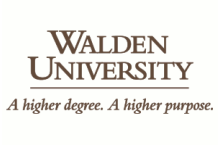

2020

Security Strategies to Prevent Data Breaches in Infrastructure as a Service Cloud Computing

Alberta Amanda Pratt-Sensie
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Alberta Pratt-Sensie

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. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Jodine Burchell, Committee Member, Information Technology Faculty
Dr. Charlie Shao, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

Security Strategies to Prevent Data Breaches in Infrastructure as a Service Cloud Computing

by

Alberta Pratt-Sensie

MS, University of Maryland at Baltimore, 2001

BS, Clayton State University, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2020

Abstract

Due to the ever-growing threat of security breaches that information technology (IT) organizations continually face, protecting customer information stored within the cloud is critical to ensuring data integrity. Research shows that new categories of data breaches constantly emerge; thus, security strategies that build trust in consumers and improve system performance are a must. The purpose of this qualitative multiple case study was to explore and analyze the strategies used by database administrators (DBAs) to secure data in a private infrastructure as a service (IaaS) cloud computing. The participants comprised of 6 DBAs from 2 IT companies in Baltimore, Maryland, with experience and knowledge of security strategies to secure data in private IaaS cloud computing. The disruptive innovation theory was the conceptual framework for this study. Data were collected using semistructured interviews and a review of 7 organizational documents. A thematic analysis was used to analyze the data. Four key themes emerged: importance of well-defined security measures in cloud computing, measures to address security controls in cloud computing, limitations of existing security controls in cloud computing, and future and potential security measures solutions in cloud computing. The findings may benefit DBAs and IT organizations by providing strategies to prevent future data breaches. Well-defined security strategies may protect an individual's data, which in turn may promote individual well-being and build strong communities.

Security Strategies to Prevent Data Breaches in Infrastructure as a Service Cloud Computing

by

Alberta Pratt-Sensie

MS, University of Maryland at Baltimore, 2001

BS, Clayton State University, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2020

Dedication

Thanks be to God that this journey is finally over; without God's guidance and strength, I would not have achieved this goal. This study is dedicated to my mother and two children. Thank you, Mom, Mrs. Pamela Elizabeth Pratt-Sensie, for believing in me and instilling in me that my goals are always attainable and that, if I cannot reach for the skies, I should reach for the mountain top. To my children, Ahmed Farooq Dura and Rianee Sannie-Ariyibi, many times I would tell you I had to study or write my paper, and I could sense the disappointment in your voice or your body language when I bailed out on spending quality time with you two. Thank you for not giving up on me, and I hope that I am an inspiration to you both to pursue higher education. Finally, I would like to dedicate this study to my supportive family and friends who gave me support and encouragement when I lost interest over the past 5 years. Your words of encouragement motivated me and helped me reach the finish line.

Acknowledgments

I would like to express my gratitude and appreciation to my chair, Dr. Miles, for mentoring me through this process. Dr. Miles has a way of calming me down and making me understand the feedback received as positive. Thank you so much for your unwavering support and patience. I would like to thank my second committee member, Dr. Burchell, for ensuring that my study met the academic writing standards. I would like to also thank my URR, Dr. Shao, for taking the time to review my work and ensure that it was IT security-focused; I am forever grateful.

This accomplishment would not have been possible without the unwavering support from my family. Thank you, Mom, for believing in me and always encouraging me to go get what I want. To my late uncle Alberta Sensie, I finally did it, and as promised I got my doctorate. I bet you are up in Heaven smiling at me and saying, "I told you so, you are a true Sensie." To my big sister, Dr. Shirley Gembeh, I emulated your footsteps, and I thank you for your unwavering support. I would also like to thank my editor and constructive critic, Mrs. Pamela Gibbs. Thank you for keeping me straight. Lastly, to my children, Ahmed Farooq Dura and Rianee Sannie-Ariyibi, I hope that you both learn from my achievements that learning is better than silver and gold. Remember that no one can take away your education, and once you have earned it, it is yours for eternity. I love you all and pray that you both emulate my footsteps.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

For information technology (IT) organizations to remain competitive and stay in business, IT leaders must strategize ways to remain competitive and keep up with constant changes in technology. Technological developments such as cloud computing have allowed businesses to incorporate computable platforms for storing, processing, and distributing sensitive data (Bhatia & Verma, 2017). Accommodating the emerging trend of data storage by organizations has, in turn, led IT leaders to change their business logic (Yu, Cao, & Schniederjans, 2017).

Safeguarding business information is one key cloud computing-related issue facing IT leaders. Storing data in the cloud has posed privacy and security concerns for organizations that implement cloud computing (Noblin, Cortelyou-War, & Servan, 2015). Cyber hacking customers' and employees' confidential and sensitive data are on the rise (Gootman, 2016), and some organizations are reluctant to embrace cloud computing because of the security challenges. Thus far, IT leaders have not fully addressed the security challenges posed by cloud computing technologies, according to experts (Igbal et al., 2016). One of the topmost concerns relates to data security and storing personally identifiable information (PII) by third-party cloud vendors (Neumann, 2014). Due to these concerns and challenges of data security, there remains a fundamental requirement for security with the evolution of cloud infrastructures (Kaaniche & Laurent, 2017). Cloud computing continues to become more pertinent to business operations, and these security concerns need to be resolved.

Problem Statement

With the new paradigm shift to cloud computing, data security is a concern for IT organizations using third-party vendor private cloud databases for storing confidential and proprietary data in data centers or at an infrastructure level (Neumann, 2014). Ninety-three percent of IT professionals in one study in the U.K. and U. S. were concerned about securing data after sensitive data were moved into the cloud (Aleem & Christopher, 2013). The general IT problem is that IT organizations have challenges securing sensitive data that reside in the cloud because appropriate security procedures are not in place. The specific IT problem is that some database administrators (DBAs) lack strategies for securing data in private infrastructure as a service (IaaS) cloud computing.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies DBAs used to secure data in private IaaS cloud computing. The targeted population consisted of DBAs at two IT organizations located in the state of Maryland who have successfully implemented at least one IaaS cloud computing security strategy within the past 3 years in their organizations to prevent data breaches. The results of this study may provide a better understanding of the security strategies that DBAs in IT organizations used to minimize costs for data breaches. Application of study findings by DBAs may allow IT businesses to stay competitive with potential business growth.

Nature of the Study

I selected a qualitative case-study design for this study. A qualitative study allows a researcher to investigate the compound issues pertinent to gaining an in-depth understanding of the study phenomenon (Houghton, Murphy, Shaw, & Casey, 2015). Because the primary focus of this study was on exploring and investigating the issues pertinent to the security strategies used by DBAs to prevent database breaches, a qualitative study was the appropriate research method. Quantitative researchers measure a phenomenon using numbers and percentages (Barnham, 2015) and are statistically focused on analyzing the values of variables (Onen, 2016). Qualitative research was appropriate for this study because no hypothesis was tested and no relationships between variables were studied. A mixed-method study is a combination of both qualitative and quantitative research and is used by researchers to answer complex questions (Than et al., 2018). This research study was unsuitable for a mixed-method study approach because no quantitative components were collected.

I considered four qualitative research designs for my research study: ethnography, phenomenology, narrative, and case study. Researchers use ethnography designs to observe patterns or experiences of a specified cultural group or community (Thomas, 2017). This design was not appropriate for this study because I was not focusing on observing the culture of DBAs. A phenomenology design focuses on understanding the life experiences of a sample population (Kruth, 2015). This design approach was unsuitable for this study because I did not observe the lived experiences of DBAs while a database breach occurred. In using a narrative design, researchers primarily focus on

communicating the lived experiences of research participants through storytelling (Wang & Geale, 2015). The narrative design was not selected because the focus on the research study was not on the biographies and historical information of the DBAs exploring IT strategies. The purpose of my study was to explore the strategies DBAs used to secure data in private IaaS cloud computing. Therefore, the narrative design study did not align with the goals of my research study.

A qualitative case study was a preferred design for this study because it allowed me to delve deeper and understand the research topic and questions. A case study is defined as an investigation of an enclosed group of people from multiple viewpoints (Larrinaga, 2017). A case study research design was beneficial because it answered the how and why questions concerning the preferred security measures that DBAs used to minimize data breaches (see Larrinaga, 2017). A case study researcher chooses and deduces information and does not form statistical conclusions (Larrinaga, 2017). The use of a case-study design allowed me to better understand what the preferred strategies are for preventing data breaches based on the research participants' insights and perceptions. Qualitative research is pragmatic, originating from experience and/or observation (Lewis, 2015; Marks, 2015). A case study produces knowledge about the viewpoints, situations, and skills of participants. It involves the efficient use of research skills and tools such as data analysis to understand the participant's perception of a problem through ascertaining patterns or themes (Lewis, 2015). Moreover, qualitative research was appropriate for my study because a central focus was on collaboration among IT professionals. Conducting

interviews with participants' gave me insight on their perceptions of and strategies for collaborating with colleagues.

Research Question

What are strategies database administrators used to secure data in private infrastructure as a service (IaaS) cloud computing?

Interview Questions

I posed the following interview questions to participants.

1. What was your experience in database security in cloud computing? Please explain.
2. Have you encountered database breaches? If so, were security measures in place?
3. Have you ever used security measures to prevent database breaches in cloud computing? If so, how was this done?
4. How did your existing organization use security measures to prevent data breaches in IaaS cloud computing?
5. What solutions did your organization provide with regard to preventing data breaches?
6. What security measures did your organization have in place that was effective in preventing cloud computing data security breaches?
7. If your organization did not have a standard protocol for preventing data security breaches, have you implemented security measures to prevent cloud computing data security breaches in your organization?

8. What was the least effective security measures used in preventing cloud computing data breaches?
9. With your DBA experience, what obstacles did you face concerning implementing cloud computing security measures, and how was this done?
10. In terms of cloud computing, what were your concerns in implementing security measures, and had the organization done to rectify these concerns?

Conceptual Framework

The framework chosen for this study was the disruptive innovation theory (DIT). DIT was initially published by Christensen in 1997. Christensen (1997) proposed that organizations can be successful when their leadership support new technology instead of evading it or refusing to acknowledge it. DIT was the basis of a series of mature technological innovation studies, the focus of which was on identifying radical innovation (e.g. Bohnsack & Pinkse, 2017; Christensen, 2011). The impact of this radical nature of DIT changed the existing core business logic in organizations and created new business units that performed diverse value activities (Christensen, 2011). Thus, this shift in the organization's core business logic resulted in resistance to change from the organization's business stakeholders. Additionally, Christensen (2011) contended that DIT has gained more success from new start-up organizations than established organizations because leaders built new infrastructure to accommodate disruptive innovation, unlike leaders of established organizations who had to dismantle their existing infrastructure and core business logic. Thus, new organizations that utilized DIT were more successful than established organizations.

The DIT framework worked well for my cloud computing study because it is a process that focuses on getting the business model right from the outlying market to the conventional market, and it is a slow process that takes time to evolve, with resistance along the way. Security and privacy challenges have been an obstacle to adopting cloud computing in many organizations (Singh & Chatterjee, 2017). Cloud computing has been a slow process for organizations to implement due to the security and privacy challenges that remain unanswered. Moreover, IT professionals and organizations are reluctant to adopt new technology even though it has cost-saving benefits (Christensen, Raynor, & McDonald, 2015). I studied the impact of security and privacy challenges for implementing strategies for securing data in private IaaS cloud computing. Christensen (1997) stated that the DIT supports innovations and spawns evolution, which enhances performance in the current IT environment. Therefore, DIT supported the qualitative case study because the research emphasis was on the opinions of IT professionals regarding security strategies on cloud computing used to prevent data breaches in IaaS private cloud. Knowledge arising from the study may help IT leaders to improve the process of organizations implementing cloud computing and make use of the cost-saving benefits of this technology.

Additionally, the DIT framework supported the development of cloud computing, a new evolving technology, which allowed early adopters in companies such as Amazon Web Services to venture into this developing market (Streitfeld, 2014). Cloud computing was also touted by Yu et al. (2017) as a disruptive innovation due to its frequent use by organizations. New technology was also the root of disruptive innovations because it

altered the service process, and organizations used this transformation for achieving a competitive edge (Padgett & Mulvey, 2007). Cloud computing have made organizational leaders change the way they conducted business, such as accessing software anywhere and anytime as long as it had Internet capability.

Disruptive innovation has changed the way organizations conduct business to remain competitive in the IT market. Organizational leaders were threatened by technologies that disrupted the way they conducted business because they could not incorporate new technology such as cloud computing (Neumann, 2014; Vecchiato, 2017). The implementation of DIT by business leaders strategically changed the way they did business, and this required constant improvement of their products and services, as well as provided organizations with a competitive edge (Vecchiato, 2017). Disruptive innovation also modified organizations' business processes by meeting market demands and eliminated existing archaic business practices (Sims, 2016). For example, organizations were no longer paying rent for physical buildings to store databases. Instead, these data-stored services were now done through cloud service providers, thus minimizing energy costs (Schniederjans & Hales, 2016). With cloud computing representing the new way to store data, DBAs need to know what strategies are required to secure data stored in the cloud.

Operational Definitions

The following key operational terms are used in this cloud computing study:

Cloud computing: A resource pool of hardware and software infrastructure provided by a cloud computing vendor that is efficiently and flexibly accessed by users based on the availability of internet connectivity (Parisha, Puneet, & Sheenu, 2017).

Cloud service provider: A vendor that provides numerous services which include basic types of hardware and software architecture services, such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), based on the business needs of organizations (Supriya, Sangeeta, & Patra, 2016).

Community cloud: A cloud deployment model infrastructure for collective use by multiple organizations and upkeep in an exclusive community that has shared security, privacy, concerns, similarities, and minimized costs (Goyal, 2014).

Database administrators: A specialized computer systems administrator. A DBA's role includes storing and organizing data and maintaining a successful database environment by ensuring data are secure from unauthorized access (see Zhou, Sun, Song, & Song, 2017).

Disruptive innovation: A high-tech improvement, new commodities, or new amenities with low cost that entail a tactical effect that frequently surpasses the foremost major technologies or status quo commodities, resulting in a disruption in a market (Nagy, Schuessler, & Dubinsky, 2016).

Hybrid cloud: A cloud deployment model infrastructure encompassing two or more cloud deployment models (private, community, or public) working jointly as a solitary system that allows application and data transport among them (Goyal, 2014).

Infrastructure as a service (IaaS): Utility computing that allows customers to access virtualized hardware and computing on-demand via the Internet such as processing, storage services, and networks with the capability to implement and run the random software, which includes operating systems and applications (Igbal et al., 2016).

Platform as a service (PaaS): Services that customers use to construct, test, host, and apply consumer-created or acquired applications using application program interface (API) to upkeep the life cycle of building and delivering web-based applications (Goyal, 2014).

Private cloud: A cloud deployment model infrastructure operated entirely for a business that is controlled and managed by the organization or a third-party vendor, either on-site or off-site (Goyal, 2014).

Public cloud: A cloud deployment model infrastructure that is available to the community and shared by the general public (Yuvaj, 2015).

Software as a service (SaaS): A means of providing applications over the Internet via a thin client on a Web browser to customers (Igbal et al., 2016).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are expectations which the researcher believed were true, and this posed a risk to the research study. Identifying assumptions upfront allowed the readers to understand better what the researcher believed to be true regarding the research study (Rubin & Babbie, 2016). An assumption was an unconfirmed fact assumed to be factual that led to possible threats (Thomas, 2017). The initial assumption in this study was that

the research participants' responses to the interview questions were impartial and truthful. Another assumption was that participants were knowledgeable about cloud computing security and had adopted it based on its benefits.

