.W., & Khoa, N.M. (2017). On security of wireless sensor networks: A data authentication protocol using digital signature. *Wireless Networks, 23*, 1113-1131. doi:10.1007/s11276-016-1208-0

Fok, M. P., Wang, Z., Deng, Y., & Prucnal, P. R. (2011). Optical layer security in fiber-optic networks. *IEEE Transactions on Information Forensics and Security, 6*(3), 725-736. doi:10.1109/TIFS.2011.2141990

Fun, T. S. & Samsudin, A. (2016) A survey of homomorphic encryption for outsourced big data computation. *Transactions on Internet and Information Systems, 10*(8), 3826-3851. doi:10.3837/tiis.2016.08.022

Furdek, M., Skorin-Kapoc, N., Zsigmond, S., & Wosinska, L. (2014, July). *Vulnerabilities and security issues in optical networks*. Paper presented at the 16th International Conference on Transparent Optical Networks (ICTON), Graz Austria. doi:10.1109/ICTON.2014.6876451

Fusch, P. I., & Ness, L. P. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from https://tqr.nova.edu

Gabriele, E. F. (2003). The Belmont ethos: The meaning of the Belmont principles for human subject protections. *Journal of Research Administration, 34*(2), 19-24. Retrieved from https://www.srainternational.org

Garg, P., & Goel, S. (2017). Data security approach in cloud computing by using DOS attack. *International Journal of Information Dissemination and Technology, 7*(3), 196-199. doi:10.5958/2249-5576.2017.00023.1

Gaidhani, D., Koyeerath, J., Kudu, N., & Mehra, M. (2017). A survey report on techniques for data confidentiality in cloud computing using homomorphic encryption. *International Journal of Advanced Research in Computer Science, 8*(8), 389-394. doi:10.26483/ijarcs.v8i8.4746

Ghazizadeh, E., Zamani, M., Manan, J.A., & Alizadeh, M. (2014). Trusted computing strengths cloud authentication. *Scientific World Journal, 2014*. 1-18. doi:10.1155/2014/260187

Ghosh, S., & Sampalli, S. (2019). A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access*, *7*, 135812-135831. doi:10.1109/ACCESS.2019.2926441

Gibson, W., Webb, H., & Lehn, D. V. (2014). Analytic affordance: Transcripts as conventialised systems in discourse. *Sage Journals, 48*(4), 780-794. doi:10.1177/0038038514532876

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15-31. doi:10.1177/1094428112452151

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8*(4), 597-606. Retrieved from https://tqr.nova.edu

Goldberg, E. (2013). Preventing a data breach from becoming a disaster. *Journal of Business Continuity & Emergency Planning, 6*(4), 295-303. Retrieved from https://www.ingentaconnect.com

Gore, R. (2018, March 26-27) *Privacy breach:A concern of cloud integrated IoT framework for smart city*. Paper presented at 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), India. doi:10.2139/ssrn.3170523

Goscinski, A. & Brock, M. (2010). Toward dynamic and attribute based publication, discovery and selection for cloud computing. *Future Generation Computer Systems, 26*(7), 947-70. doi:10.1016/j.future.2010.03.009

Goyal, S. (2014). Public vs. private vs. hybrid vs. community-cloud computing: A critical review. *International Journal of Computer Network and Information Security, 3,* 20-29. doi:10.5815/ijcnis.2014.03.03

Granneman, J. (2018). The business guide to improving information security. Journal of Equipment Lease Financing, *36*(3), 1-9. Retrieved from https://www. Leasefoundation.org

Guetterman, T. C. (2015). Descriptions of sampling practices within five approaches to qualitative research in education and the health sciences. *Forum: Qualitative Social Research, 16*(2), 1-23. doi:10.17169/fqs-16.2.2290

Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: A taxonomy. *Complex Adaptive Systems Modeling, 2*(5), 1-37. doi:10.1186/s40294-014-0005-9

Harper, C., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report, 17*(2), 510-517. Retrieved from https://nsuworks.nova.edu

Hashem, I.A., Yaqoob, I., Anuar, N.B., Mohktar, S., Gani, A., & Khan,S.U. (2014). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47*(2015), 98-115. doi:10.1016/j.is.2014.07.0006

Haydon, G., Browne, G., & van der Riet, P. (2018). Narrative inquiry as a research methodology exploring person centred care in nursing. *Collegian, 25*(1), 125-129. doi:10.1016/j.colegn.2017.03.001

Hayes, B., Bonner, A., & Douglas, C. (2013). An introduction to mixed methods research for nephrology nurses. *Renal Society of Australasia Journal, 9*(1), 8-14. Retrieved from http://www.renalsociety.org

Hentea, M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management*, 3, 73–86. Retrieved from https://www.informingscience.org

Holloway, I., & Wheeler, S. (2013). *Qualitative research in nursing and healthcare.* Oxford, United Kingdom: John Wiley & Sons.

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242-260. doi:10.1108/JFC-09-2013-0055

Hong, K.S., Chi, Y.P., Chao, L. R., & Tang, J.H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248. doi:10.1108/09685220310500153

Hong, K.S., Chi, Y.P., Chao, L. R., and Tang, J.H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104– 115. doi:10.1108/09685220610655861

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigor in qualitative case-study research. *Nurse Researcher, 20*(4), 12-17.doi:10.7748/nr2013.03.20.4.12.e326

Huang, D.L., Rau, P.L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies, *69* (12). 870-883. doi:10.1016/j.ijhcs.2011.07.007

Hunt, L. (2014). In defense of qualitative research. *Journal of Dental Hygiene, 88*(2), 64-65. Retrieved from http://jdh.adha.org

Hurmerinta, L., & Nummela, N. (2016). Mixed-method Case Studies in International Business Research. *Rethinking the Case Study in International Business and Management Research, 12*, 210-217. doi:10.4337/9780857933461.00021

Hustad, E., Bekkevik, F. M., Holm, O. R., & Vassilakopoulou, P. (2020). Employee information security practices: A framework and research agenda. *International Journal of E-Services and Mobile Applications (IJESMA), 12*(2), 1-14. doi:10.4018/IJESMA.2020040101

Igure, V. M., Laughter, S. A., & Willams, R. D. (2006). Security issues in SCADA networks. *Computers & Security, 25*(7), 498-506. doi:10.1016/j.cose.2006.03.001

Irvine, A., Drew, P., & Sainsbury, R. (2013). Am I not answering your questions properly? Clarification, adequacy and responsiveness in semistructured telephone and face-to-face interviews. *Qualitative Research, 13*(1), 87-106. doi:10.1177/1468794112439086