Limitations

Limitations are restrictions or weaknesses that threatened the research validity and results (Busse, Kach, & Wagner, 2016). The precision of the research outcomes was contingent on the participants' credibility and reliability of the information they provided. This study was impacted by two limiting factors that could not be controlled by the researcher and dismissed: First, the validity and credibility of the findings were determined by the research participants, and second, cloud computing was still evolving, and participants years of experience was limited. Therefore, some of the cloud computing participants' experience was based on the customary IT database storage instead of their direct experience with security strategies used to secure data in private IaaS cloud computing.

Delimitations

Delimitations referred to the boundaries of the study within the researcher's control and prevented the researcher from making unexpected claims about the study (Rubin & Babbie, 2016). The biggest delimitation that was imposed on the scope of this doctoral study was the geographic location of the population. The geographical location of the population was only limited to the Baltimore, Maryland area, and the population itself was only limited to IT DBAs and security professionals. Another delimitation was the sample sizes of the study. Purposive sampling was commonly used in qualitative

research studies, and research participants were selected based on their experience and ensured a balance of participants as related to the country, gender, and discipline (Brew, Boud, Lucas, & Crawford, 2017).

Significance of the Study

Contribution to Information Technology Practice

This study was valuable to IT practitioners because it explored security strategies to prevent data breaches in IaaS cloud computing. The importance of exploring security strategies was because data security of confidential and sensitive data remained a challenge since organizations' data were hosted in remote data centers (Bayramusta & Nasir, 2016). Exploring these security strategies to prevent data breaches by expert professionals was also beneficial in cost savings and improved both the operations and technical capabilities of the organizations. This study increased the use of cloud computing for IT organizations because it gave them insights to the effective security strategies that prevented data breaches and the use of cloud architectural solutions (IaaS, software as a service (SaaS), platform as a service (PaaS), resource pooling and sharing, on-demand services, pay-as-you-go services, which provided organizations the elasticity to better improve their IT resources. This study increased the use of cloud computing because it informed organizations interested in adopting cloud computing about the security strategies that may be used to minimize data breaches in private IaaS cloud computing. With the use of these security strategies, organizations felt comfortable in adopting cloud and allowed the third-party provider to host their sensitive data. Adoption of cloud computing, despite its trepidations, provided a competitive edge for

organizations with this new product and services it brought, such as on-demand access, self-service, pay-as-you-go, resource pooling, and multi-tenancy, changed the way business was done. Thus, with these security strategies in place to minimize data breaches, customers would feel confident that their data was secured and not compromised.

This research may impact social change in communities because the implementation of cloud computing has changed the way organizations managed their businesses, such as hospitals. Hospitals regularly shared medical information of patients by their healthcare providers. If the security strategies were in place to protect database breaches, this might increase the confidence of medical facilities to store the sensitive data of patients in the cloud, such as patient information and their credit cards (Shao et al., 2015). With these security strategies in place, sensitive data would be encrypted before storage in the cloud and before data being transmitted (Shao et al., 2015). Securing patient information and their credit cards could save lives and help keep their personal information from being compromised. Finally, the use of secure cloud computing may lead to the minimal use of hardware, which according to Moyano, Fernandez-Gago, and Lopez (2013) and Song, Li, Wang, and Zhu (2013), reduced unrecyclable components deposited to landfills.

Implications for Social Change

This research impacted social change in communities because the implementation of cloud computing had changed the way organizations managed their businesses, such as hospitals. Hospitals regularly shared medical information of patients by their healthcare

providers. If the security strategies were in place to protect data breaches, this may increase the confidence of medical facilities to store the sensitive data of patients in the cloud, such as patient information and their credit cards (Shao et al., 2015). With these security strategies in place, sensitive data can be encrypted before storage in the cloud and before data being transmitted (Shao et al., 2015). Securing patient information and their credit cards would save lives and help keep customers' personal information from being compromised. Finally, the use of secured cloud computing may lead to the minimal use of hardware, which according to Moyano et al. (2013) and Song et al. (2013), would reduce unrecyclable components deposited to landfills.

A Review of the Professional and Academic Literature

The focus of this qualitative multiple case study was on exploring the database security strategies DBAs use to secure data in IaaS cloud computing. In reviewing the literature, I was guided by the research question: What are strategies DBAs use to secure data in private IaaS cloud computing? I conducted a qualitative multiple case study to identify the successful strategies employed by DBAs to secure data in cloud computing in IT organizations in Baltimore, Maryland. The review of literature focuses upon the study's DIT conceptual framework and the security strategies used by DBAs to secure data in IaaS cloud computing. Related topics such as cloud computing architecture, cloud computing data security risks, and the strategies use by DBAs to secure data in cloud computing are also discussed.

Literature Search Strategy

I used the following Walden University Library databases to locate peer-reviewed articles for my study: Google Scholar, ProQuest Central, IEEE digital library, and the Thoreau Multi-Database Search. These databases provided access to a large number of peer-reviewed articles and journals on cloud computing. The procedures used to locate these articles included the use of keywords related to my topic of study. These included *cloud computing definition*, *data security*, *cloud computing and regulations*, *cloud computing and cost*, *cloud computing and benefits*, and *cloud computing and risks*. A total of 246 refereed articles have been incorporated into this research study; 130 of these articles were included in the literature review. Of the 130 articles in the literature review, 92% are peer-reviewed and published within 5 years or less of my projected graduation date of 2020.

Disruptive Innovation Theory (DIT)

For the study's conceptual framework, I chose Christensen's (1997) DIT. Christensen first coined the term *disruptive innovation theory* in 1995 and published it in his book *An Innovator's Dilemma* in 1997. Christensen's (1997) series of case studies in the book gained notoriety because it showed how incumbent organizations become incapacitated when a new technology with low performance and low costs disrupts the existing market and traditional firms. He emphasized that in the initial stages of disruption, the lower-performing innovation meets the necessities of a little portion of the current client base, but as the innovation advances, its execution enhances, and the development addresses the issues of more clients in the business (Christensen, 1997).

Moreover, in the long run, the incumbent organizations are driven out of the business as the innovative disruption meets the needs of the standard market (Christensen, 2011). DIT is beneficial to large organizations because it provides a means of identifying ways to implement new technology to remain competitive.

DIT serves as a benchmark to evaluate the impact of innovative technology on organizations. The core of Christensen's work is the notion that the disruption sets the trend wherein the incumbent organizations give up the lower margin elements of their product offerings and the organizations' overall profit margins often increase (Christensen, 2007). Additionally, this innovative disruption results in organizations expanding net revenues, even as the disruption leads to a failure by the incumbent organizations (Christensen, 1997). Christensen's motive for developing this theory was to recognize the reasons organizations fail and better understand the disruption of the failure. Christensen (1997) suggested that large organizations must assess the marketplace for new products or services that will disrupt the core business. His assessment of the disk drive industry led him to believe that there are three patterns of disruption: First, disruptive products were technologically straightforward; second, advanced technology helped sustain the performance of the organizations and did not fail; and, third, new entrants were more willing to implement and lead disruptive technologies than incumbent leading organizations. Christensen found that established organizations were customer-first oriented and this impacted the vision of the leading firms; this customer-first oriented vision allowed new entrants organizations to seize the opportunity to use disruptive technology to topple large organizations slowly.

Disruptive technologies have impacted large organizations by changing the way they conduct business. Christensen (2006) viewed established organizations as being unprepared for the loss of their markets by disruptive technologies that were originally simple products related to performance benchmarks set by the majority of their customers. These disruptive technologies satisfied the needs of new entrants' customers, which improved over time to meet the needs of mainstream customers. He first tested this theory using the disk drive industry in the 1970s and 1980s (King & Baatartogtokh, 2015). King and Baatartogtokh (2015) summarized the four key elements that the DIT is based on: "that incumbents in a market are improving along a path of sustaining innovation, that they overshoot customer needs, that they possess the capability to respond to disruptive threats, and that incumbents end up floundering as a result of the disruption" (p. 79).

Christensen's DIT continues to be modified with the evolving change in technology. In later work, Christensen et al. (2015) surmised that the focus of DIT is to make products affordable, easily accessible, and, with continued use, readily available to the general public. Christensen et al. added that DIT starts in low-end markets or new market footholds. The authors predicted that low-end technology becomes successful when adopted by established organizations due to its convenience and cost savings (Christensen et al., 2015). The performance of low-end disruptive technology can lead to improved products and changes in the industry, and it occurs infrequently, resulting in performance problems (Goldstein, 2015; Sultan, 2015). Christensen in his original work

and in his later research further defined disruptive innovation as being one of two key types: as a low-end market or as a new market as shown in Table 1.

Table 1

A Comparison of Low-End and New Market Disruptive Innovations

Disruptive innovation criteria	Low-end DI	New market DI
Performance measures	Concerning standard product or service	Varies from the typical product or service
Existing customers	Works better for new entrants because the existing products or services were high-priced	Varies from the typical product or service
Incumbents' reaction	Desert the low-edge advertise market section and extend the high-edge market section	New entrants have not used or purchased these products
Value network	Starts the same as the existing organizations	Disregard and overtime the DI adopts the customers that cannot afford the high-priced technology

Note. Adapted from "Opportunities for Disruption," by C. C. Hang, E. Garnsey, and Y. Ruan, 2015, *Technovation, 83-93*, p. 85. Copyright 2015 by Elizabeth Garnsey. Adapted with permission (see Appendix A).

DIT can be used to predict the success of new products based on the customers' acceptance of the disruptive, innovative product (Hang et al., 2015). The use of disruptive innovation is successful depending on the affordability, ease of use, and convenience of the product, and with time it may slowly topple customary products.

Cloud computing is considered a disruptive innovation. Cloud computing emergence, though slow, confirmed Christensen's argument in that this new IT technology disrupted the IT market (Kaltenecker, Hess, & Huesig, 2015). DIT relates to cloud computing, which is a good example of how new technology disrupts the way

organizations conduct business and develop strategies to secure data in private IaaS. Additionally, cloud computing is a disruptive technology and creates an opportunity for start-up organizations to align with the existing market (Hang et al., 2015). The purpose of DIT is to explain how low-end disruptive technology such as cloud computing improves products and system performance (Goldstein, 2015; Sultan, 2015). Based on the research studies spotlighted in this paragraph, start-up organizations may benefit from cloud computing, which will allow the start-up organizations to align with the existing organizations

Evolution of disruptive innovation theory. In the literature review, I analyze several theories or conceptual models that have been proposed to evaluate how new technology is adopted by consumers based on features such as cost savings, ease of use, and convenience. Christensen developed the DIT to examine the convenience of technological improvements in the evaluation procedure of accepting creative products in an IT firm (Christensen, 2011; McMurtry, 2012). DIT intends to exemplify the IT marketplace, which uses by-products and services designed and built according to the execution profile needed by buyers and conveyed by the IT pioneers (Dan & Chang Chieh, 2010). The idea of DIT is also referred to as a radical innovation that focuses on breakthrough products or services that often change existing technology and the way of conducting business (Nigra & Dimitrijevic, 2018). Customers tend to embrace these lower-performing products and services because of other characteristics such as ease of use, ease of management, lower costs, or usability (Caldarelli, Ferri, & Maffe, 2017). Despite the negative impact on organizations, once DIT is implemented, it provides

substantial innovative changes to an organization's business logic (Ali, Warren, & Mathiassen, 2017).

A disruptive innovation such as cloud computing provides organizations access to innovative technology that meets business needs and minimizes the impediments to innovation (Ali et al., 2017). King and Baatartogtokh (2015) found that innovative technology allows organizations to stay competitive with their competitors. The DIT was applicable for this research study because it allows IT managers to see the value of using innovative cloud computing technology. This theory was also acceptable for this study because, with the rapid growth of cloud computing, IT organizational leaders are changing their way of doing business (Mahtoa, Belousovab, & Ahluwalia (2017). Thus, with this change in the core business logic in IT firms, DBAs need to understand the strategies required to secure sensitive data in cloud private IaaS.

Over the past 2 decades, DIT has been misinterpreted and modified by researchers. Christensen and researchers have refined and perfected this theory in multiple research studies to address its shortcomings (Weeks, 2015). Additionally, several researchers have proposed that DIT has allowed start-up organizations to leverage innovative technology that is not well known by making it popular, which may be a pitfall for large organizations as their business models do not deem new technology as initially profitable (Schmidt & Druehl, 2008). In an attempt to clearly define disruptive innovation, Schmidt and Druehl (2008) described it as a low-end encroachment. They further found that low-end encroachment initially impacts the low end of the existing market and then spreads upward. The researchers developed a new framework based on

the economic "linear price model," which consisted of a three-step process mapped to the Christensen and Raynor (2003) DIT: immediate form of low-end encroachment, fringe market encroachment, and detached market encroachment (Schmidt & Druehl, 2008). According to Schmidt and Druehl, the goal of this framework was to evaluate the effect of new products over a period with the focus on costs, revenues, market segments, and quantities and how they will spread through low-end or high-end disruption. First, the immediate form of low-end encroachment is associated with Christensen's low-end disruptions that impact low-end customers and then spreads upward by the impact of the existing market. Then, the fringe market and detached market situation are linked to Christensen and Raynor's (2003) new market disruption. In this situation, the new innovative technology occurs by identifying the customers' needs in comparison to the existing low-end customers before encroaching on the low-end of the previous product and then spreading it toward the high-end (Schmidt & Druehl, 2008).

A good example of disruptive innovation is that of Southwest Airlines, which, when first introduced, focused on customers who preferred driving and offered them eye-catching prices for air tickets (Schmidt & Druehl, 2008). This introduction of Southwest Airlines resulted in opening opportunities for these customers to fly inexpensively, and over a period, this disruption progressed upward and opened prospects for those customers who could not afford flying. The example illustrates how adopting cloud, regardless of its concerns, offers a cost reduction solution for organizations with its new products and services such as reduced investment in hardware, limiting payment for

resources to those that the organization needs, easy mobility with access to the data anytime and anywhere, and increased flexibility (Caldarelli et al., 2017).

The use of DIT by start-up organizations has shown that low-end customers' needs are met cost-effectively by adopting innovative technology. Throughout use, the disruptive innovation technology's performance not only meets the needs of the low-end customers but subsequently increases with development to satisfy the mainstream customers (Vecchiato, 2017). In terms of cloud computing, DIT has many benefits; however, IaaS implementation of cloud computing within organizations makes them vulnerable to data breaches, compromised security credentialing and broken authentication, and hacked interfaces and API (Jathanna & Jagli, 2015). Because cloud computing is considered a disruptive innovative technology, organizations now have cloud service providers (CSPs) that are responsible for managing and maintaining voluminous data of proprietary information for their organizations (Jathanna & Jagli, 2015). Because of the proprietary information stored in the cloud, it is often an attractive medium for data breaches by hackers (Jathanna & Jagli, 2015). This proprietary information when hacked can result in loss of confidence by customers, legal actions, and exposure of sensitive data, which can negatively impact an organization's credibility, image, and business for years to come (Jathanna & Jagli, 2015). It is common for CSPs to offer APIs as part of their cloud computing data storage services package; however, these APIs are managed by third parties. As a result, organizations become reliant on third parties, which also require access to proprietary information, but may not provide security measures in place.

Additionally, data stored in IaaS poses a security risk to organizations by unintentionally providing unauthorized access to internal employees and external hackers (Jathanna & Jagli, 2015). DBAs should develop a strong identity management infrastructure to ensure the appropriate permissions are granted or removed based on the user's role and relationship to the organization (Jathanna & Jagli, 2015). For example, the 2015 Anthem breach resulted in 800 million customers' records being compromised was due to the improper credentialing of user authentication (Jathanna & Jagli, 2015). Cloud computing relies on third-party providers such as CSPs to store proprietary information. Thus, IT professionals and DBAs should focus on the strategies that work best to prevent data breaches in a cloud computing infrastructure to safeguard customers' data.

DIT serves as a business model that forces organizations to change their business model when implementing a new product or service or changing procedures (Sims, 2016). New, innovative technologies may compel leaders in considering these business decisions to remain competitive in the IT market (Sims, 2016). The goal of DIT should be for IT managers of organizations to make use of successful innovative technology to succeed in the market instead of falling prey to the DIT (Sims, 2016). Christensen (2011) stated that start-up organizations fare better than large organizations in leveraging innovative technology, which leads to an increased success rate because they do not have to change their business model as they are only building their business model. In their review and analysis of the various research studies, Christensen et al. found that DIT used by new or start-up organizations that lack existing infrastructure and business models tend to be successful because they do not have to develop new infrastructure and do not

require input from their customers. The use of DIT by new or start-up organizations results in an improved success rate in utilizing an innovative technology (Christensen, 2011).

The DIT is helpful for this study because it forms the basis of how low-end disruptive technology such as cloud computing has forced organizations to change how business is conducted to stay competitive by improving products and system performance in the continuously evolving technological age by exploiting the disruption. Unlike the customary IT infrastructure, cloud computing as a DIT has made IT infrastructure readily accessible without upfront costs and delays to new organizations that could not have afforded it (Rogers & Cliff, 2012). Thus, using low-end disruptive technology like cloud computing has led to organizations changing their business portfolio to remain competitive in the IT sector while providing flexibility and convenient methods of data transfer and cost savings (Yu et al., 2017). Furthermore, exploiting DIT products has led startup organizations to afford innovative technology with minimal upfront costs.

Today, researchers continue to argue that DIT is ambiguous and not well defined, and researchers have broached broad claims about this theory. For example, researchers have attempted to define DIT and have fallen short of adequately capturing what the concept is (Nagy et al., 2016). Other researchers such as Danneels (2004) questioned the ambiguity of Christensen's definition of disruptive innovation and stated that the meaning of disruptive innovation was problematic. He also indicated that further research is required to accurately define disruptive innovation (The term disruptive innovation is loosely used and is separate from Christensen's premise of his framework). Danneels

(2004) stated that a reexamination of DIT needs to be reconsidered by researchers to improve the definition and provide a better comprehension of how the term shapes the destiny of organizations. In examining what distinguishes technology from being disruptive, he found that Christensen did not differentiate what is a "disruptive technology" (Danneels, 2004). By examining 16 empirical studies, he found that the term disruptive technology was used conflictingly based on the effect of technological shifts on incumbent organizations (Danneels, 2004). The author believed that DIT might result in changing of the guard wherein the incumbents are progressively replaced by the entrants, and organizations should respond to this change by accepting the disruption instead of developing a separate unit. Since cloud computing is a DIT, it continues to provide products and services for organizations that have implemented it by having an inferior performance to those customary products and services (Hang et al., 2015). The results from these studies support the research question of my study: IT professionals such as DBAs need to understand the strategies that work best to minimize data breaches and improve performance. Before the implementation of cloud computing in organizations, DBAs must ensure that they understand what cloud computing is and its associated risks, which can negatively impact financial, legal, and regulatory compliance impact on their organization (Jathanna & Jagli, 2015). For example, phishing and fraud are common techniques adopted by hackers to gain unauthorized access to sensitive information. As a government employee, my federal department sends out frequent phishing exercises to determine whether users are using due diligence in mitigating risks when they receive suspicious e-mails.

IT managers and DBAs in established firms are hesitant to embrace DIT in their organizations due to the apprehension of failure if the DIT is not successful. Christensen's (1997) DIT has gained momentum and it is applied among managers and DBAs. Managers are faced with challenges of switching long-standing dependable technologies and business models with untested ones (Crockett, McGee, & Payne, 2013). DBAs are managers of the database and therefore, should be considered managers as stated by Christensen. Christensen (2011) argued that new firms perform well than conventional firms in implementing DIT. Unlike these traditional incumbent firms, new firms lack a current business foundation and standard (Vecchiato (2017). These new entrants have to build their business foundation and standards purposefully for the DIT and would not have to experience changes to their core business logic like the incumbent firms (Vecchiato (2017). Managers and DBAs have to be open to change their way of doing traditional business to remain competitive in the constantly evolving IT market. Buy-in from managers to implement disruptive technology may be beneficial for the success of IT organizations.

Managers and DBAs are the keys to the success of DIT in organizations. DIT influences existing organizations' managers to expand their business opportunities through the evaluation of customer needs as well as evolving new markets (Vecchiato, 2017). Vecchiato (2017) stated that the manager's perception plays a key role in the causes of DIT changes in the existing IT market. For example, these changes can be due to social impact wherein the customers use the product to meet their need for friendship versus the esteemed impact wherein the customers need for using the product meets their

need for achievement (Vecchiato, 2017). In Vecchiato's research study, this framework was tested between the smartphone business and the operating system. The results showed that the major intent why the existing managers fail in the rise of DIT is due to incapacity to distinguish between the mounting social market where customers use products to satisfy their need for friendship or the esteemed market where the customers use products to gratify their demand for success (Vecchiato, 2017). Managers and DBAs cognition of DIT may result in a positive impact if they view DIT performance in the evolving market as a means to satisfy their customers' needs, which in turn will ultimately outperform the conventional market through rationalization and eagerness of the new technology opposing competition effects (Vecchiato, 2017). Managers and DBAs perception and cognition of disruptive innovation are either embraced as an opportunity or threat to the organization and position the potentials of the organization toward change (Kranz, Hanelt, & Kolbe, 2016; Osiyevskyy & Dewald, 2015). Therefore, for IT managers and DBAs to remain competitive, they have to adapt to the evolving changes in the IT marketplace and embrace disruptive innovation technologies to satisfy their customers' needs.

Research studies have proposed that DIT by Christensen remains ambiguous and not fully understood. Two key premises of Christensen's DIT are focused on the performance of the innovative technology and the effects of those organizations who prefer to ignore it and continue listening to what their customer's need (Tellis, 2006). Tellis (2006) agreed with other researchers that Christensen's DIT had gaps in the DIT definition and lack of validity of the sampling size. Additionally, Christensen (2006)

concurred with researchers that have improved the DIT definition, but he stated that DIT is still an ongoing process. In his attempt to research why DIT definition is ambiguous, with trepidation, he suggested that disruptive technology is centered on five premises: the innovative technology initially underperforms the leading one; it has characteristics such as low-priced, modest, and useful than the leading technology; organizations tend to lean to their customers' needs by ignoring the new technology and are reluctant to invest in it; progressive performance improvement of this new technology based on customers' market demand; and the new disruptive technology catches up with the existing leading technology and displaces it (Tellis, 2006). More research is required to understand the generalized premise of DIT and its associated risks especially in terms of securing the new DIT cloud computing from breaches or attacks. More research is required to understand the risks, especially in terms of securing the new technology from breaches or attacks. For example, since DBAs gave up control of data stored locally to CSPs, storing of data in the cloud environments may no longer have the protection of data when handling data tasks sure as migration (Liu, Yang, Zhang, & Chen, 2015). The new requirements posed by data storage in cloud computing such as security and verification of data have made it challenging for DBAs to secure data (Liu et al., 2015). Therefore, more research needs to be done to identify security strategies to secure data in the cloud computing environment. Tellis (2006) questioned the logic of Christensen's (1997) sampling, whether the sampling size of disk drives was used to build upon the DIT or to test the theory using the S curve. His research studies concluded that changes related to new technology in organizations are impacted by the organization's internal culture

instead of the external technological factors to be successful or lead to failures. Cloud computing is progressively changing organizations' internal culture by getting them to move away from the traditional data storage in physical centers to data storage in the cloud despite its security concerns (Shahzad, 2014). Cloud computing is progressively disrupting the way organizations conduct business. Despite the ambiguity of DIT, its impact on new technology such as cloud computing is impacting organizations' internal culture, and this has allowed these firms to move away from the traditional data storage in physical data centers to cloud computing data storage even with the data security concerns.

Other researchers have challenged Christensen's work emphasizing that his DIT is not valid because this theory is based on handpicked cases and it is not well examined. Questions of Lepore's (2014) concerns about DIT were focused on the anomalies from the research findings such as Christensen's research strategy and the conclusions drawn from his analysis. Lepore's (2014) findings refuted Christensen's DIT by stating it is not widely enough tested due to limited use in selected case studies. The research details showed a lack of supporting evidence of why the specific cases tested were handpicked and lack of suitable exploration of the data that disproves his framework (Lepore, 2014). Lepore (2014) questioned the credibility of Christensen's DIT because it is only editorially reviewed and lacked peer review. Weeks (2015) evaluated the three major concerns of Lepore's weaknesses in Christensen's theory: inadequate definition of DIT, lack of predictive power at the managerial level, and an unclear element of evaluation of the industry, firms, or firm leaders.

These contrasting views provide information on what has already been researched on DIT and provide a better understanding of this theory by cautioning researchers when using lower-cost technology. The weaknesses in the DIT primarily focus on how loosely the term disruptive is used, how it is applied, and its repercussions (Weeks, 2015). Caution should be applied to how to use DIT since the definition of DIT is still not well defined, and it continues to be modified (Weeks, 2015). These findings also indicate that it is not solely the definition of DIT that needs rework, but further research will be beneficial in determining organizations' use of new technology and how to accept it to remain competitive (Fador, 2014). Cloud computing remains a new technology, and it provides opportunities for startup organizations based on their needs, but these organizations have to be aware of the security risks and better understand how to use security strategies to prevent data breaches (Rubóczki & Rajnai, 2015). The security strategies that DBAs should be focused on are data migration via the internet from local servers, handling of data by CSPs, securing networks, browsing of APIs, and data encryption (Alamoudi & Alamoudi, 2016). Additionally, sharing data via a multitenancy environment poses security threats due to data theft (Barrow, Kumari, & Manjula, 2016). It is important no matter the size of the organization to educate staff in preventing or minimizing data breaches (Rubóczki & Rajnai, 2015). This education may be in the form of virtual or in-person training on how to minimize data breaches (Rubóczki & Rajnai, 2015). Organizations should ensure that they employ a trusted third-party, which operates in securing data confidentiality and have service level agreements (SLAs) that provide end-end security that is scalable (Zissis & Lekkas, 2012). These organizations must also

implement a training infrastructure to provide their employees with adequate knowledge and how to securely operate within a cloud computing environment (Rubóczki & Rajnai, 2015). In summary, training and education related to cloud computing security strategies, and the trusted third-party are pivotal to the successful implementation of cloud computing by DBAs to minimize data breaches. DIT definition remains ambiguous and use of it varies per the perception of the organization. For organizations to remain competitive, they need to determine how best to use this DIT in accepting the use of innovative technologies.

Critical analysis related to the conceptual model. Many researchers have attempted to question Christensen's DIT. DIT is a form of radical change that impacts the way organizations adapt to the evolving changes in the information technology market (Christensen, 2011). DIT has the potential to provide value, which may lead to new opportunities that an organization can exploit to remain competitive in the IT market (Pérez, Dos, & Cambra-Fierro, 2017). DIT is now a common theme used by cutting-edge companies to define the impact of new technology both in academia and practice (Chen, Guo, & Zhang, 2016; Reinhardt & Gurtner, 2015). Since the DIT was introduced 2 decades ago by Christensen (1997), researchers continue to improve the impact of DIT on companies and its outcomes of storing data on disc drives in the 90s is now history (Takahashi, Shintaku, & Ohkawa, 2013). Data storage has evolved into using technology such as smartphones, which were forms of disruptive technology upon the initial emergence of it (Christensen, 1997). Smartphones slowly disrupted the use of Blackberry because the owners of this product were reluctant to invest in touchscreens and the

consumers preferred using touch screens versus typing out emails (Reinhardt & Gurtner, 2015). Reinhardt and Gurtner (2015) believed that DIT products such as smartphones initially underperformed, and large firms did not value it in the mainstream. However, with time, according to the authors, its performance improved and became cost-saving and attractive to its early adopters, which led to the displacement of Blackberry in the technology market. Mahtoa et al. (2017) added that DIT involves a risk-taking approach by entrepreneurs in lower or higher-end markets. Feder (2018) also concurred that DIT is linked to new products, which results in a shift in the way organizations conduct business, and the evolving of new products leads to the displacement of existing products. Despite the research studies focused on concerns about DIT, this conceptual framework remains valuable to organizations to determine the success of new products and its change in organizations' core business logic, as well as securing DIT from security breaches. DIT is viewed by some researchers as a breakthrough in the way organizations conduct business when a disruption in technology occurs. Bohnsack and Pinkse (2017) concluded that disruption could occur only when a product or service results in a breakthrough in the traditional way organizations conduct business and customers buy into the change in the innovation. DIT is achieved through improved product performance, and customers start to value the product. However, Bohnsack and Pinkse (2017) cautioned that this process is drawn-out. For example, 3D printing can be a DIT, but the printed parts are not satisfying the robustness prerequisites for some applications, and the innovation is still somewhat pricey for most firms (Bohnsack & Pinkse, 2017). Initially, organizations were hesitant to implement cloud computing due to

the threat of security risk that it posed, which is in line with the DIT Theory by Christensen (Guttentag, 2015). Guttentag (2015) stated that with the introduction of new technology, early adoption is limited due to lack of understanding and profit, which is considered to be unimportant by large organizations that already have established strategies and business logic in place. However, as time goes by and these innovations improved due to growth and experience in using the technology, the disruptive technology becomes more appealing and adopted, which is the case for cloud computing (Guttentag, 2015).

This emergence of new technology's impact on low-end markets is beneficial to my study because organizations are progressively leaning on storing data in the cloud that can be easily accessible by multiple users simultaneously. The risks for implementing cloud computing as a DIT continues to pose security challenges because there is no standardization of security solutions (Hashem et al., 2015). Each organization requires specialized security solutions, thus new challenges continue to emerge (Hashem et al., 2015). Sultan (2015) also stated that the emergence of the American Southwest Airlines is a good example of a combination of new market and low-end DIT. New-market and low-end DIT is due to the strategic goal of the airlines to attract customers that preferred driving cars or riding buses over flying. These customers were enticed by the low-end fares and fewer rules, and the low-end DIT pulled customers out of the major airlines because of the low-end fares (Sultan, 2015). Additionally, Korean automobile makers' business strategy resulted in DIT because they designed low-end cars that were affordable and basic in comparison to the big and fancy American cars (Sultan, 2015).

Presently, cloud computing is viewed as a low-cost DIT that has changed data storage from physical datacenters to being stored in the cloud.