Ishak, N. M., & Bakar, A. Y. A. (2014). Developing sampling frame for case study: Challenges and conditions. *World Journal of Education, 4*(3), 29-35. doi:10.5430/wje.v4n3p29

Ismail, S., Sitnikova, E., & Slay, J. (Eds.) (2015). *Studying SCADA organisations information security goals: An integrated system theory approach*. Proceedings of the Pacific Asia Conference on Information Systems, Xiamen, China. Retrieved from http://aisel.aisnet.org/pacis2015/77

Ismail, S., Sitnikova, E., & Slay, J. (2014a). Towards developing SCADA systems security measures for critical infrastructures against cyber-terrorist attacks. *ICT Systems Security and Privacy Protection, 428*, 242–249. doi:10.1007/978-3-642-55415-5_20

Ismail, S., Sitnikova, E., & Slay, J. (2014b, Aug 19-21). *Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures : A pilot study*. Paper presented at the 11th International Conference on Fuzzy Systems and Knowledge Discovery, Xiamen, China. doi:10.1109/FSKD.2014.6980976

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of Big Data, 3*(25), 1-25. doi:10.1186/s40537-016-0059-y

Jamshed, S. (2014). Qualitative research method – Interviewing and observation. *Journal of Basic and Clinical Pharmacy, 5*(4), 87-88. doi:10.4103/0976-0105.141942

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*(5), 332–349. doi:10.1108/09685221211286511

Jawad, M. A. (2018). Cloud computing: Major challenges and counter acts. *International Journal of Advanced Research in Computer Science, 9*(2), 618-625. doi:10.26483/ijarcs.v9i2.5861

Joan, R. (2014). Basic information about cloud computing related to modern situation. *I-manager's Journal on Cloud Computing, 1*(2), 7-12. doi:10.26634/jcc.1.2.3051

Johnston, M. P. (2014). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries, 3*, 619-626. Retrieved from www.qqml-journal.net

Kahle-Piasecki, L., Ritzman, M. E., & Ellingson, D. (2017). Up in the cloud: Managers, employees, and security training for cloud computing to avert cyber threats. *American Journal of Management, 17*(7), 58-63. doi:10.33423/ajm.v17i7.1703

Kajiyama, T., Jennex, M., & Addo, T. (2017). To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. *Information and Computer Security, 25*(11), 634-659. doi:10.1108/ICS-07-2016-0051

Kalaiprasath, R., Elankavi, R., Udayakumar (2017). Cloud security and compliance – A semantic approach in end to end security. *International Journal of Mechanical Engineering and Technology (IJMET), 8*(5), 987–994. Retrieved from http://www.iaeme.com

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces, 36*(4), 759–775. doi:10.1016/j.csi.2013.12.010

Kasemsap, K. (2015). The role of cloud computing adoption in global business. *IGI Global, 3*, 26-55. doi:10.4018/978-1-4666-8210-8.ch002

Kaur, A., & Kaur, R. (2018). Cloud computuing: A focus on security issues in cloud computing region. *International Journal of Advanced Research in Computer Science, 9*(2), 267-269. doi:10.26483/ijarcs.v9i2.5556

Kaur, A.A, & Mustafa, K.K. (2019). A critical appraisal on password based authentication. *I.J. Computer Network and Information Security, 1*, 47-61. doi:10.5815/ijcnis.2019.01.05

Kaur, S., Sood, S., & Kaur, G. (2017). Cloud computing interoperability: Introduction, concerns and challenges. *International Journal of Advanced Research in Computer Science, 8*(5)*,* 939-943. doi:10.26483/ijarcs.v8i5.3499

Kazim, M., & Ying, S. (2015). A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications, 6*(3)*,*109-113. doi:10.14569/ijacsa.2015.060316

Ke, C., Huang, Z., Xiao, F., Liu, L. (2017). Privacy data decomposition and discretization method for SaaS Services. *Mathematical Problems in Engineering, 2017*, 1-11. doi:10.1155/2017/4785142

Khan, M.A. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications, 71*, 11-29. doi:10.1016/j.jnca.2016.05.010

Khan, S. (2019). Cloud computing: Issues and risks of embracing the cloud in a business environment. *International Journal of Education and Management Engineering, 9*(4), 44-56. doi:10.5815/ijeme.2019.04.05

Khan, S. N. (2014). Qualitative research method - phenomenology. *Asian Social Science, 10*(21), 298-310. doi:10.5539/ass.v10n21p298

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2019). Data and privacy: Getting consumers to trust products enabled by the internet of things. *IEEE Consumer Electronics Magazine, 8*(2), 35-38. doi:10.1109/MCE.2018.2880807

Kilani, Y.. (2020). Cyber-security effect on organizational internal process: Mediating role of technological infrastructure. *Problems and Perspectives in Management, 18*(1), 449-460. doi:10.21511/ppm.18(1).2020.39

Kilhan, S., Simoens, K., De Cock, D., Eekelen, M., & Vranken, H. (2016). A survey of authentication and communications security in online banking. *ACM Computing Surveys, 49*, 61-61:35. doi:10.1145/3002170

Kim, H., & Song, Y. (2018). An integrated measure of accessibility and reliability of mass transit systems. *Transportation, 45*(4), 1075-1100. doi:10.1007/s11116-018-9866-7

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review, 28*(3), 308–319. doi:10.1016/j.clsr.2012.03.003

Kouatli, I. (2014). A comparative study of the evolution of vulnerabilities in IT systems and its relation to the new concept of cloud computing. *Journal of Management History, 20*(4), 409-433. doi:10.1108/JMH-02-2014-0018

Kovaliuk, D. O., Huza, K. M., & Kovaliuk, O. O. (2018). Development of SCADA system based on web technologies. *International Journal of Information Engineering and Electronic Business, 10*, 25. doi:10.5815/ijieeb.2018.02.04

Ksherti, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134-1145. doi:10.1016/j.telpol.2014.10.002

Kumar, A., Kumar, V., Singh, P., & Kumar, A. (2012) A novel approach: Security measures and concerns of cloud computing. *Int.J. Computer Technology & Applications, 3*(3), 1008-1014. Retrieved from www.ijcta.com

Kushida, K. E., Murray, J. & Zysman, J. (2011). Diffusing the cloud: cloud computing and implications for public policy. *Journal of Industry Competition and Trade, 11*, 209–237. doi:10.1007/s10842-011-0106-5

Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud computing: From scarcity to abundance. *Journal of Industry, Competition and Trade, 15*, 5-19. doi:10.1007/s10842-014-0188-y

Lafuente, G. (2015). The big data security challenge. *Network Security, 2015*(1), 12-14. doi:10.1016/S1353-4858(15)70009-7

Lainie, F. R. (2006). What is wrong with the physician charter on professionalism. *The Hastings Center Report, 36*(4), 17-19. doi:10.1353/hcr.2006.0066

Lakshmi, L. (2017). Encryption schemes in cloud computing – A comprehensive study. *International Journal of Advanced Research in Computer Science, 8*(5), 170-175. doi:10.26483/ijarcs.v8i5.3264

Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. *IEEE Communications Magazine*, *55*(8), 211-217. doi:10.1109/MCOM.2017.1600899.