Research findings focused on whether DIT is disruptive innovation or sustaining innovation. Nagy et al. (2016) focus on DIT was based on three questions: what is disruptive innovation? How can a disruptive innovation be disruptive to some and yet sustaining to others? How can disruptive innovations be identified before a disruption has occurred in an organization? The authors redefined DIT as "innovation with the following attributes: radical functionality, discontinuous technical standards, and/or new forms of ownership that redefine marketplace expectations (Nagy et al., 2016). The authors stated that if these newly defined innovation attributes of DIT are utilized by an organization, then the innovation is not considered disruptive. On the other hand, if these attributes are not used by an organization, innovation can result in disruption (Nagy et al., 2016). For instance, cloud computing, a disruptive innovation has redefined marketplace expectations, by physically changing the traditional way of storing sensitive data (Yu et al., 2017). Thus, disruptive innovation is disruptive when it changes the traditional way of organizations doing business by adopting an innovative technology that progressively refines the marketplace expectations.

Future directions for the DIT. More research needs to be conducted to define DIT better and verify its validity. In reviewing and synthesizing the literature available on DIT, the positive benefit of DIT is that organizations can use it to evaluate the emergence of innovative technology by understanding how to implement it (Weeks, 2015). However, the broad definition of this theory indicates that more research is required to

narrow the definition of DIT to avoid misinterpretation and misuse (Weeks, 2015). Additionally, the validity of the DIT sampling size needs more research that should be rigorously peer-reviewed (Weeks, 2015). Organizational decision-making on the use of or rejection of technology should be based on the situation and needs of an organization, as well as the benefit and drawbacks of the success and failure of this technology (Crockett et al., 2013). Implementation of cloud computing, despite the potential security breaches of data, may still provide business and organizations alike a competitive advantage (Carvalho, Andrade, Castro, Coutinho, & Agoulmine, 2017). This advantage takes form in increasing accessibility and autonomy, reducing costs, encouraging resource pooling, and multi-tenancy (Mell & Grance, 2010). Researchers have identified cloud computing as a disruptive innovation, which has gained popularity due to its easy access and flexibility via the Internet (Kranz et al., 2016); however, security measures need to be in place to secure the data of cloud users (Alamoudi & Alamoudi, 2016). These security measures, when implemented, will build the trust and confidence of its users and the organizations to utilize this new disruptive technology.

Contrasting theories. In reviewing research on DIT, contrasting or opposing researchers were identified. There are several theories related to the use of IT and innovative technology that not only influence an organization's core business model but change the business processes (Fador, 2014). Possible theories I considered for my research study were Innovation Diffusion Theory (IDT) also known as diffusion of innovation theory (DOI) and technology acceptance model 2 (TAM2). DOI is a contrasting theoretical framework for my study. This theory by Rogers was developed in

the 1950s, was first used by the U.S. Department of Agriculture, and later used in public health (Rogers, 1962). It is also one of the initial social science theories, which gained steam by spreading through a specific social system (Rogers, 1962). Rogers (2004) defined DOI as the spread of a new idea through various communication channels in a social system. This theory focuses on adopting and bringing about change using new technology (Rogers, 2004). I did not choose it because I am not focusing on IT professionals adopting or disseminating cloud computing.

In addition to DOI, TAM2 was also considered. TAM2 was developed by Davis in 1985 and has evolved over the years (Davis, 1989; Venkatesh & Davis, 2000). It is based on reasoned actions and determines the usefulness of technology to its users (Venkatesh & Davis, 2000). In investigating suitable research frameworks, I considered the new modified model of TAM2, which is the unified theory of acceptance and use of technology (UTAUT). TAM2 clarifies how social and psychological procedures influence users (Venkatesh & Davis, 2000). TAM2 proposed that when users provided a new technology, their choice of utilizing this innovation is based on two factors: how the technology is perceived and is the technology user-friendly (Fador, 2014). TAM2 was not a good foundation for my study because I am not focusing on users' behavior.

Cloud Computing Architecture

Cloud computing architecture is composed of deployment and service models, which provide computing resources for organizations. These services are provided by CSPs via the internet based on the organization's needs, and organizations subscribe to the CSPs to utilize these services. (Igbal et al., 2016; Soni & Hasan, 2017). Cloud

computing continues to evolve into a system that allows IT organizations to provide effective control and management services in a different network environment (Zhang et al., 2018). This use of cloud computing is achieved through real-time access to customers' sensitive data at any time, anywhere as long as there is internet connectivity, and it is affordable (Mell & Grance, 2010). Cloud computing constitutes of service models and deployment models as depicted in Figure 1.

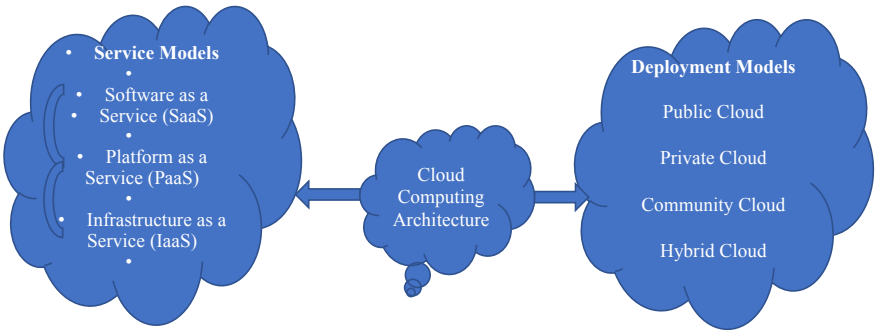

Figure 1. Cloud computing service models.

Cloud computing service models. There are three types of service models provided by CSPs: SaaS, PaaS, and IaaS. These models are arranged in an architectural hierarchy with the SaaS software being the topmost layer, PaaS is the middle layer, and

IaaS is the bottom layer (Barrow et al., 2016). IaaS is the model to be studied for this research. IaaS is a form of cloud computing that is delivered through the internet and remote data centers (Hashem et al., 2015). IaaS is considered the most important component of cloud computing due to its capability of being the foundation of the architectural hierarchy of the entire cloud system and it supports multiple virtual machines (Jathanna & Jagli, 2015). Because of these functionalities, IaaS is susceptible to data breaches. My doctoral study is focused on securing data in private IaaS cloud computing. It is easier to monitor and maintain who accesses data when, how, where, and what in private cloud IaaS versus public IaaS cloud (Barrow et al., 2016). DBAs can easily identify the malevolent users in private cloud systems if a data breach occurs by analyzing the how, where, what, and when data were accessed resulting in the breach or security compromise (Barrow et al., 2016). DBAs will utilize appropriate end-end logging and reporting controls of information of how, who, what, where, and when data are accessed (Barrow et al., 2016).

Although cloud computing is disruptive, cloud computing as an innovative product can adversely affect companies (Werfs, Baxter, Allison, & Sommerville, 2013). Once adopted, cloud computing offers organizations considerable innovation opportunities. IaaS, a type of cloud service model, has gained increasing popularity due to administration display of the assets it provides through CSPs such as clients/machines that incorporate personal computers as virtual machines, data storage, firewalls, load balancers, and network devices (Manvi & Krishna, 2014). IaaS provided data storage, hardware, and application program interfaces (API) (Igbal et al., 2016; Shana &

Abulibdeh, 2017). IaaS was also known as virtual infrastructure (Igbal et al., 2016). Supporting virtualized technologies and infrastructure was achieved through the development of APIs, which allows IaaS to perform administrative functions (Igbal et al., 2016). However, the creation of the APIs makes the IaaS susceptible to data security breaches (Igbal et al., 2016). Storing data in cloud computing is usually done through a third-party. However, this third-party control storing data makes the IaaS database storage susceptible to database breaches by other users sharing the same cloud space and cloud resources (Ali et al., 2018). Additionally, multiple cloud organizations referred to as multi-tenant using the same virtual cloud environment may compromise cloud data and unauthorized access to data. Moreover, the use of cloud through other nodes such as computing, storage, physical, and virtual machines also increase the risk of security breaches (Ali et al., 2018). The use of the cloud multitenancy model by organizations makes organizations susceptible to data breaches with more implications than data breaches in a traditional IT environment (Ali et al., 2018). Additionally, the significant issues associated with IaaS are resource management, data management, network infrastructure management, virtualization and multi-tenancy, application programming interfaces (APIs), interoperability, and security (Madni, Latiff, Coulibaly, & Abdulhamid, 2016). Additionally, Manvi and Krishna (2014) emphasized that multitenancy capability in IaaS is critical because it allows multiple users to share resources to data with locations unknown. This poses a security risk to data protection and legislator issues (Manvi & Krishna, 2014). An example of IaaS is the Amazon Web Service (AWS), which provides EC2 administrations like a virtual machine with a

product stack (Singh & Chatterjee, 2017). Organizations no longer have to purchase infrastructures. Instead, they can access the infrastructure based on their business needs and demands, a feature of cloud computing (Barrow et al., 2016). IaaS also serves as a protective shield of the cloud from outside threats by surrounding it with protective devices such as firewalls and load balancing (Singh & Chatterjee, 2017).

Additionally, IaaS has enabled organizations to provide flexibility to its users with the capability of easy access to their proprietary information anywhere, anytime via a secured Internet (Rubóczki & Rajnai, 2015). However, a key drawback of this web-based cloud computing hierarchy architecture is security challenges because of data pooling, sharing from multitenancy, and data storage in a remote data center. The three cloud computing service models are used based on an organization's business need. However, security challenges remain an issue due to data pooling, multitenancy, and data storage in the cloud. Moreover, Barrow et al., (2016) state that CSPs do not provide 100 % security assurance. Therefore, DBAs need to develop and design security strategies to prevent data breaches in IaaS Cloud computing architecture. This doctoral study focuses on the security strategies that will be used to minimize data breaches in IaaS cloud computing.

Deployment models. There are three cloud deployment models for cloud services: public, private, and community or hybrid. *Public cloud computing* is readily available to the public, and it is associated with security challenges. Public cloud computing is an open cloud managed by the CSP, and the physical framework may be located at an off-site area of the client (Singh & Chatterjee, 2017). The cloud assets are shared among the numerous users and organizations pay the CSP based on their business

needs (Singh & Chatterjee, 2017). *Community cloud computing* involves sharing infrastructure by a group of organizations, and this empowers the sharing of assets (mission, security policies) by organizations while keeping up the proprietor's restrictive access to the devices (Apolonia, Freitag, & Navarro, 2017; Singh & Chatterjee, 2017). Community cloud computing serves as a virtual community for a specified group of users in an organization (Deng, Yang, Du, & Song, 2018).

Private cloud computing is solely owned by an organization. Private clouds are managed internally by a third-party or CSP (Singh & Chatterjee, 2017). Private cloud computing is used by various departments in an organization (Taylor, 2017). The use of private cloud is determined by the organizations (Taylor, 2017). It may also reside in the organization or at an offsite location. The utilization of private cloud by organizations is deemed as a cost-saving measure because it allows the organization to evade regulatory control or jurisdictional issues that might be related to open cloud contributions (Taylor, 2017). A drawback of private cloud is that even though it has expanded versatility, it may need huge numbers of the institutionalized practices for interoperability expected out in public cloud (Taylor, 2017). Cloud computing offers robust computing clout and a vast storage data capacity for organizations, which includes private data of government sensitive information (Zhang, Yang, & Chen, 2016). This vast data cloud storage poses the risk of data breaches by malevolent attackers, which may result in data theft and loss of proprietary and sensitive data. This data theft and loss may not only impact government employees or staff, but it may also result in legal concerns that may impact the Health Insurance Portability and Accountability Act (HIPAA) (Zhang et al., 2016).

Despite private clouds being managed onsite of the government agency, there remain security threats. Private cloud computing is the environment chosen for this study. Goyal (2014) posited that private cloud computing provides organizations with more security control of their proprietary information than public cloud computing. Since private cloud computing is hosted in the organization's data center, it limits who has authorized access to proprietary data and this aspect minimizes data breaches (Goyal, 2014).

Hybrid cloud computing is a combination of two or more clouds utilizing the same infrastructure and capabilities (Singh & Chatterjee, 2017). It involves part of the private and public clouds. For the private cloud aspect, organizations utilize security benefits such as cloud sensitive password protection between specified users (Yu et al., 2017). As for the public cloud aspect, organizations benefit from its cost-savings such as increased collaboration and sharing of resources that are cost-saving (Yu et al., 2017). Thus, this increased collaboration between organizations strengthens trust among partners (Yu et al., 2017).

Cloud Computing Data Security Risks

Storing data in cloud computing is a new product or technology that has changed the way IT organizations store data, As noted in the DIT, new innovative technology poses risks. Organizations are now storing data in the cloud instead of in the traditional physical data centers (Shahzad, 2014). While there are many benefits of adopting cloud computing, there are also some key data security risks to implementation. One of the topmost obstacles in implementing cloud computing is security risks about privacy. For organizations to implement cloud computing infrastructure, data security and data

migration to CSPs must be considered. With the evolution of cloud computing, organizations are now in a data-driven world that requires managing the security of data (Davoll, 2017). Databases store data that contains proprietary information of organizations and this proprietary information is a target for malevolent behavior (Dayıoglu, Kiraz, Birinci, & Akın, 2014). Due to the increased risk of potential attacks to gain access to the proprietary information in databases, DBAs have challenges to maintain and secure the data in the cloud (Dayıoglu et al., 2014). Moreover, Dayıoglu et al. (2014) emphasized that with cloud computing services increased use by government and private organizations, security measures should be implemented to resolve the increase potential attacks of the data in cloud computing.

However, due to the global use of the internet, cloud computing poses new data challenges such as data confidentiality of personally identifiable information (PII) and safeguarding of the physical data storage (Srivastava & Kumar, 2015). Internet use has also posed worldwide financial, political, and social impact, where strict directions do not generally oversee the utilization of Internet assets (Sindhu & Mushtaque, 2014). Moreover, cloud computing uses the internet to access data, and this public access to sensitive data via the Internet poses different vulnerabilities to data security (Flores, Antonsen, & Ekstedt, 2014; Srivastava & Kumar, 2015). Despite all the benefits of cloud computing, organizations continue to hold back on investing in it due to its security risks and data storage that relieves organizations from controlling their data. Although cloud computing has been lauded as a utility, there remains increasing concerns about data security and privacy when organizations lose control of storing their data in their own

data centers to CSPs (Shahzad, 2014). Shahzad (2014) summarizing the National Institute of Scientific Technology (NIST) framework, warned that data security is the leading challenge for cloud computing due to the outsourcing of data to third-party CSPs, and this has made organizations reluctant to invest in this new technology. A customer's sensitive data (financial data, social network profiles, and medical records), once outsourced to a third-party, CSPs are no longer considered private (Shahzad, 2014). Despite the efforts by CSPs to implement security measures such as firewalls and virtualization, these measures are inadequate to safeguard against data breaches (Shahzad, 2014). Because keeping sensitive data in the cloud remains a security priority, DBAs must ensure they understand the potential problems that come along with implementing the cloud within their infrastructure and weigh these problems against the potential benefits. DBAs understanding the security strategies that can be used to prevent data breaches in cloud computing supports the research question for this study.

Security measures for storing data in cloud computing remain ongoing, and there is still no institutional standardization for it. Data privacy and integrity are still pivotal concerns when migrating data into the cloud and this requires improved data security (Shaikh & Sasikumar, 2015). Moreover, the lack of standardized security measures is the limiting acceptance of cloud computing by organizations because concerns about data confidentiality and integrity remain. Security measures to safeguard data confidentiality is still a work in progress, and data encryption seems to be the topmost security measure that may work to build confidence in organizations to utilize cloud computing (Rao & Selvamani, 2015). Security challenges remain a pivotal concern by organizations to adopt

cloud computing. Modi and Acha (2016) stated that SLAs may help minimize the IaaS cloud computing attacks since there is no legal policy in place to protect data breaches. The lack of legal policy to protect data in the cloud will compromise data security in cloud computing. Finally, the lack of standardized policies and inconsistent SLAs to govern cloud computing during data breaches remains a major concern for organizations, and security strategies need to be implemented to secure data storage in IaaS cloud computing. Without SLAs and insecurity policies in place, DBAs need to identify security strategies that will minimize possible data breaches in IaaS cloud computing that may be used as best practices in the future.

Storing data in cloud computing is increasing among organizations, and the security challenges associated with the centralized storage of data by organizations pose a security risk. Protecting data in IaaS cloud computing is a complex security challenge. A common security challenge is data sharing by numerous tenants referred to as multi-tenancy. Ali, Khan, and Vasilakos (2015) described multi-tenancy as sharing of resources in a physical location by multiple users without any linkage. In IaaS cloud computing, multi-tenancy and APIs pose security risks. Multi-tenancy is also one of the most common issues associated with IaaS cloud computing (Madni et al., 2016). Another security challenge in IaaS cloud computing is safeguarding data in transit, data at rest, and data during processing (de Fuentes, González-Manzano, Tapiador, & Peris-Lopez, 2017). In summary, IaaS cloud computing is a disruptive innovation product that has many advantages, but the IT functionality of storing data in the cloud poses major security challenges that should be addressed by DBAs. The research studies mentioned in

this paragraph spotlights the need to incorporate successful strategies to secure data in IaaS cloud computing by DBAs.

Strategies Used to Secure Data in Cloud Computing

The emergence of cloud computing has changed the way organizations do business. Shahzad (2014) stated that cloud computing has changed the way organizations conduct business due to its on-demand services such as SaaS, PaaS, and IaaS. These services are easily accessible anywhere and anytime via a secured network. Storing data in cloud computing is a new business perspective that is attractive to organizations due to its computational resources based on the organizations' needs (Silva, Barbosa, Marinho, & Brito, 2018). Even though storing data in cloud computing poses security challenges, the cost savings attached to it is an enticing benefit that has enabled 80% of organizations to cut costs by 10-20% (Bayramusta & Nasir, 2016). Despite the security challenges that cloud computing poses, organizations are still motivated to implement cloud because of its economic benefits such as a reduction in capital and operational expenditures and shared services such as software, hardware, and physical infrastructure (Kaaniche & Laurent, 2017; Silva et al., 2018). The shared services provided through shared infrastructure pose both internal and external threats of data breaches such as the stealing of passwords and unauthorized access to the application programming interface (API) (Silva et al., 2018). Therefore, protecting proprietary and sensitive data are a top priority for DBAs managing cloud computing databases. As a result of these security concerns, protective strategies must be implemented to minimize these human threats of stealing passwords and exploiting the cloud computing database. Therefore, because of the

potential security concerns posed by cloud computing data storage, DBAs will need to develop security strategies to secure data in private IaaS cloud computing.

Only a few security methodologies are effective in ensuring information security within the cloud; data encryption is suggested as one of the topmost solutions to safeguarding data in IaaS cloud computing (Rao & Selvamani, 2015). DBAs can utilize encryption strategies such as scrambling data before storing it in the cloud server (Rao & Selvamani, 2015) to better secure information. Employing this strategy helps prevent access to data from various clients and makes the information unusable (Rao & Selvamani, 2015). Researchers Dayıoglu et al. (2014) believed that CrytDB, a database management system, may help prevent database attacks in cloud computing effectively utilizing SQL queries. Furthermore, CrytDB is a viable contrast to other endeavors at addressing the security challenges of encrypted data, because it allows easy migration of the data to cloud without security. After all, data are already encrypted, and the data in its encrypted form is not revealed to the CSPs (Dayıoglu et al., 2014). Barrow et al. (2016) proposed the use of the DESCAST algorithm. This use of the DESCAST algorithm by DBAs will ensure data are encrypted while transferred via the network from the server and will remain encrypted at rest in the cloud server (Barrow et al., 2016). Barrow et al. (2016) believed that the DESCAST algorithm will secure the data from brutal attacks and compromise via birthday glitches. Barrow et al., (2016) are confident that the DESCAST algorithm is stronger in comparison to other algorithms. For the successful implementation of cloud computing services within an organization, DBAs must identify

adequate strategies to implement and prevent data breaches in private IaaS cloud computing.

Additionally, DBAs developed data hiding techniques to secure data from being exploited and compromised. Watermarking and data encryption are two of the most preferred strategies used by DBAs to secure data in cloud computing (Yesilyurt & Yalman, 2016). Digital watermarking and encryption prevents unauthorized users to access data secured in cloud computing by validating the authentication of the user accessing the cloud database (Yesilyurt & Yalman, 2016). Accomplishing validation of the user's identity is done through invisible digital watermarking and the use of encryption algorithm to prevent violation of the user's data confidentiality, data integrity, and authentication rights (Yesilyurt & Yalman, 2016). Additionally, Tankard (2017) believed that the use of data encryption diminishes the exploitation of data in cloud computing through cyber-attacks. Despite encryption being a means of data protection in cloud computing, DBAs should also employ other strategies to secure data by using endpoint security, network security, application security, and physical security systems (Tankard, 2017). Therefore, the use of data hiding security strategies such as digital watermarking and data encryption by DBAs will secure data in private IaaS cloud computing.

Auditing protocol is another way to secure data in the IaaS cloud computing. Jian, Dengzhi, Qi, Debiao, and Xingming (2017) proposed that besides data encryption to secure data, organizations should consider data auditing protocol by a third-party to adhere to the security requirements of data privacy and verification in cloud computing

infrastructure. This new technique will assure DBAs that shared resources in the cloud will be protected from forgery attacks (Jian et al., 2017). Moreover, researchers have proposed various schemes to secure data and its integrity when stored in the cloud. For example, Xu, Wu, Khurram, Choo, and He (2017) proposed using a public data auditing strategy associated with variable-size file blocks. Another strategy used by DBAs to secure data in IaaS cloud computing is the use of firewalls. A firewall is a means to secure sensitive data and proprietary information from data breaches and unlawful access (Flores et al., 2014; Sindhu & Mushtaque, 2014); therefore, DBAs can benefit from using firewalls as a means to secure their data in cloud computing.

Another common security strategy employed by DBAs is the use of multifactor authentication. Using single passwords regardless of how strong it is with a mix of letters, numbers, and symbols are no longer secure to protect the authorized user's identity. Multifactor validation of users password is now the emerging strategy which uses not only a fixed password, but also demands two or more proof of the three types of verification factor types: knowledge of what you know (password), what you possess, (Personal identification verification (PIV) card) and what you are (Jim, 2013). This validation is used by the user using the single password, plus a code sent to the user's personal mobile phone on file for the user to access the database. This multifactor verification process makes it difficult for an unauthorized user to fraudulently log in to the database. A fraudulent user may gain easy access to an authorized user's password via a phishing email, but with the multifactor authentication process in place, the person

will be unable to access the database (Jim, 2013). Moreover, the use of multifactor authentication will secure data in private IaaS cloud computing.

Principles of data security for design and implementation. Designing and implementing data security in IaaS cloud computing should be centered on the three principles of data security: confidentiality, integrity, and availability (CIA). Tchernykh, Schwiegelsohn, Talbi, and Babenko (2019) defined confidentiality as a set of rules that restricts unauthorized access to PII. Tchernykh et al. (2019) described integrity as an entire information structure, which is a fundamental concept of data security and the data stored in the cloud ought not to be changed by anyone other than the proprietor. The availability of data means that the data are available to users at any time (Tchernykh et al., 2019). According to Aminzade (2018), the three principles of data security is the classic CIA triad and he purported that the CIA is used to make business saving decisions, identify security deficiencies, and develop a mitigation plan for risks. Data security threats are present wherever there is data with some intrinsic value, and securing data should be paramount. Therefore, data security for the design and implementation of systems must be centered on the three principles of data security: CIA. Currently, DBAs embrace the three principles of data security CIA to ensure data security in the IaaS cloud computing. Managing data breaches remains challenging due to proprietary ownership of data stored in cloud and data sharing via multitenancy (Weinberg, Milne, Andonova, & Hajjat, 2015)

With the global use of the internet and increased connectivity, in safeguarding PII and data transmission, DBAs need to protect customers' data by maintaining its CIA

(Weinberg et al., 2015). Designing and implementing the data security triad CIA is now a paramount goal of organizations to gain customers' respect and trust (Weinberg et al., 2015). With the advancement in IT technology, storing data in the cloud has yielded more attention to data security due to data breaches or node crashes (Wang, 2017). Wang (2017) also added that data stored in IaaS cloud computing is now the new way of storing data and the data owner has minimum control of its data (Wang, 2017). Data security impacts CIA. Kumaril and Mrunalini (2018) supported the idea that storing data in IaaS cloud computing is complex because the data owner loses control of the data and is unaware of where the data are stored. The lack of ownership and not knowing where the data resides posed a security challenge (Kumaril & Mrunalini, 2018). DBAs can design and implement certain security strategies to minimize the security challenges posed by storing data in the cloud by securing the three principles of data security: CIA. In terms of confidentiality, DBAs need to design and implement a secure network to prevent the exploitation of data and data leakage (Kumaril & Mrunalini, 2018). DBAs focus should be centered on maintaining data integrity by keeping the data from manipulation by unauthorized users (Kumaril & Mrunalini, 2018). DBAs should meet the data availability requirement by designing and implementing a system, which is always functional to ensure reliability and flexibility (Kumaril & Mrunalini, 2018).

Strategy: Infrastructure design and analysis. Data security needs to be included in IaaS cloud computing infrastructure design and analysis. Maluf, Sudhaakar, and Choo (2018) in the context of data security in the cloud computing environment stated that a typical attack happens when the unauthorized user is probing for weakness

or vulnerabilities that can be manipulated. Ali et al. (2015), concurred that cloud computing due to its capability to centrally store and access data, is a potential threat for data breaches. The central storage of data in IaaS cloud computing poses a threat to exploitation by internal and external threats of data at rest and in transit (de Fuentes, et al., 2017). Storing data in the cloud environment poses security challenges. Information Technology & Innovation Foundation (ITIF) declared that cloud computing is increasingly becoming popular, and 93% of United States businesses depend on it for data storage; and over three million data centers are operating to meet the increasing need of cloud computing services (Tinkler, Smith, Yiannakou, & Robinson, 2018). These security challenges occur because customers lose control of their proprietary data by outsourcing data to CSPs who have to manage it in a virtual environment (He et al., 2016). These security threats are increased because the organizations are unaware of who is utilizing data and deleting data (He et al., 2016). Moreover, the basis of the security challenges is due to data sharing in the virtualized cloud computing environment (He et al., 2016). Therefore, due to the increasing risks of security challenges that may impact data security, DBAs need to identify strategies to reduce security risks and secure data.

Since migrating data into the cloud poses security challenges, DBAs need to design ways to secure data and maintain its integrity (Xu et al., 2017). Entrusting physical data control to CSPs remains questionable by organizations because financial reasons may lead the CSPs to delete data to minimize management and decrease data storage costs in cloud computing (Xu et al., 2017). Furthermore, customers' data might

be lost or tainted due to software or hardware faultiness, managerial errors, or data breaches against the CSPs (Xu et al., 2017).

Strategy: Database application and design. In my doctoral study, I chose to focus on private IaaS cloud computing data security. McKendrick (2018) stated that private cloud computing provides heightened data storage security than public cloud, but this remains unproven. Due to the live migration of data entrusted to a third-party, data theft and privacy is a major concern because the live data migration from the server through the internet may be compromised (Alamoudi & Alamoudi, 2016). Alamoudi & Alamoudi (2016) identified cloud risks such as data explosion, governance, skill sets, data portability, and data protection. If the employees are not properly vetted, the private data can still be hacked due to unauthorized access. Therefore, it is the goal of DBAs to ensure the optimal performance of the database so that data confidentiality and security are maintained (Davoll, 2017). DBAs should also be knowledgeable about how to maintain an effective database that has information readily available in real-time (Davoll, 2017). The DBAs are also responsible for incorporating strategies that secure database management systems and training staff on how to effectively secure data and adhere to privacy policies (Davoll, 2017). With the increased use of data storage in the cloud, DBAs have to be skilled and knowledgeable about managing data in the cloud, as well as securing data to prevent data breaches (Davoll, 2017).

In the past, DBAs' roles were mundane and included maintenance of mainframe. However, with the increasing implementation of cloud computing by organizations, DBAs are challenged with managing data in the cloud and learning about new

technologies to resolve database administration (McKendrick, 2015). Moreover, data security ranks as one of the top three challenges DBAs face when data are stored in the cloud. The three top challenges that DBAs face are the growth of unstructured and structured data (66%), improving data security in the cloud (55%), and implementing data in cloud computing (35%) (McKendrick, 2015). In summary, with the evolving role changes of DBAs, DBAs have to remain knowledgeable about new technologies and develop strategies on how to secure data in cloud computing to prevent data breaches.

Strategy: Data storage security. IT organizations are now utilizing IaaS cloud computing to store data due to cost savings, improved performance, and adaptability than the customary physical data centers without thinking of management of the physical data centers (Ardagna, Asal, Damiani, & Quang, 2015). However, concerns still linger about the data storage security in IaaS cloud computing. Ardagna et al. (2015) stated that security concerns such as vulnerabilities and attacks focus on the three principles of data security CIA at three levels: Application level, tenant level, and provider-on-tenant or tenant-on-provider level.

Xiang and Zhu (2019) stated that entrusting data in cloud computing to CSPs poses a security threat for organizations and this impacts CIA of data. Arki, Zitouni, and Dib (2018) research also supported that data stored remotely in the cloud poses concerns because IT organizations are still worried about the security of their data and the guarantee of the confidentiality and integrity of the data. Despite the benefits of cloud computing such as multi-tenancy and remote data storage, data security remains a topmost concern on how to maintain data security (Arki et al., 2018). Moreover, the IT

organizations are perplexed about remotely storing their sensitive data in the IaaS cloud computing (Arki et al., 2018). Therefore, the attributes of cloud computing such as multi-tenancy and data storage pose a data storage security risk among the users of cloud computing (Arki et al., 2018). Research on securing data storage in cloud computing remains ongoing by protecting CIA of data. My study emphasizes the need for DBAs to understand and maintain awareness of data breaches in IaaS cloud computing and to identify the successful strategies to be used to minimize the data breaches.

Literature has revealed that there are several strategies used to secure data in private IaaS cloud computing, and encryption seems to be the first line of defense in securing data. Ye and Ng (2019) pointed out that encryption is a means of protecting data in cloud computing from attacks. Tankard (2017) also noted that encryption and key administration ought to be viewed as the foundation of any information security. Tankard (2017) recommended that data encryption should be done when data are stored, at rest, and in transit separate from the encryption key. The use of encryption minimizes data breaches. When data encryption is used, it maintains the CIA of data (Parisha, Khanna, Sharma, & Rizvi, 2017). On the other hand, Ardagna et al. (2015) proposed four forms of cloud security solutions: encryption, signature, access control, and authentication. DBAs need to identify security strategies that will help minimize data breaches in private IaaS cloud computing.