Langley, A., & Klag, M. (2017). Being where? Navigating the involvement paradox in qualitative research accounts. *Organizational Research Methods*, *19*(2), 1-24. doi:10.1177/1094428117741967

Lazarova, V. (2016). Managing user access to cloud services by company administrators. *TEM Journal, 5*(3), 289-293. doi:10.18421/TEM53-06

Leavitt, N. (2009). Is cloud computing really ready for prime time? IEEE Computer Society, 42(1), 15-20. Retrieved from www.engr.sjsu.edu

Leavy, P. (2017). *Research design: Quantitative, qualitative, mixed methods, arts-based and community-based participatory research approaches*. New York, NY: The Guilford Press.

Lee, W.W., Zankl, W., & Chang, H. (2016) An ethical approach to data privacy protection. *ISACA Journel, 6*, 1-9. Retrieved from www.isaca.org

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design.* New York, NY: Pearson.

Li, J., Chen, X., Li, M., Li, J., Lee, P. P., & Lou, W. (2014). Secure deduplication with efficient and reliable convergent key management. *Parallel and Distributed Systems, IEEE Transactions*, *25*(6), 1615–1625. doi:10.1109/tpds.2013.284

Li, Q., Zhao, J., Gong, Y., & Zhang, Q. (2019). Energy-efficient computation offloading and resource allocation in fog computing for the Internet of everything. *China Communications*, *16*(3), 32-41. Retrieved from https://ieeexplorer.ieee.org

Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*(1), 28–36. doi:10.1016/j.ijinfomgt.2013.09.004

Liu, Y., Sheng, X., & Marston, S. R. (2015). The impact of client-side security restrictions on the competition of cloud computing services. *International Journal of Electronic Commerce*, *19*(3), 90–117. doi:10.1080/10864415.2015.1000224

Lohle, M. F., & Terrell, S. R. (2014). Real projects, virtual worlds: Coworkers, their avatars, and the trust conundrum. *The Qualitative Report, 19*, 1-35. Retrieved from http://nsuworks.nova.edu

Lu, R., Zhu, H., Liu, X., Liu, J., & Shao, J. (2014). Toward efficient and privacy-preserving computing in big data era. *Network IEEE, 28*(4), 46-50. doi:10.1109/MNET.2014.6863131

Lueng, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4*(3), 324-327. doi:10.4103/2249-4863.161306

Luo, X., Zhang, W., Li, H., Bose, R., & Chung, Q. B. (2018). Cloud computing capability: Its technological root and business impact. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 193-213. doi:10.1080/10919392.2018.1480926

Lv, J., Wang, Y., & Liu, J. (2019 November 8-10). *A security problem in cloud auditing protocols*. Paper presented at 2019 International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI*)*, China. doi:10.1109/MLBDBI48998.2019.00016

Majumdar, S., (2019 November 18-20). *Multi-level proactive security auditing for Clouds*. Paper presented at 2019 IEEE Conference on Dependable and Secure Computing (DSC), China. doi: 10.1109/DSC47296.2019.8937641.

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research, 26*(13), 1753-1760. doi:10.1177/104973231561744

Mancini, F., Coghill, G. M., & Lusseau, D. (2017). Using qualitative models to define sustainable management for the commons in data poor conditions. *Environmental Science & Policy, 67*, 52-60. doi:10.1016/j.envsci.2016.11.002

Manral, B., Somani, G., Choo, K. K. R., Conti, M., & Gaur, M. S. (2020). A systemic survey on cloud forensics challenges, solutions, and future directions. *ACM Computing Surveys, 52*(6), 1-38. doi:10.1145/3361216

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the target data breach. *Business Horizons*, *59*(3), 257-266. doi:10.1016/j.bushor.2016.01.002

Marchisotti, G.G., Joia, L.A., & De Carvalho, R.B. (2019). The social representation of cloud computing according to Brazilian information technology professionals. R*evista De Administração De Empresas, 59*(1), 16-28. doi:10.1590/S0034-759020190103

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in is research. *Journal of Computer Information Systems, 54*(1), 11-22. doi:10.1080/08874417.2013.11645667

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing: The business perspective. *Decision Support Systems, 51*(1), 176–189. doi:10.1016/j.dss.2010.12.006

Masrom, M., & Rahimli, A. (2015). Cloud computing adoption in the healthcare sector: A SWOT analysis. *Asian Social Science, 11*(10), 12-18. doi:10.5539/ass.v11n10p12

Maylor, H., & Blackmon, K. (2015). Analyzing qualitative data. *Researching Business and Management, 25,* 343-367. doi:10.1007/978-1-137-11022-0

McAlpine, L. (2016). Why might you use narrative methodology? A story about narrative. *Eesti Haridusteaduste Ajakiri, 4*, 32-57. doi:10.12697/eha.2016.4.1.02b

Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G., & Guo, S. (2016). Protection of big data privacy. *IEEE Access, 4*, 1821-1834. doi:10.1109/ACCESS.2016.2558446

Mehran, N., & Khayyambashi, M. R. (2017). Performance evaluation of authentication-encryption and confidentiality block cipher modes of operation on digital image. *International Journal of Computer Network and Information Security, 11*(9), 30-37. doi:10.5815/ijcnis.2017.09.04

Meinecke, A. K., Welsing, P., Kafatos, G., Burke, D., Trelle, S., Kubin, M., … (2017). Series: Pragmatic trials and real world evidence: Paper 8. Data collection and management. *Journal of Clinical Epidemiology, 91*, 13-21. doi:10.1016/j.jclinepi.2017.07.003

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology, 53*(6), 50. Retrieved from https://csrc.nist.gov

Meyers, G., & Lampropoulou, S. (2013). What place reference can do in social research interviews. *Sage Journals, 15*(3), 333-351. doi:10.1177/1461445613480589

Miyan, M. (2017). FHE implementation of data in cloud computing. *International Journal of Advanced Research in Computer Science, 8*(3) Retrieved from www.ijarcs.info

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of cloud computing. *The Journal of Supercomputing, 63*, 561-592. https://doi.org/10.1007/s11227-012-0831-5

Mohlameane, M., & Ruxwana, N. (2014). The awareness of cloud computing: A case study of South African SMEs. *International Journal of Trade, Economics, and Finance, 5*(1), 6-11. doi:10.7763/IJTEF.2014.V5.332

Moysiadis, V., Sarigiannidis, P., & Moscholios, I. (2018). Towards distributed data management in fog computing. *Wireless Communications & Mobile Computing*, *2018*, 14. doi:10.1155/2018/7597686

Naik, N. & Jenkins, P. (2016, 29 March – 1 April). *A secure mobile cloud identity: Criteria for effective identity and access management standards.* Paper presented at the IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. United Kingdom. doi:10.1109/MobileCloud.2016.22

Nikou, S.A., & Economides, A.A. (2017). Mobile-based assessment: Investigating the factors that influence behavioral intention to use. *Computers & Education, 109*, 56-73. doi:10.1016/j.compedu.2017.02.005

Nowell, L.S., Norris, J.M., White, D.E., and Moules, N.J. (2017) Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*, 1-13. doi:10.1177/1609406917733847

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014, May 17-18). *Understanding insider threat: A framework for characterizing attacks*. Paper presented at the IEEE Security and Privacy Workshops, San Jose, CA. doi:10.1109/spw.2014.38

O'Cathain, A. (2018). Frameworks, study designs, and guidance. *Oxford Medicine Online*. doi:10.1093/med/9780198802082.003.0002

O'Cathain, A., & Thomas, K. (2015). Combining qualitative and quantitative methods. *Qualitative Research in Health Care*, *9*, 102-111. doi:10.1002/9780470750841.ch9

O'Connor, H., & Gibson, N. (2003). A step-by-step guide to qualitative data analysis. *A Journal of Aboriginal & Indigenous Community Health, 1*, 63-90. Retrieved from http://www.pimatisiwin.com

O'Keeffe, J., Buytaert, W., Mijic, A., Brozovic, N., & Sinha, R. (2016). The use of semi-structured interviews for the characterisation of farmer irrigation practices. *Water for Food Faculty Publications, 33,* 1911-1924. doi:10.5194/hess-20-1911-2016

Olusegun, O.J., & Ithnin, N.B. (2013). People are the answer to security: Establishing a sustainable information security awareness training (ISAT) program in organization. *International Journal of Computers Science and Information Security, 11*, 1-8. retrieved from www.arXiv.org

Onen, D. (2016). Appropriate Conceptualization: The foundation of any solid quantitative research. *Electronic Journal of Business Research Methods, 14*(1), 28. Retrieved from http://www.ejbrm.com

Ormona, J. (2013). Sampling in qualitative research: Improving the quality of research outcomes in higher education. *Makerere Journal of Higher Education, 4*(2), 169-185. doi:10.4314/majohe.v4i2.4

Ouahman, A. A. (2014). Security and privacy issues in cloud computing. *Journal of Defense Resources Management, 5*, 99-108. Retrieved from http://www.jodrm.eu

Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S., & Dubois, E. (2015). Security transparency: The next frontier for security research in the cloud. *Journal of Cloud Computing, 4*(12), 1-14. doi:10.1186/s13677-015-0037-5

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration Policy in Mental Health and Mental Health Services Research, 42*, 533-544. doi: 10.1007/s10488-013-0528-y

Pacho, T. O. (2015). Exploring participants' experiences using case study. International *Journal of Humanities and Social Science, 5*(4), 44-53. Retrieved from http://www.ijhssnet.com/

Panah, A., Panah, A., Panah, O., & Fallahpour, S. (2014). Challenges of security issues in cloud computing layers. *Report and Opinion, 4*(10), 25-29. Retrieved from www.sciencepub.net

Pandve, H. T. (2016). Qualitative research in ergonomics: An added advantage. Journal of Ergonomics, 6(2), 1. doi:10.4172/2165-7556.1000e150

Parakh, A. & Kak, S. (2009). Online data storage using implicit security. *Information Sciences, 179*(9), 3323-3331. doi:10.1016/j.ins.2009.05.013

Patton, M. (1990). *Qualitative evaluation and research methods* (2nd ed.).
Beverly Hills, CA: Sage.

Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). Thousand Oaks, CA: Sage.

Pearson, S., Shen, Y., & Mowbray, M. (2009). A privacy manager for cloud computing. *Cloud Computing, 5931*, 90-106. doi:10.1007/978-3-642-10665-1_9

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report, 20*(2), 76-85. Retrieved from http://nsuworks.nova.edu

Pinheiro, A., Canedo, E. D., De Sousa Junior, R. T. De Oliveira Albuquerque, R., Garcia Villalba, L. J., & Tai-Hoon, K. (2018). Security architecture and protocol for trust verifications regarding the integrity of files in cloud services. *Sensors, 18*(3), 753. doi:10.3390/s18030756

Piplode, R., & Singh, U.K. (2012). An overview and study of security issues & challenges in cloud computing. *International journal of advanced research in computer science and software engineering, 2*(1), 115-120. Retrieved from www.ijarcsse.com

Pitropakis, N., Lyvas, C., & Lambrinoudakis, C. (2017). The greater the power, the more dangerous the abuse: Facing malicious insiders in the cloud. *Cloud Computing 2017*, 156-160. Retrieved from https://www.researchgate.net

Poresky, C., Andreades, C., Kendrick, J., & Peterson, P. (2017). Cyber security in nuclear power plants: Insights for advanced nuclear technologies. Department of Nuclear Engineering, University of California, Berkeley, Publication UCBTH-17-004. Retrieved from https://www.researchgate.net

Pratt, B., & Loizos, P. (2015). Choosing research methods. *Oxfam Development Guidelines*, 5-120. doi:10.3362/9780855986803.001

Pugazhenthi, A., & Chitra, D. (2019). Data access control and secured data sharing approach for health care data in cloud environment. *Journal of Medical Systems, 43*(8), 1-9. doi:10.1007/s10916-019-1381-7

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management, 8*(3), 238-264. doi:10.1108/11766091111162070

Rajamanickam, S., Vollala, S., Amin, R. & Ramasubramanian, N. (2020) Insider attack protection: Lightweight password-based authentication techniques using ECC. *IEEE Systems Journal, 14*(2), 1972-1983. doi:10.1109/JSYST.2019.2933464.