Another data storage security strategy used by DBAs is authentication. According to Yesilyurt and Yalman, (2016), authentication is a strategy used to verify the user's identity, which prevents unauthorized access to data CIA. A common authentication

strategy now used by DBAs to prevent data breaches in IaaS cloud computing is multifactor authentication. Multifactor authentication is used to safeguard data in IaaS cloud computing by ensuring that data CIA. Simon (2019) pointed out that multifactor authentication is reliable than complex passwords because it uses two forms of verification (a password and something the user possesses) to prevent data breaches in IaaS cloud computing. Heatherly (2016) supports the use of multifactor authentication to safeguard data CIA to prevent data breaches in IaaS cloud computing.

Authorization is granting access rights to users based on their roles in their IT organizations. Cusack and Ghazizadeh (2016) suggested that authorization is based on users' access control to the data stored in the IaaS cloud computing. DBAs provide users' access controls to the data stored in the IaaS cloud. Foresti, Paraboschi, Pelosi, and Samarati (2018) noted that regulatory rights are given to the users to different parts of the data to maintain data confidentiality. Ramachandran and Chang (2016) also believed that authorization is permitted using the user's role in the IT organization. Ramachandran and Chang (2016) also revealed that granting authorization to users is using access controls such as a unique user ID and password. DBAs can track the assigned user IDs to specific users of the data to monitor any suspicious network activity to prevent data breaches.

Data auditing is pivotal in cloud computing to maintain data integrity. Tian et al. (2019) were concerned that CSPs may tend to or even purposely erase data once in a while belonging to some data owners to save data space in IaaS cloud computing. Therefore, data auditing is critical to creating effective reviewing processes to guarantee data integrity in the cloud. Sookhak et al. (2015) also concurred that entrusting data in the

cloud o CSPs makes it susceptible to both internal and external threats, which may impact data integrity. Data auditing is a means of scrutinizing and identifying data corruption and ensuring it remains intact (Sookhak et al., 2015). DBAs need to consider using data auditing to ensure data integrity of data stored in IaaS cloud computing to prevent data breaches. Additionally, Sookhak, Yu, and Zomaya (2018) questioned the data integrity of data stored in IaaS cloud computing to CSPs. Sookhak et al. (2018) found instead that having data auditing procedures in place is required to ensure data integrity of data stored in IaaS cloud computing. Data auditing is a security control measure in cloud computing that DBAs can utilize to minimize data breaches in IaaS cloud computing.

Outsourcing data storage to CSPs has increased because it reduces the cost of physical storage of data and this relieves IT organization of management and data maintenance (Subha & Jayashri, 2017). Research purported that 79% of organizations have decreased their spending on physical data centers by outsourcing data to CSPs to focus on strengthening their business and improve efficiencies (Subha & Jayashri, 2017). Securing data in cloud computing requires maintaining data integrity through data auditing to prevent data breaches. DBAs can use this data auditing strategy to minimize data breaches in private IaaS cloud computing. However, Garg and Bawa (2016) emphasized that there are different types of auditing protocols used for data auditing in the cloud, and more research is still needed to identify the most successful data auditing protocol. The above research studies spotlight the need to incorporate data auditing in IT

organizations to mitigate data breaches by recognizing that data stored in the cloud and managed by CSPs require auditing to ensure data integrity is maintained.

Strategy: Management issues. Data security is not a priority by IT organizations. IT leaders do not completely comprehend the importance of security controls and are less inclined to enforce security controls, which places data integrity at risk (Noguerol & Branch, 2018). Data confidentiality and integrity risks pose management issues for IT leaders. Gale (2018) posited that IT organizations are faced with increased pressure to secure the confidentiality of data for their customers. Gale (2018) also stated that after the Facebook privacy scandal in 2018, organizations are now open to mitigate data breaches. Moon, Choi, and Armstrong (2018) also agreed that IT security executives are constantly on the edge trying to adapt the information needs of the business with the IT security resources. Managing data security is challenging, and IT leaders have to ensure that their data are secured by implementing security controls to minimize data breaches in IaaS cloud computing. It is the DBAs' role to ensure that security measures are in place to prevent data breaches in IaaS cloud computing.

To manage data security issues, IT leaders need to buy into updating their systems from data breaches consistently even if their data storage systems are free of such breaches. Choong, Hutton, Richardson, and Rinaldo (2016), expressed concerns that the budget allocated to data security by IT organization leaders remains minimal despite the increasing challenges posed by data breaches. Therefore IT organizational leaders should invest enough funds toward data security to mitigate data breaches (Schniederjans & Hales, 2016). Since cloud computing continues to evolve and has changed the way

organizations do business, DBAs need to implement and manage security controls to minimize data breaches.

Transition

The primary focus of the literature review was to study prior research of IT business professionals who addressed barriers when adopting cloud computing technology. The framework of the discussion explained how low-end disruptive technology such as cloud computing, improves products and system performance. Section 1 also addressed the following topics for this research study: defined the IT problem, provided the background of the problem, specified the problem statement, and the purpose statement.

Section 2 will focus on the role of the researcher, participants, research method and design, population sampling, ethical research, data collection/ instruments/ techniques, reliability, and validity. Section 3 will examine the research findings and how the conceptual framework is linked to the research findings. Additionally, this section will also review the effects of the findings on social change as conveyed regarding tangible improvements to individuals, communities, organizations, institutions, cultures, or societies. Finally, this section will discuss future recommendations and actions, and a convincing concluding statement.

Section 2: The Project

In this doctoral study, I investigated the strategies DBAs used to secure data in private IaaS cloud computing. This section includes an explanation of the role of the researcher, participants, research methodology, research design, population and sampling, and ethical research procedures. I also described the data collection instruments, and techniques, the public organizational documents; the data analysis plan; and reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies DBAs used to secure data in private IaaS cloud computing. The targeted population consisted of DBAs in 2 IT organizations located in the state of Maryland who have successfully implemented at least one IaaS cloud computing security strategy within the past 3 years in their organizations to prevent data breaches. The results of this study may provide a better understanding of the security strategies that DBAs in IT organizations used to minimize costs for data breaches. Application of study findings by DBAs may allow IT businesses to stay competitive with potential business growth.

Role of the Researcher

I was the central instrument of data collection for this qualitative research study. In qualitative research, the researcher is involved in all phases of the study from characterizing an idea to the configuration, interviewing of research participants, interpretation of results, confirmation of findings, and coding of concepts and themes (Sanjari, Bahramnezhad, Fomani, Shoghi, & Cheraghi, 2014). The researcher is, thus,

central in the instrumentation process used in qualitative research (Sanjari et al., 2014). I was responsible for creating the interview questions and the interview protocol guide, and choosing the research participants. As the central instrument for data collection, I collected data personally from the research participants. I followed Yates and Leggett's (2016) protocol by initiating interviews by asking open-ended questions to generate themes that can be later reviewed and examined. Identification of themes was done by perusing interview transcripts or other printed material to identify themes or codes. My analysis of data was deductive because my study was explorative and used an existing framework. Yates and Leggett stated that valid evaluation of data and generation of themes leads to solving the research questions or creating new research questions. Peters and Halcomb (2015) suggested that semistructured interviews allow the researcher to develop predefined questions, which generates rich participant responses that improve understanding of their experiences and views.

I used the interview protocol to pose the same questions to research participants. Castillo-Montoya (2016) stated that using strong interview guidelines captures meaningful data based on the participant's experiences. I conducted the interviews using predefined open-ended, semistructured questions. This approach allowed me to delve deeper into information as the research participants responded to the questions. I managed the interview guidelines by ensuring that unforeseen issues did not occur such as room temperature control, poor lighting, and noise distractions. This proactive approach of interviewing research participants generated more robust data, which, I believed, reflected the participants' experiences and perceptions. In addition to the

semistructured interviews, I examined and reviewed the organizational documents focused on security strategies. The focus of my interview questions and document review was appropriate because my research study will be focused on exploring the security strategies DBAs use to prevent data breaches in IaaS cloud computing.

Furthermore, I examined the data collected from my interview notes and used a personal diary to notate interview observations. An audio recording of interviews was a key component of the interview, which improved data evaluation (see Yates & Leggett, 2016). My diary contained descriptions of issues raised during the interviews, which was useful when coding and identifying themes. This participatory action by the research participants was a form of data collection that ensured continuous improvement through planning, acting, observing, and reflecting (see Yates & Leggett, 2016). I also observed members' responses or difficulties while reacting to the interview questions and knew when to ask probing or follow-up questions appropriately. These follow-up questions allowed further elaboration on the participants' responses (see Reid & Mash, 2014). I asked the participants if I could audiotape them. If they agreed, all interviews were audio-recorded, transcribed, reviewed, and the data analysis of the data was done using qualitative data analysis software to determine codes and themes.

I currently reside in Laurel, a city in three counties: the northern Prince George's County, Anne Arundel County, and Howard County, Maryland, United States, located midway between Washington, DC, and Baltimore. I selected my research participants from two IT organizations located in Baltimore. Residing in Laurel had no impact on the choice of potential participants selected for this doctoral study. I had no past connection

with the two organizations or the potential research participants. Before the beginning of this study, I was not a subject matter expert in cloud computing. Conducting semistructured interviews also prevented my knowledge of the topic from biasing study results because questions focused on the research participants' experiences resulting in comprehensive data collection. In addition, participants' responses were audio-recorded and transcribed verbatim. As the instrument for this doctoral study, I listened carefully and adjusted or changed paths during the interview process. I also followed my intuition during the interview process by adhering to the interview protocol. Castillo-Montoya (2016) stated that even with the change of paths during interviews, the researcher should still adhere to the interview protocol and not deviate from it. Finally, I followed the interview protocol while remaining sensitive to the verbal and body cues of the research participants.

I have more than 17 years' experience in IT and contracting businesses. This experience helped increase my awareness and sensitivity of the issues and challenges identified with key and strategic IT innovations and developments. Reid and Mash (2014) stated that a qualitative research study is subjective and the researcher brings his or her own bias regarding the research study (Reid & Mash, 2014). This bias was mitigated through the use of the interview guidelines and the recording of interviews (see Reid & Mash, 2014). Getting the participants to validate the interview transcript ensured that the data collected reflected their experience and perceptions as well as minimized bias (see Morar et al., 2015). Experts contend that this validation by research participants of the recorded interviews improves the credibility of the study (Thomas, 2017).

Methodological triangulation was done by comparing the feedback and edits received from research participants with internal and external documents to minimize bias and also validate findings. Examples of internal and external documents include communication tools, white papers, presentations, and blogs (Kranz et al., 2016). In Section 3, I listed the organizational documents I reviewed.

Moreover, I internally pilot-tested my interview questions with my peers, as well as reviewed the interview findings with them to validate the consistency of the findings and how they sounded. Kallio, Pietila, Johnson, and Kangasniemi (2016) emphasized that to mitigate researcher bias, the interview guide should be tested to detect uncertainties and leading questions. Additionally, the researcher could also role-play as a participant and answer the interview questions posed by another researcher, to get a feel for answering sensitive questions and to ensure that the study is ethical (Kallio et al., 2016). Therefore, as the researcher of this doctoral study, I removed bias by adhering to the interview guidelines and audio-recording and transcribing all interviews verbatim.

I protected the rights of all the research participants participating in this study. The protection of the rights of the research participants was accomplished by following the guidelines of the *Belmont Report*. The *Belmont Report* was established in 1979 by the National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research as an ethical guide to safeguarding research participants' rights involved in a research study. The Belmont Report focused on three primary ethical principles that were adhered to when conducting research: respect for individuals, beneficence, and justice (The Belmont Report, 1979; Miracle, 2016). Respect for

individuals was done by giving the research participants the autonomy to decide whether they would like to participate in the research study (Miracle, 2016). Voluntary participation was done in my study by informing the research participants that they had the right to decide to participate in the research study or not. I also gave the participants time between questions and assessed their level of comfort to adapt to the interview protocol. Beneficence entailed protecting the research participants from harm. Beneficence was done by making the participants aware of any known or unknown possible harm that may occur during this study using a consent form. Approval of the study from Walden University Institutional Review Board (IRB) further protected the research participants from harm. The IRB's basic role was to examine the research standards and shield participants from hurt and ensuring that risks are minimized. Informed consent was completed to protect the research participants from harm, voluntary participation, and withdrawal from the study without retaliation. Justice was met by treating all research participants equally and fairly and informed them they can change their minds in participating in the research study without fear of retaliation (Miracle, 2016). Confidentiality was maintained throughout the interview by keeping the participant's names anonymous. All participants were treated equally without discrimination (Miracle, 2016). The research participants were informed about the inclusion and exclusion of the research study such as the age limit and experience criteria. Finally, as the researcher, my goal was serving as the participant's advocate and evaluated their ability to provide informed consent. Serving as the participant’s advocate was done by ensuring detailed information was provided to them about the research

study, assessed the participant's knowledge about the risk and benefits of the study and any possible consequences, and the participant's rights whether to participate or not in the study (Miracle, 2016).

Participants

The target population for the qualitative study was focused on two IT organizations in Baltimore Maryland with successful implementations of cloud computing. These two IT organizations stated that cloud computing has been cost-effective and allows their staff to access data anywhere and anytime without problems and the organizations trust the cloud providers storing their proprietary data in the cloud. Additionally, I used a set of participant criteria to identify successful implementations of cloud computing based on asking general questions about the organizations have experienced data breaches in cloud computing. The DBAs in the two organizations selected stated that data breaches have not been experienced by their organizations. Potential participants were four Database Administrators (DBAs) from each organization engaged in security strategies to secure data in private Infrastructure as a Service (IaaS) cloud computing. Consent was obtained from the DBAs in both organizations to gain their voluntary participation in the research study. Informed consent could be challenging to obtain from some participants because they felt that they have unofficially consented to participate in the interview (Peticca-Harris, DeGama, & Elias, 2016). Since informed consent can be challenging to obtain at times, I ensured that the consent form clearly stated the purpose of the study, described the details, participants' option to voluntarily participate in the study with the option to withdraw from the study at any time

without retaliation. A copy of the signed consent form was given to each participant. Reid and Mash (2014) added that the interview questions were designed to gather comprehensive responses from each research participant. Semi-structured open-ended questions were asked to build trust with the participants and strengthen the working relationship. For researchers, the use of open-ended questions allowed the participants to elaborate on their experiences instead of giving one-word responses (Tinkler et al., 2018). I asked each participant open-ended questions, and all the participants were asked the same question in chronological order. I made sure the interview questions were clear, short, and logical. Follow-up questions were generated from the initial interview questions based on the participant's responses. The use of the interview guide created a structured environment (Tinkler et al., 2018).

The eligibility criteria for the potential participants included the following: the DBAs were 28 years or older with an IT work experience of five years or more, and three years of cloud computing experience as related to data security. Etikan (2016) stated that one of the criteria for participant’s selection was based on their knowledge and experience. The criteria that I used to select my research participants was based on five years of IT work experience, and three years of cloud computing experience as related to data security. The nonrandom technique was beneficial for this qualitative study because of limited resources and time (Etikan, 2016). Once provisional IRB acceptance was received from two of the IRB members at Walden University, I contacted a few IT organizations in the Baltimore area to identify the organizations that had implemented cloud computing. Contacting the organizations allowed me to identify potential research

participants and I sent each participant a letter of invitation (Appendix B) via e-mail or U.S. postal mail. Working as an IT Specialist for the federal government, I was aware of several IT organizations that had contracts with the federal government that I could reach out to. The size of the company varied, but I was focused on companies with 10- 20 employees. Peticca-Harris et al. (2016) cautioned that gaining access to research participants can be arduous at times, but once accomplished, there is a joyful relief of progress by the researcher. I obtained permission from two of the organizations to interview employees for my research study based on the inclusion and exclusion criteria developed. I obtained an email list from the Chief Information Officer (CIO) of employees meeting the inclusion criteria for my research study and sent emails to these potential participants informing that participation in my study was voluntary and their decision not to participate would not lead to retaliation by their organization. The email gave the participants two weeks to decide to participate. A timeframe of whether to participate in a research study allows participants to ask questions and make their informed consent (Tinkler et al., 2018). Once consent was obtained from the participants to participate in my research study, details of the date, time, location and other requirements of the interview were outlined. I also had an informal discussion (either via telephone or face-to-face upon receipt of the e-mail responses) with the research participants before the semi-structured interview to get a sense of their experience and feelings of the interview. To further gain trust from the participants, I shared my interview questions with the participants before the interview to acquaint them with the questions that would be asked. I also obtained data from IT security policies and

procedures, and organizational documents related to strategies minimizing database breaches. Palinkas et al. (2015) emphasized that research participants who met the researcher's eligibility criteria, owned knowledge of the topic of interest, and this provided rich data for the study. With all these interview strategies in place, this provided rich data collection from the research participants.

Research Method and Design

This section described the research method used for this study, justified why this specific research method was used over other research methods, and why the research design selected was appropriate for researching the problem statement.

Research Method

Since the qualitative method was exploratory, I chose a qualitative study to explore strategies database administrators used to secure data in private Infrastructure as a Service (IaaS) cloud computing. The goal of a qualitative multiple case study was to explore and compare experiences of individuals with organizational resources to get a comprehensive understanding of the phenomena (Li, Wang, Liu, Xu, & Cui, 2018). A qualitative multiple case study was chosen because it generated rich data from the DBAs' experience and knowledge. The use of qualitative research techniques such as open-ended semi-structured interviews provided rich data from research participants and elicited further probing for more details by the researcher (Boz & Dagli, 2017). This qualitative method also provided a deeper insight into how DBAs developed strategies to secure data in private IaaS cloud computing. The qualitative research method also allowed the researcher to generalize the insights of the participants to a specified

population (Dey & Lehner, 2017). Stockman (2015) stated that the means of data collection in qualitative research was through interviews, focus groups, documentation, and observations. I used semi-structured interviews and organizational documents to collect data for my qualitative study.

Quantitative research was not appropriate for my research study because I was not collecting numerical data. Quantitative research was statistical because it used numbers to conclude a research study (Onen, 2016). Quantitative research was unsuitable for this study because it dealt with figures and was statistical. Quantitative research used independent and dependent variables to generalize relationships and verified research problem statements and questions (Hesse-biber, 2016). This study's data collection was based on the participant's responses to the interview questions and organizational documents that were not statistical. Qualitative research used verbal responses transcribed from the audio recorded interviews, written notes by the researcher, as well as nonverbal cues during the interview to explore phenomena. Therefore, a quantitative research method was inappropriate to provide an in-depth explanation of my problem statement since it does not test a hypothesis. I considered using mixed-methods for this study. Stockman (2015) defined a mixed-method as a research study consisting of both qualitative and quantitative research methods that could time-consuming. The mixed-method is inappropriate for this study because it is a combination of qualitative and quantitative methods and using both in my research study would be time-consuming. The researcher had to know multiple methods, and this allowed the researcher to use the strengths of both methods and minimize the weaknesses (Molina-Azorín & López-

Gamero, 2016). The researcher used mixed-method and quantitative results of the study to support the qualitative findings (Demir, Mutlu, & Şişman, 2018). Since this study relied on an in-depth exploration of the problem statement, using quantitative data was not suitable and mixed-methods do not apply to this study.

Research Design

There are five types of qualitative designs, and four of these five types will be described in this research study: ethnographic design, phenomenology design, narrative design, and case-study design, and three out of the four designs were considered as alternative design approaches for my research study. The ethnographic design was based on the researcher's understanding of the social and cultural perspectives of the mall-scale of people (Rashid, Caine, & Goez, 2015). The ethnographic design was not suitable for my study because the focus of the research was to understand the social and cultural perspectives of the small-scale of people. This ethnographic design was time-consuming because the researcher had to spend a vast amount of time learning the small-scale people's language and unfamiliar culture (Rashid et al., 2015). My study did not require an in-depth understanding or knowledge of the culture or social habits of DBAs regarding how they developed security strategies used to secure data in private IaaS cloud computing. Reich (2015) stated that in the ethnography design approach, the researcher lived in the participant's social world. I was not living in the DBAs' environments to understand their social and cultural perspectives. My study was focused on exploring the security strategies DBAs used to secure data in private IaaS cloud computing. Ethnography involved living in the participant's natural environment and experiencing

their daily lives (Marion, Eddleston, Friar, & Deeds, 2015). Since living in the participant's environment involved long-term commitment and immersion in their culture, this design was not feasible for my research study because I explored the security strategies used to secure data in private Infrastructure as a Service (IaaS) cloud computing. The phenomenological design approach focused on the daily lived experiences of a specific group of people (Mohajan, 2018). The researcher through the interviews gained an understanding of the experiences and perceptions of the research participants (Pelin, & Soner, 2015). My study was not about the lived experiences of one or more DBAs; whereas, it was about how DBAs developed security strategies to secure data in private IaaS cloud computing. Hannaford (2017) asserted that the researcher in phenomenological design attempted to comprehend a specify population perception of phenomena through their lens. In my research study, I was not trying to understand the behavior of DBAs when data breaches occurred. Instead, my study was to explore the security strategies DBAs used to secure data in private IaaS cloud computing. The narrative design approach focused on the personal stories of individuals and a sequence of events (Mohajan, 2018). The use of this qualitative research design was time-consuming for the researcher, and it involved a limited number of participants (Mohajan, 2018). The narrative design also provided individual life stories that generated a rich content of narratives. (Happel-Parkins, A., & Azim, 2017). My study was based on semi-structured interviews of research participants not on storytelling. The narrative design was centered on storytelling through textual information or dialogs (Hege, Dietl, Kiesewetter, Schelling, & Kiesewetter, 2018). This research study was not suitable for

my study because I explored the security strategies DBAs used to secure data in private IaaS cloud computing. A multiple case-study design was the research design for this study. I independently interviewed 6-8 individuals from two IT organizations. Gentles, Charles, Ploeg, and McKibbon, (2015) stated that a case study consisted of independent individuals and other organizational documents. A case study was also exploratory and explanatory, and this helped the researcher to answer how and why questions (Fagerholm, Kuhrmann, & Münch, 2017). The phenomenon that was explored in this study was the strategies DBAs used to secure data in private IaaS cloud computing. Multiple case study helped improve the credibility of study findings (Fagerholm et al., 2017). A multiple case study allowed the collected data from research to compare and contrast the strategies DBAs used in the two IT organizations to secure data in private IaaS cloud computing.

Data saturation was pivotal in the qualitative research method. It ensured when the participant's responses become redundant, and no new information was valuable to the study or generated new themes or codes (Gentles et al., 2015; Kline, 2017). To get data saturation, I interviewed 6-8 participants for this study. I achieved data saturation by conducting semi-structured interviews with DBAs until was no new information using the eligibility criteria for the research and ensured comprehensive and quality data was collected based on the participant's responses. The research participants were asked identical interview questions in chronological order without skipping questions or going out of order. I l reviewed data from the personal diary and field notes to identify concerns raised during the interview.

Population and Sampling

My population for this study was IT Database Administrators (DBAs) from two companies in Baltimore, Maryland with experience and knowledge in security strategies used to secure data in private IaaS cloud computing. Since I am an IT Specialist for the federal government, I was aware of five IT organizations in the Baltimore area that work with cloud computing; I contacted these five organizations in the Baltimore area that worked with cloud computing. Hoyland, Hollund, and Olsen (2015) stated that to identify the selected population for a study, details must be provided by the researcher. So, based on the responses received, I selected two organizations that were used as my multiple case study organizations. Both cases are small businesses with a budget of less than $30 million a year. Case A delivers Healthcare IT, Cybersecurity, and Telecommunications solutions that improve the life and health of millions of Americans while defending our national interests on the battlefield. Case B vision is focused on igniting innovation, inspire transformation, and implemented digital solutions for a healthier nation. Contact was initiated with these organizations via email introducing myself, asking permission to consider participating in my research study and providing details about the study. The email also informed the participants that their participation in the study was confidential and the anonymity of their responses was ensured by using unique identifiers for each participant. The interview data was safeguarded, and the data collection process was created that posed the least disruption to their workplace. Additionally, having an alliance with a gatekeeper to an organization positively impacted the perception of the research study (Hoyland et al., 2015). Such an alliance was through owners of the organizations

that I had worked with while as a contractor or they had working relationships with my federal employer as a contractor.

Having well-defined eligibility criteria in place was required for a qualitative study because it identified the research participants for the study (Hanson et al., 2016). The DBAs that were selected for this study met the eligibility criteria set by the researcher. The eligibility criteria that was used to identify potential research participants were (1) the DBAs will be 28 years or older, (2) IT work experience of five years or more, and (3) three years of cloud computing experience as related to data security. The qualitative sampling was difficult to attain, and the key focus should be in-depth perception and richer data with a small sample size (Roy, Zvonkovic, Goldberg, Sharp, & LaRossa, 2015). A small sample size of DBAs shared their experience with security strategies used to safeguard data in private IaaS cloud computing by answering the semi-structured interview questions. The qualitative research utilized a small sample size, and it was not representative of the general population (Twining, Heller, Nussbaum, & Tsai, 2017). DBAs working in IT and cloud computing were anticipated to be knowledgeable about cloud computing an evolving technology, and about 10-12 DBAs were selected from multiple organizations.

Purposive sampling was used to select the research participants. Purposive sampling was a popular strategy used in qualitative research to select a specific group of people based on their knowledge or experience about a specific topic (Palinkas et al., 2015). Using purposive sampling provided convenience and focus on the features of organizations that had implemented cloud computing data security strategies to prevent

data breaches in private IaaS cloud computing. Etikan (2016) purported that purposive sampling was a type of non-random sampling technique used to select a sample of participants from a specified population. My research participants for this study were DBAs with IT and cloud computing experience in implementing security strategies used to prevent data breaches in private IaaS cloud computing. Etikan (2016) purported that the central focus of purposive sampling was data saturation. I selected research participants that had knowledge and experience about cloud computing security strategies which provided rich, unique and valuable data for my study. Fusch and Ness (2015) believed consideration should be made toward using a sample size that provided thick rich data. I used a total of 6-8 research participants in my study from two IT organizations in the Baltimore area.

Census sampling, a form of purposive sampling, was suitable for this study. The goal of census sampling was to ensure that the researcher focused on data saturation by having an in-depth understanding of the sample until no new information or data was discovered (Etikan, 2016). Even though the number of research participants was reasonably small, census sampling encompasses all DBAs identified by the gatekeeper, and they were included in the study. Lucas (2014) added that census sampling occurred when the researcher incorporated in the research the whole population that fits the predefined eligibility criteria. The DBAs who met the research eligibility criteria for this study had knowledge and experience in IT, as well as database securities strategies in cloud computing. I chose to use census sampling because the 6-8 DBAs were a representation of the entire population of DBAs from the chosen organizations. Based on

the eligibility criteria, data collection and analysis were from 6-8 participants from both IT organizations. Random sampling was considered as statistical inference (Griffiths, Daniels, Austerweil, & Tenenbaum, 2018). Random sampling was not considered for this study because it was not suitable for a qualitative case study. The selection of sampling techniques implemented strategies that ensured quality, credibility, and validity (Roy et al., 2015). The implementation of sampling technique strategies was done through member checking of interview responses by participants and data triangulation.

As the researcher, my goal was to maintain an amicable working relationship with the research participants. Kallio et al. (2016) emphasized that the use of semi-structured interviews in a qualitative study was successful because it allowed exchange between the interviewer and participant. The semi-structured interview was used for each of my participants using an interview protocol to ensure that each participant was asked the same question in chronologic order. It was also pivotal that the location of the interview was based on the participant's preference (Foley, Boyle, Jennings, & Smithson, 2017). I worked with the participants to ensure the appropriate interview location of their choice with the least distraction while conducting the interview.

Moreover, interviewing participants in a setting of their choice made the participants comfortable to freely share their insights and this enhanced privacy, and created a positive rapport with the researcher. Ecker (2017) supported the notion that an interview setting was powerful because it provided the chance for a comprehensive understanding of research topics. I ensured that the informed consent provided details about the research purpose and maintained the confidentiality of the participants. Once

informed consent was given and understood, each participant signed the consent. The research participant was informed about how long the interview would last, and the interview was audio-recorded, and notes were taken. The participant was informed that a transcript of the audiotape and sharing of the interview notes would be provided to him or her for review and any corrections needed to ensure that the researcher captured the correct responses were encouraged.

Ethical Research

My recruitment of research participants' was done when my Institutional Review Board (IRB) approval of my doctoral study was received from Walden University ensuring that it met the human rights protection from harm. Barnard (2016) stated that the research should garner approval from the ethics committee subject matter experts that would agree if the research study was harmful and justified. I completed the IRB application for Walden University to ensure that the IRB members agreed if the research study conducted was safe and justified. The Belmont Report (1979) served as an ethical guide to safeguard research participants' rights involved in a research study. I adhered to the Belmont Report's three ethical principles of respect for individuals, beneficence, and justice during the semi-structured interview process for each research participant (The Belmont Report, 1979).

As the central instrument for data collection, I explained my role as the researcher to the participants. Finding and securing participants for a research study was a pivotal requirement before a research study can be conducted (Peticca-Harris et al., 2016). I obtained informed consent from each participant. The informed consent provided the

purpose and description of the research study, the expected duration of the interview, voluntary participation, and the option of not to participate, and a guarantee from the researcher to adhere to ethical conduct.

Careful consideration of maintaining ethical standards must be in place when selecting research participants for a research study (Lloyd, & Hopkins, 2015). Participants were able to choose not to participate at any time, and they were assured that if they decided not to participate in the research study while data collection was in the process, the data would be deleted, and the participant would be informed of the action. According to Auger (2016), informed consent must be obtained from all participants who consented to participate in the research study without duress voluntarily. The informed consent allowed participants the right to withdraw or stop the audio recording during any portion of the interview if they do not feel comfortable without retaliation. I got signed consent from all participants who voluntarily agreed to participate in the research study, and once they agreed to participate voluntarily, a copy of the signed consent form was given to each participant for their records. Finally, I let the participants know that I completed a National Institutes of Health (NIH) online training course to build trust and ensure that ethical principles were adhered to during the research study.

The consent form provided an option for all participants to opt-out of the study. My contact information including e-mail and telephone number was provided to the participants in case they decided to withdraw from the research study whenever they want to. Artal and Rubenfeld (2017) stated that full disclosure, informed consent, and voluntary participation was pivotal in a research study. The participants were informed of

any benefits and harm that the research study would pose and their participation in the study was voluntary. The participant letter of invitation is in Appendix B. The business letter of invitation (see Appendix C) was signed by the head of the organization. Barnard (2016) emphasized the importance of informed consent, which addressed the confidentiality of the research participants, data storage, and security of responses of participants. Collected data would be kept in a safety deposit box for five years to safeguard the participant's confidentiality. Ibrahim and Edgley (2015) assured confidentiality and anonymity while conducting a research study. Confidentiality of the participants was protected by assigning each organization and the participants a unique identification number, and all the data stored were password protected.