Ranney, M. L., Meisel, Z., Choo, E. K., Garro, A., Sasson, C., & Morrow, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis, and results, reporting. *Research Methods & Statistics, 22*(9), 1103-1112. doi:10.1111/acem.12735

Ranz, R. (2018). More than knowledge: using reading diaries and case studies in an international social work course. *Social Work Education*, *38*(3), 1-12. doi:10.1080/02615479.2018.1504912

Renwick, S. L., & Martin, K. M. (2017). Practical architectures for deployment of searchable encryption in a cloud environment. *Cryptography, 1*(3), 1-17. doi:10.3390/cryptography1030019

Resnik, D. B. (2014). What is ethics in research & why is it important. *National Institute of Environmental Health Sciences*. Retrieved from https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm

Rejin, P. R., & Paul, R. D. (2019). Verification of data integrity and co-operative loss recovery for secure data storage in cloud computing. *Cogent Engineering, 6*(1), 1-12. doi:10.1080/23311916.2019.1654694

Riad, K., & Ke, L. (2018). Secure storage and retrieval of IoT data based on private information retrieval. *Wireless Communication and Mobile Computing, 2018*, 1-8. doi:10.1155/2018/5452463

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research*, *10*, 281-305. doi:10.1007/s40685-017-0045-z

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*(1), 25-41. doi:10.1080/14780887.2013.801543

Rosenberg, J. M., & Koehler, M. J. (2015). Context and technological pedagogical content knowledge (TPACK): A systematic review. *Journal of Research on Technology in Education, 47*(3), 186–210. doi:10.1080/15391523.2015.1052663

Roy, A., Sarkar, S., Ganesan, R., & Goel, G. (2015). Secure the cloud: From the perspective of a service-oriented organization. *ACM Computing Surveys (CSUR)*, *47*(3), 41. doi:10.1145/2693841

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy, 12*(5), 16–26. doi:10.1109/msp.2014.89

Rule, P., & John, V. M. (2015). A necessary dialogue: Theory in case study research. *International Journal of Qualitative Methods, 14*(4), 1-11. doi:10.1177/160940691561157

Rutberg, S., & Bouikidis, C.D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal, 45*(2), 209- 212. Retrieved from http://www.homeworkgain.com

Saeed, M. Y., & Khan, M. N. A. (2015). Data protection techniques for building trust in cloud computing. *I.J. Modern Education and Computer Science, 7*(8), 38-47. doi:10.5815/ijmecs.2015.08.05

Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: State of the art and future challenges. *Journal of Medical Systems, 40*(155), 1-16. doi:10.1007/s10916-016-0509-2

Sandelowski, M. (2000). Combining qualitative and quantitative sampling, data collection, and analysis techniques in mixed-method studies. *Research in Nursing & Health, 23*, 246-255. doi:10.1002/1098-240X(200006)23:3<246::AID_NUR9>3.0.CO;2-H

Sandelowski, M. (2014). A matter of taste: Evaluating the quality of qualitative research. *Nursing Inquiry, 22*(2), 86-94. doi:10.1111/nin.12080

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B.,… Jinks, C. (2017). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 52*, 1893-1907. doi:10.1007/s11135-017-0574-8

Scheibe, M., Reichelt, J., Bellmann, M., & Kirch, W. (2015). Acceptance factors of mobile apps for diabetes by patients aged 50 or older: A qualitative study. *Medicine 2.0*, *4* (1), E1. doi:10.2196/med20.3912

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 3(2)*, 314-341. doi:10.1080/07421222.2015.1063315

Shaik, K., Kumar, N. S., Rao, T. V. (2017). Implementaion of Encryption Algorithm for data security in cloud computing. International Journal of Advanced Research in Computer Science, 8(3), 579-583. Retrieved from www.ijarcs.info

Sharma, S. (2017). A review of security of data storage and retrieval on cloud using homomorphic encryption. *International Journal of Advanced Research in Computer Science, 8*(5), 796-800. doi:10.26483/ijarcs.v8i5.3425

Sharma, P.. K., Kaushik, P. S., Agarwal, P., Jain, P., Agarwal, S., & Dixit, K. (2017 October 19-21). *Issues and challenges of data security in a cloud computing environment.* Paper presented at *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, New York. doi: 10.1109/UEMCON.2017.8249113.

Siddiqui, N. A., Rabidas, V. N., Sinha, S. K., Verma, R. B., Pandey, K., Singh, V. P., & Das, P. (2016). Snowball vs. house-to-house technique for measuring annual incidence of kala-azar in the higher endemic blocks of Bihar, India: A comparison. *PLoS Neglected Tropical Diseases, 10*(9), 1-15. doi:10.1371/journal.pntd.0004970

Silva, E. A., Silva, V. G., Lucrédio, D., & Fortes, R. P. (2013 Oct 7-11). *Towards a model-driven approach for promoting cloud PaaS portability.* Paper presented at *2013 XXXIX Latin American Computing Conference (CLEI)*, Venezuela. doi: 10.1109/CLEI.2013.6670667.

Silva, L. V., Barbosa, P., Marinho, R., & Brito, A. (2018). Security and privacy aware data aggregation on cloud computing. *Journal of Internet Services and Applications, 9*(1), 1-13. doi: 10.1186/s13174-018-0078-3

Sims, J. M. (2010). A brief review of the Belmont Report. *Dimensions of Critical Care Nursing, 29*(4), 173-174. doi:10.1097/DCC.0b013e3181de9ec5

Sindhuja, P. (2014). Impact of information security initiatives on supply chain performance: An empirical investigation. *Information Management & Computer Security*, *22*(5), 450-473. doi:10.1108/IMCS-05-2013-0035

Sindhuja, P., & Kunnathur, A. S. (2015). Information security in supply chains: A management control perspective. *Information & Computer Security*, *23*, 476-496. doi:10.1108/ICS-07-2014-0050

Singh, S. K., & Singh, D. K. (2017). Cloud computing: Security issues and challenges. *International Journal of Advances in Engineering & Technology, 10*, 338-343. Retrieved from https://www.ijaet.org

Smith, G. S. (2016). Evaluating materiality in cybercrime footnotes. *Journal of Corporate Accounting and Finance, 27*(2), 77–87. doi:10.1002/jcaf.v27.2

Sokolova, M., & Matwin, S. (2016). Personal privacy protection in time of big data. *Challenges in Computational Statistics and Data mining, 605*, 365-380. doi:10.1007/978-3-319-18781-5_18

Solms, S. H. (2005). Information security governance – Compliance management vs operational management. *Computers & Security, 24*(6), 443-447. doi:10.1016/j.cose.2005.07.003

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Steen, J., DeFillippi, R., Sydow, J., Pryke, S., Michelfelder, I. (2018). Projects and networks: Understanding resource flows and governance of temporary organizations with quantitative and qualitative research methods. *Project Management Journal, 49*(2), 3-17. doi:10.1177/875697281804900201

Stirling, C. M., Dwan, C. A., & McKenzie, A. R. (2014). Why carers use adult day respite: A mixed method case study. *BMC Health Services Research*, *14*(1), 1-8. doi:10.1186/1472-6963-14-245

Stuckey, H. L. (2013). Three types of interviews: Qualitative research methods in social health. *Methodological Issues in Social Health and Diabetes Research, 1*(2), 56-59. doi:10.4103/2321-0656.115294

Stuckey, H. L., Kraschnewski, J. L., Miller-Day, M., Palm, K., Larosa, C., & Sciamanna, C. (2014). "Weighing" two qualitative methods: Self-report interviews and direct observations of participant food choices. *Field Methods, 26*(4), 343-361. doi:10.1177/1525822X14526543

Suguma, R., & Raja, K. (2018). Data security and data privacy in cloud computing environment using data obfuscation technique. *International Journal of Advanced Studies in Computers, Science, and Engineering, 7*(3), 24-29. Retrieved from www.ijcsma.com

Sultan, N. (2013). Cloud computing: A democratizing force? *International Journal of Information Management*, *33*(5), 810-815. doi:10.1016/j.ijinfomgt.2013.05.010

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks, 10*(7), 1-9. doi:10.1155/2014/190903

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy, 68*, 226-231. Retrieved from https://www.cjhp-online.ca

Tabrizchi, H., Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(7), 4771 – 4880. doi:10.1007/s11227-020-03213-1

Tai, L. (2015). The impact of corporate governance on the efficiency and financial performance of GCC National banks. *Middle East Journal of Business, 10*, 12-16. doi:10.5742/mejb.2015.92594

Talesh, S.A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry, 43*(2), 417-440. doi:10.1111/lsi.12303

Tasevski, P. (2016). IT and cyber security awareness-raising campaigns. *Information & Security, 34*(1), 7-22. doi:10.11610/isij.3401

Teiceira, C., Pinto, J.S., Azevedo, R., Batista, T., & Monteiro, A. (2014). The building blocks of a PaaS. *J network system management, 22*, 75-99. doi:10.1007/s10922-012-9260-2

The Council of Economic Advisors. (2018). *The cost of malicious cyber activity to the U.S. economy.* Retrieved from https://www.whitehouse.gov

Theron, P. M. (2015). Coding and data analysis during qualitative empirical research in practical theology/kodering en data-analise tydens kwalitatiewe empiriese navorsing in praktiese teologie. *In Die Skriflig, 49*(3), 1-9. doi:10.4102/ids.v49i3.1880

Thomas, P.Y. (2011). Cloud computing: a potential paradigm for practising the scholarship of teaching and learning. *The Electronic Library, 29*(2), 214-224. doi:10.1108/02640471111125177

Tianfield, H. (2012, October 14-17). *Security issues in cloud computing*. Paper presented at 2012 IEEE International Conference on Systems, Man, and Cybernetics. South Korea. doi:10.1109/ICSMC.2012.6377874

Toma, M., & Leuca, S. (2018). Approaches to providing security data in quality management. *Journal and Science Today, 16*(2), 42-49. Retrieved from www.ceeol.com

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review, 15*(4), 404-428. doi:10.1177/1534484316671606

Trafimow, D. (2014). Considering quantitative and qualitative issues together. *Qualitative Research in Psychology, 11*(1), 15-24. doi:10.1080/14780887.2012.743202

Tsene, L. (2016). *Qualitative multi-method research: Media social responsibility*. Sage Research Methods Cases.

Tyagi, M., Manoria, M., & Mishra, B. (2019, November 1-5). *An enhanced access control and data security framework for cloud application*. Paper presented at 2019 Internationl Conference on Electrical, Electronics and Computer Engineering (UPCON), India. doi:10.1109/UPCON47278.2019.8980079

Udendhran, R. (2017). A hybrid approach to enhance data security in cloud storage. *Association for Computing Machinery, 90*, 1-6. doi:10.1145/3018896.3025138

Upadhyay, D., Sampalli, S., & Plourde, B. (2020). Vulnerabilities' assessment and mitigation strategies for the small linux server, onion omega2. *Electronics, 9*(6), 1-14. doi:10.3390/electronics9060967

Valerio, M. A., Rodriguez, N., Winkler, P., Lopez, J., Dennison, M., & Liangrbara, Y. J. T. (2016). Comparing two sampling methods to engage hard-to-reach communities in research priority setting. *BMC Medical Research Methodology, 16*(146), 1-11. doi:10.1186/s12874-016-0242-z

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21-54. doi:10.25300/MISQ/2013/37.1.02

Vijayalakshmi, M.M., Pradeep. S. (2013). Implementation of secure cloud storage gateway using symmetric key algorithm. *IOSR Joournal of Computer Engineering, 12*(6), 87-90. Retrieved from www.iosrjournals.org

Villaronga E.F., & Millard, C. (2019). Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cybver-physical ecosystems. *Robotics and Autonomous Systes, 119*, 77-91. doi:10.1016/j.robot.2019.06.003

Wang, L., Song, H, & Liu, H. (2016). A novel hybrid color image encryption alogrithim using two complex chaotic systems. *Optics and Lasers in Engineering, 77*, 118-125. doi:10.1016.j.optlaseng.2015.07.015

Wara, Y. M., & Singh, D. (2015). A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). *African Journal of Computing & ICT, 8*, 1-8. Retrieved from http://www.ajocict.net

Wazid, M., Das, A.K., Hussain, R., Succi, G., & Rodrigues, J.J. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. *Journal of Systems Architecture, 97*, 185-196. doi:10.1016/j.sysarc.2018.12.005

Wei, j., Zhou, A., Yuan, J., & Yan, F. (2018). Aiming: Resource allocation with latency awareness for federated-cloud applications. *Wireless Communications & Mobile Computing, 2018*, 1-13. doi:10.1155/2018/4593208

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, *258*, 371–386. doi:10.1016/j.ins.2013.04.028

Wei-Wen, W., Lan, L. W., & Yu-Ting, L. (2013). Factors hindering acceptance of using cloud services in university: A case study. *The Electronic Library, 31*(1), 84–98. doi:10.1108/02640471311299155

Weinbaum, R. K., & Onwuegbuzie, A. J. (2016). Getting more out of your interview data: Toward a framework for debriefing the transcriber if interviews. *Journal of Educational Issues, 2*(1), 248-264. doi:10.5296/jei.v2i1.9216

Weiss, N. E., & Miller, R. S. (2015). *The target and other financial data breaches: Frequently asked questions* (Report No. R43289). Washington, D.C.: Library of Congress: Congressional Research Service. Retrieved from https://digital.library.unt.edu

Wheatley, A. (2014). Do-it-yourself privacy: The need for comprehensive federal privacy legislation with a private right of action. *Golden Gate University Law Review, 45*, 265-286. Retrieved from http://digitalcommons.law.ggu.edu

Wheeler, A., & Winburn, M. (2015). *Cloud storage security: A practical guide*. Amsterdam, Netherlands: Elsevier.

White, P. (2017). Where do research questions come from? *Developing Research Questions*, 1-37. doi:10.1057/978-1-137-49048-3_1

Widodo, H. P. (2014). Methodological considerations in interview data transcription. *International Journal of Innovation in English Language Teaching and Research, 3*, 101-107. Retrieved from http://www.novapublishers.org

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management, 5*, 1-5. Retrieved from https://perspectives.ahima.org/

Wilerson, J. M., Iantaffi, A., Grey, J. A., Bockting, W. O., & Rosser, B. R. (2014). Recommendations for Internet-based qualitative health research with hard-to-reach populations. *Qualitative Health Research, 24*(4), 561-574. doi:10.1177/1049732314524635

Wilshusen, G. C. (2015). *Recent data breaches illustrate need for strong controls across federal agencies* (Report No. GAO-15-725T). Retrieved from https://www.gao.gov

Wilson, A. D., Onwuegbuzie, A. J., & Manning, L. P. (2016). Using paired depth interviews to collect qualitative data. *The Qualitative Report, 21*, 1549-1573. Retrieved from http://nsuworks.nova.edu

Wilson, V. (2014). Research methods: Triangulation. *Evidence Based Library and Information Practice*, *9*, 74-75. Retrieved from http://creativecommons.org/licenses/by-nc-sa/2.5/ca/

Woodley, X. M., & Lockard, M. (2016). Womanism and snowball sampling: Engaging marginalized populations in holistic research. *The Qualitative Report, 21*, 321-329. Retrieved from https://nsuworks.nova.edu

Wu, W.W. (2011). Mining significant factors affecting the adoption of SaaS using the rough set approach. *The Journal of Systems and Software, 84*(3), 435- 441. doi:10.1016/j.jss.2010.11.890

Yang, T., Ku, C., & Liu, M. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research*, *19*(1), 21-41. doi:10.1080/13669877.2014.940593

Yang, W. P., Wang, L., & Wen, H. (2013, April 7-10). *A queueing analytical model for service mashup in mobile cloud computing*. Paper presented at the 2013 IEEE Wireless Communications and Networking Conference (WCNC), China. doi:10.1109/WCNC.2013.6554886.

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber-security requirements education game (SREG). *Information and Software Technology, 95*, 179-200. doi:10.1016/j. infsof.2017.12.002

Yasrab, R., & Gu, N. (2016). Multi-cloud PaaS architecture (MCPA): A solution to cloud lock-in. Paper presented at *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, China. doi:10.1109/ICISCE.2016.108.

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation, 19*(3), 321-332. doi:10.1177/1356389013497081

Yin, R. K. (2015). *Qualitative research from start to finish*. New York, NY: Guilford Publications.

Yin, R. K. (2017). *Case study research: Designs and methods* (6th ed.). Thousand Oaks: Sage.

Yisa, V. L., Meshach, B., Osho, O., & Sule, A. (2018). Application of geo-location-based access control in an enterprise environment. *International Journal of Computer Network and Information Security, 10*(1), 36. doi:10.5815/ijcnis.2018.01.05

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., … (2017). A methodlogical guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution, 2018*(9), 10-19. doi:10.1111/2041-210X.12828

Young, S. N. (2009). Bias in the research literature and conflict of interest: An issue for publishers, editors, reviewers and authors, and it is not just about money. *Journal of Psychiatry & Neuroscience, 34*, 412-417. Retrieved from https://jpn.ca

Young, W., & Leveson, N.G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM, 57*(2), 31-35. doi:10.1145/2556938

Yusop, Z. M., & Abawajy, J. (2014). Analysis of insiders' attack mitigation strategies. *Procedia - Social and Behavioral Sciences, 129,* 581–591. doi:10.1016/j.sbspro.2014.03.716

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal, 27*(1), 13-15. doi:10.4314/mmj.v27i1.4

Zang, W., & Creswell, L. (2013). The use of "mixing" procedure of mixed methods in health services research. *Med Car, 51(8)*, 51-7. doi:1097/MLR.0b013e31824642fd

Zhang, X., Du, H., Chen, J., Lin, Y. & Zeng, L. (2011, May 14-15). Ensure data security in cloud storage. *Paper presented at* 2011 International Conference on Network Computing and Information Security, China. doi:10.1109/NCIS.2011.64.

Zineddine, M. (2015). Vulnerabilities and mitigation techniques toning in the cloud: A cost and vulnerabilities coverage optimization approach using cuckoo search algorithm with Lévy flights. *Computers & Security, 48*, 1-18. doi:10.1016/j.cose.2014.09.002

Zou, Y., & Schaub, F. (2019). Beyond mandatory: Making data breach notifications useful for consumers. IEEE Security & Privacy*, vol. 17*(2), 67-72. doi:10.1109/MSEC.2019.2897834.

Appendix A: Interview Protocol

Interview Protocol	
Actions	**Dialogue**
Introduction	Hello Mr./Mrs. AAA. I'd like to thank you once again for being willing to participate in the interview aspect of my doctoral study. My name is ABA. I work with ABB where I am an ABC. I am a doctoral candidate at Walden University in the Doctor of Business Administration with a concentration in Homeland Security. As I have mentioned to you before, the purpose of this qualitative multiple case study is to explore strategies that some information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches. This interview should take no more than two hours. I will ask 6 main questions (will repeat any questions for clarification purposes). You have the right to refuse to answer any question. As a reminder, this interview is confidential; your name, the name of your organization, and any other personal identifying information that could lead to you or your organization being identified will not be used anywhere in my paper. As I begin recording, I will refer to you as participant 001A and your organization as 001. Let me know if at any point you want me to turn off the recorder or keep something you said off the record. Do you have any questions or concerns before we begin? I will begin the interview at this time.
• Begin interview • Watch for nonverbal cues • Observe nonverbal communication/direct observation	1. What strategies do you use to protect cloud-based data from security breaches? 2. How do you assess the effectiveness of your organization's strategies for protecting cloud-

• Record • Allow participants to revisit any question	based data from security breaches? 3. What strategies were not successful for protecting cloud-based data from security breaches? 4. What barriers did you encounter to the implementation of strategies for protecting cloud-based data from security breaches? 5. How did you overcome these barriers to the implementation of strategies for protecting cloud-based data from security breaches? 6. What additional information would you like to add regarding securing cloud-based data that you have not discussed?
End interview, thank participants, and inform participants of member checking	Thank you so much for your time and participation in this study. The next step in this process is for me to transcribe the data you provided in this interview. I will email you a copy of the interview transcript to each question for your review, feedback, and confirmation. If I did not accurately capture your response, please email me back what you meant to say so that I can update my information. In the meantime, can you provide me with electronic copies of any internal documents or other pertinent documentation you consider relevant to my study to get a better understanding on how your organization intends to secure data within the cloud? Do you have any additional questions at this time? If you have any questions or concerns that may develop later, please feel free to contact me by phone or email. Once again, thank you for your time and commitment.

Appendix B: Recruitment Letter

Date:

Dear (Prospective Participant),

My name is Latasha Rivers and I am a doctoral candidate student enrolled in the Doctor of Business Administration (DBA) program with a concentration in Homeland Security at Walden University. You are receiving this letter because a friend and/or relative of yours participated in my study and thought that you possess the expertise necessary to be a candidate for participation.

The purpose of this qualitative multiple case study is to explore strategies that some information security leaders in the aerospace and defense contractor industry use to protect cloud-based data from security breaches. Participation will involve a face-to-face interview that will be no more than two hours and member checking. In order to be eligible to participate one must have experience in developing and implementing security policies, protocols and procedures; familiarity with cloud security frameworks, principles, and functions; familiarity with security controls relevant to compliance and regulatory requirements for cloud environments; and experience migrating data to a cloud platform. In addition, the participant must have a minimum of five years of experience in the IT industry and have worked for their current employer for a minimum of three years while having a comprehensive understanding of cloud and cloud security. Should you decide to participate in this study, your anonymity would be guaranteed. Please do not think that you have to participate solely because you obtained this letter. If you do not wish to participate, I thank you for your time. If you do wish to participate, please contact me at lrivers23@hotmail.com or (703) 586-8610. Your help will be very much appreciated.

Sincerely,

Latasha Rivers

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

Appendix C: Informed Consent

You are invited to take part in a research study about Strategies for Reducing the Risk of Data Breach Within the Internet Cloud. The researcher is inviting information security managers who display the following: (a) experience developing and implementing security policies, protocols and procedures; (b) familiarity with cloud security frameworks, principles, and functions; (c) familiarity with security controls relevant to compliance and regulatory requirements for cloud environments; and (d) experience migrating data to a cloud platform. Additionally, the participants should have a minimum of five years of work experience in the IT industry and have worked for their current employer for a minimum of three years while having a comprehensive understanding of cloud and cloud security to be in the study. I obtained your name/contact info via your current boss at the company. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named Ms. Latasha Rivers, who is a current doctoral student at Walden University. You might already know the researcher as a contract administrator, but this study is separate from that role.

Purpose of the Study

The purpose of this qualitative multiple case study is to explore strategies that some information security managers in the aerospace and defense contractor industry use to protect cloud-based data from security breaches.

Procedures:

If you agree to be in this study, you will be asked to:

- Answer all questions as truthful as possible
- Choose a comfortable environment to conduct the interview
- Take their time in thinking about their responses and if any clarification is needed, please make sure to stop me at any time to repeat
- Be available for at least two hours (for the interview process)
- Be available 30 days from the date of contact which will include a face-to-face interview, transcribing the data collected, and member checking

Here are some sample questions:

- What successful strategies do you use to protect cloud-based data from security breaches?
- How do you assess the effectiveness of your organization's strategies for protecting cloud-based data from security breaches?

- What strategies were not successful for protecting cloud-based data from security breaches?

Researcher's Role in the Study

For this qualitative multiple case study, I will serve as the primary data collection instrument. My role in this qualitative multiple case study will be designing the study, developing interview questions, choosing the participants, collecting the data, organizing the data, and evaluating the data. As the primary data collector, I will ask open-ended interview questions.

Statement of Confidentiality

I will not be sharing any information about you to anyone outside of this room. Reports coming out of this study will not share the identities of individual participants. Details that might identify participants, such as the location of the study, also will not be shared. The researcher will not use your personal information for any purpose outside of this research project. All paper documents collected during the research will be stored in a locked safe. The data created or collected electronically will be password protected and stored in a separate file on the computer. All information about you will have a unique study ID instead of your name. I, the researcher, will know what your study ID is and I will lock that information up with a lock and combination that will be stored for five years. It will not be shared with or given to anyone. Data will be kept for a period of at least 5 years, as required by the university.

Withdrawal from the Study

Your participation in this study is voluntary. It is up to you to decide whether or not to take part in this study. You are free to accept or turn down the invitation. No one will treat you differently if you decide not to be in the study. If you decide to be in the study now, you can still change your mind later and you will be asked to sign this consent form. You may stop at any time. Please note that the researcher will follow up with all volunteers to let them know whether or not they were selected for the study. If you do decide to withdraw from the study before data collection is completed, your data will be returned to you or destroyed.

Description of Incentives/Compensation

No incentives or compensation will be offered to take part in the research.

Risks and Benefits of Being in the Study:

Being in this study would not pose risk to your safety or wellbeing. There will be no direct benefit to you, however, your participation might help me find out more about how to prevent data breaches with the Internet cloud.

Contact Information

You may ask any questions you have now. Or if you have questions later, you may contact the researcher Ms. Latasha Rivers, via phone at (703) 586-8610 or email Latasha.rivers@waldenu.edu. If you want to talk privately about your rights as a participant, you can call the Research Participant Advocate at my university at 612-312-1210 or contact the Institutional Review Board at IRB@mail.waldenu.edu. Walden University's approval number for this study is **03-05-19-0542898** and it expires on **04 March 2020.** The researcher will give you a copy of this form to keep.

Consent

If you feel you understand the study well enough to make a decision about it, please indicate your consent by signing below.

Printed Name of Participant ______________________________

Date of consent ______________________________

Participant's Signature ______________________________

Researcher's Signature ______________________________