There was no incentive for this study. I let the participants know that they all had a common interest in safeguarding data stored in cloud computing and minimizing data breaches of customers' personally identifiable information. Moore et al. (2016) supported the use of motivational strategies as an incentive for research participants to voluntarily participate in a research study. Successfully identifying these strategies to secure data in the cloud was of value to their organizations and may serve as benchmarks. Additionally, the participants would be recipients of the final research study. Sharing their knowledge with other subject matter experts in a research study would provide positive responses and enhance rich data collection since they all share a common interest. The final doctoral manuscript would include the Walden IRB approval number (07-03-19-0513628).

Data Collection

Data Collection Instruments

In this qualitative study, I was the central instrument for data collection, and this was done using semi-structured interviews and reviewing organizational documents. Foley et al. (2017) stated that triangulation improved the credibility and validity of research findings. The use of multiple sources such as semi-structured interviews and organization documents improved triangulation (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). I ensured triangulation by comparing the responses from the participants with the organizational documents such as policies and regulations focused on database security strategies to prevent data breaches. Fusch and Ness (2015) stated that interviews were a means of reaching data saturation and data triangulation was a means of achieving data saturation. Data saturation was achieved when no new data, no new themes, or no new codes were identified when comparing interview responses with the organizational data.

Semi-structured interviews consisted of open-ended questions to generate comprehensive data from the participants (Molina-Azorín & López-Gamero, 2016). I asked open-ended questions to allow the participants to provide detailed information about the phenomena being studied; responses were audio-recorded, analyzed, and transcribed. According to Jamshed (2014), the duration of semi-structured should last between 30 minutes to an hour. I ensured that the interview lasted no longer than one hour. If the one-hour time frame was close, I asked the participants' permission and preference if he or she would like to end the interview within the one-hour timeframe or

schedule another follow-up question interview at a later time. Jamshed (2014) stated that the semi-structured interview consisted of open-ended preset interview questions that elicited a response from the participants. All interviews were audio-recorded with the permission of the participants.

The interview protocol (see Appendix D) included the interview questions I asked the participants during the semi-structured interview. The interview protocols were used to enable researchers to ask participants the same questions in similar chronologic order, to allow comparison of responses with all participants to address validity, internal consistency, and quantify the responses (McIntosh & Morse, 2015). I asked each participant the same interview questions in chronological order using the interview protocol (see Appendix D). Methodically asking interview questions allowed easy comparison of participants' responses, and this enhanced the identification of themes and codes (Young et al., 2018). Member checking assessed the validity of the responses from the research participants (Burda, Van den Akker, Van der Horst, Lemmens, & Knottnerus, 2016). Member checking was achieved by sharing the transcript of the participant's responses with them to validate if the responses were accurate or required additional information either by sending participants the transcript via e-mail or scheduling a second meeting to review the researcher's interpretation of the data.

The member checking process was iterative until the participant's responses were captured correctly. Spillane, Larkin, Corcoran, Matvienko-Sikar, and Arensman (2017) stated that using a reflective journal communicated observed behavior and concerns raised during the interview. I kept a personal diary that contained some real issues raised

amid the interview, as well as any observed behavior from the participants. Reflexivity served as an iterative process of self-assessment by the researcher to consider the impact of their role in a qualitative research study, which included the setting, participants, data collected, analyzed, and interpreted (Orange, 2016). The use of a personal diary served as a data collection instrument, and it tracked my actions, decisions, and ethical standards. Berger (2015) posited that reflexivity was important throughout the entire research study. As the researcher, I adhered to the interview protocol and was self-reflective while interviewing the participants by asking open-ended questions and was aware of my own biases such as thoughts, reactions, and triggers. Moreover, reflexivity helped minimize biases by monitoring the researcher's actions, doubts, and insights documented in the personal diary.

Data Collection Technique

My qualitative case study data collection technique was focused on using multiple data sources such as semi-structured interviews, organizational documents, and observation. The interview was the most common data collection technique for the qualitative study (Jamshed, 2014). The semi-structured interview was collected through audio recordings and transcribed for each participant. The interview protocol (see Appendix D) consisted of open-ended questions that generated rich and thick data from the participants. I used document analysis for a review of organizational documents related to security strategies to prevent data breaches in private IaaS cloud computing, field notes, and a personal diary (reflective journal). Before starting the data collection for my study, IRB approval was required from Walden University. Obtaining access to

potential participants was a challenging task (Peticca-Harris et al., 2016). Once IRB approval was received, I recruited participants by sending out an e-mail to the IT organizations that had agreed to participate and used cloud computing for data storage. Once my participants agreed to participate in the research study, I introduced myself first and described the purpose of the research study. The point of contact for each organization that provided access to the participants was the key to minimizing challenges related to access to these participants.

Face-to-face semi-structured interviews were used for data collection for two IT organizations' from the DBAs with both IT and cloud computing experiences. I also used organizational documents focused on security strategies used to prevent data breaches in cloud computing to understand the phenomena better. Carter et al. (2014) stated that the use of multiple resources in a qualitative case study provided in-depth and thick data to understand the phenomena better. I got access to these organizational documents by working with the senior management team focused on security strategies DBAs used to prevent database breaches in private IaaS cloud computing. Before the interview, I introduced myself to each participant and obtained informed consent. The informed consent form contained a description of the study and its purpose . I audio recorded the interview of each participant and analyzed each organizational document. Kim and Miller (2015) defined informed consent as an agreement between the researcher and participant that described the purpose of the research study, risks and benefits, alternatives, and voluntary participation with the option to withdraw from the research study at any time they chose to. Once the informed consent form was explained to the participant, they

signed if they agreed to participate and a copy of the signed informed consent was given to the participant for their record.

To adhere to the ethical research standards, data collection from participants during the research study must be held confidentially. Semi-structured interviews were beneficial because they generated rich, comprehensive data about the research topic. Oates (2015) stated that face-to-face semi-structured interviews built rapport between the research and participant and provided quality data. As the researcher, I ensured that the participants selected the setting of preference for the interview, which allowed time to promote rapport and trust. The quality of data during the interview was pivotal to a research study. I also used the interview protocol to maintain the methodical structure of the interview. This protocol had the list of open-ended questions that were asked of each participant in chronological order (see Appendix D). Oates (2015) validated that for an interview to be of rich quality and comprehensive, irrelevant questioning, inappropriate timing, poor interviewing technique, problematic behavior can hinder an interview. I ensured the interview was conducted in a comfortable setting of the participant's choice with minimal distraction and the participant's time preference for the interview. I observed participants for nonverbal cues and ensured all audio recording devices were tested and in working order before the interview.

Data Organization Technique

During the data collection phase, I collected a variety of data such as organizational documents, interview recordings, and field notes. Ranney et al. (2015) stated that organizing qualitative data are a pivotal step required to ensure validity and

reliability, in a qualitative research study. I used a reflective journal and a qualitative software package such as to Atlas ti8 to create an audit trail of decisions that improved quality and validity when I analyzing and transcribing e interviews (see Vicary, Young, & Hicks, 2017).

I used a personal journal or reflective journal to track my thoughts, concerns, questions about each phase of the proposal process and review. The organization of data collected was pivotal in a research study. Orange (2016) posited that the use of a reflective journal in a qualitative study helped organize the researcher's thoughts and concepts during the data collection process. For my qualitative study, I used two types of data collection techniques: semi-structured interviews and reviewed organizational documents. From the Chief Security Officer, I obtained organizational documents related to data security of personally identifiable information of customers.

All data collected about this research study was stored on an encrypted flash drive for five years and would be disposed of after the five years. The flash drive was locked in a safety deposit box. Data collected from the interviews were compared with each participant's responses to ensure validity and credibility. Member checking as described by Burda et al. (2016) was a feedback measure from the research participants who reviewed the transcribed data and interpretation of the findings by the researcher and provided feedback and additional information to ensure the content of the data was correct. I validated the data collection findings and interpretation by sharing my transcript of the findings with the research participants. Member checking promoted data saturation. I also used my diary (reflective journal) to compare issues raised during the

interview with the participant's responses to identify themes and codes and summaries from the journal, and my field notes were shared with the participants for their review to get their feedback on modifying or adding additional information. Member checking was utilized as a means of research participants validating the accuracy of the data collected by the researcher, which enhanced the credibility of the data and the research findings (Goodell, Stage, & Cooke, 2016). I established member checking post-interview with the participants either by e-mail, telephone, or face-to-face. The interview transcript, the summaries from my field notes and reflective journal, as well as summaries from organizational documents, were made available for participants' review and feedback. I safeguarded the interview data and all other pertinent data collected from other sources in a safety deposit box and would be maintained for 5 years. After the 5 years', all the raw data will be destroyed, shredded or erased.

Data Analysis

Researchers contended that the most tedious advance in a qualitative research study happened during data analysis because the amount of data and the in-depth analysis generated from the qualitative data collection techniques for the researcher to better understand the phenomenon (Watkins, 2017). Data collected in this qualitative study was done in textual form after analyzing and reviewing organizational documents and interview recordings. I obtained organizational documents related to data security from the Chief Security Officer. Hussein (2015) opined that textual data was raw and must be converted into information that could be analyzed to show patterns that are decoded and translated into themes. Data analysis was done through the review of semi-structured

interviews and a review of organizational documents to identify themes and codes. Themes were usually created through the researcher's insights into the data collected from the interview and multiple resources (Goodell et al., 2016). These themes and codes were linked to security strategies used to prevent data breaches that will answer my research question. Themes and codes were identified by using triangulation, which was a data analysis technique. Stewart and Gapp (2017) purported that a researcher's goal was to deliver trustworthy information that was valid and credible about their research findings. My goal was to analyze and transcribe all audio-recorded interviews, field notes, and reflective journal resources verbatim and ensured the accuracy of the information through member checking and triangulation.

Data triangulation was a means of thoroughly analyzing qualitative data to ensure reliability. Goodell et al. (2016) stated that data triangulation was a rigorous analysis of qualitative data that allowed the researcher to use checks and balances in reviewing and analyzing data to ensure the quality of the data and findings. Data triangulation produced a holistic picture of the research topic from comprehensive resources. There are four types of triangulation: data, method, investigator, and theory (Morse, 2015). Data triangulation used multiple data sources such as people or groups to generate a variety of insight into the data analyzed in time and space (Fusch & Ness, 2015). This study does not apply to my study because my research study would change over time due to the effective use of the security strategies used to prevent data breaches in private IaaS cloud computing. Investigator triangulation used multiple researchers to analyze a specific phenomenon and provided different insights into the data (Carter et al., 2014). This

triangulation strategy does not apply to my study because I was the sole researcher for this study and contrasting views from multiple researchers were not required. Theoretical triangulation utilized multiple theoretical perspectives to interpret data (Fusch & Ness, 2015). This study does not apply to my study because I was using one conceptual framework for my study. Methodological triangulation was the most common triangulation used by researchers that used multiple strategies such as interviews, organizational documents, field notes, personal diary or reflective journal to analyze a specific phenomenon (Annansingh & Howell, 2016). This triangulation strategy was applicable for my study because I audio recorded all participants' interviews, reviewed and analyzed organizational data on security strategies for preventing data breaches in cloud computing, as well as used reflective journal and field notes to analyze data for my research study.

I used methodological triangulation in my research study by audio recording interviews from the research participants and transcribed the interviews verbatim, as well as analyzed the organizational documents related to security strategies used to prevent data breaches in private IaaS cloud computing. Methodological triangulation was the use of two or more data sources that minimized biases and limitations resulting from using a single method (Joslin & Müller, 2016). I also used my field notes and reflective/personal diary to analyze data that may contain issues or concerns identified during the interviews. A qualitative analysis was done using a thematic analysis approach. Thematic analysis was a process used by the researcher while transcribing data to identify emerging patterns to clarify the research question (Mohajan, 2018). I reviewed and analyzed the data in-

depth to categorize data in groups to clarify the research question based on the themes and codes identified such as common patterns in sentences, commonly used phrases that developed into thematic categories of description. Categorizing of data in groups promoted data organization and vigorous coding. Arora and Dhiman (2015) emphasized that the coding of data using unique numeric codes protected the identity of the research participants. Once the interview data was transcribed from the audio recorded interviews, each participant's responses were assigned a unique identity to ensure their responses were confidential and anonymous. Thematic analysis was a strategy used by researchers to interpret qualitative data in a comprehensive and in-depth way by identifying themes and codes to answer the research question (Pfeiler, Buffington, Rao, & Sutters, 2017). I entered the transcribed interview into my selected software, which was Atlas ti8. The Qualitative Data Analysis used a holistic approach to interpret the subjective viewpoints and understanding of the research participants as related to a specified topic (Chowdhury, 2015). There were several Computer-Assisted QAD (CAQDA) in the market used by researchers to aid in the analysis process of qualitative data, and the researcher still had to solely manage the process (Zamawe, 2015). Examples of CAQDAs included Nvivo, Atlas ti8, N6, HyperResearch, Qualrus, and MAXqda. Rodik and Primorac (2015) stated that the most commonly used CAQDA software was Atlas ti8, NVivo, and MAXQDA. The decision to use the CAQDA was based on ease of access to it, recommendations from peers, and the quality is added to the researcher's analysis of data (Rodik & Primorac, 2015). Atlas ti8 promoted reliability, validity, and trustworthiness of data

analysis through triangulation, member checking, and audit trail (Ang, Embi, & Yunus, 2016). All of these capabilities promoted the reliability and validity of QDA.

Since categorizing the content of the semi-structured interviews was time-consuming, using Atlas ti8 QDA made this process much easier (Budzise-Weaver, Goodwin, & Maciel, 2015). I uploaded one transcribed document per participant into Atlas ti8 post data collection. This uploading of documents per each participant's response enhanced the comparison of data between the participants (Olson, McAllister, Grinnell, Walters, & Appunn, 2016). I was responsible for making decisions in selecting codes and phrases. I performed an in-depth and comprehensive analysis of the semi-structured audio-recorded interviews, organizational data, field notes, and reflective journal to identifying emerging themes such as common words, description, and experiences related to security strategies that linked to the central research question and the Christensen's DIT, which was the conceptual framework for this study. With the use of Atlas ti8, I was able to apply the codes to sentences and paragraphs (Olson et al., 2016). I used Atlas ti8 to analyze data by preparing and importing it, familiarized and coded data, created families and networks. Atlas ti8 aided in organizing theoretical and conceptual relationships (Paulus, Woods, Atkins, & Macklin, 2017). The use of the Atlas ti8 tool provided easy access to codes, themes, and relationship maps constructed through the analysis of the data collected (Paulus et al., 2017). I conducted a final analysis of the coding file.

Reliability and Validity

Reliability

The researcher's role in a research study was to ensure that the research findings were reliable and valid. The reliability of a study focused on consistency and results can be replicated and may vary in the richness of data within comparable measurements (Leung, 2015). I ensured that the semi-structured interviews were conducted using an interview guide (see Appendix D) in which I asked the participants the same questions in chronological order. Dikko (2016) confirmed that reliability could be achieved by asking the participants the same questions at varying times and obtain the same responses with different wordings. All semi-structured interviews were audio-recorded, and when transcribed, the transcript was stored on an encrypted file and stored in a safe accessible only by me.

Additionally, the reliability of my research study was dependent on how honest the participant's responses were and if they answered questions completely. To promote honest responses to research questions by participants, participants were informed that their identity was protected by alphanumerically coding their responses, which was confidential. Validity depended on the unbiased honesty and precision of the participants' responses to the interview questions (Marks, 2015). The guiding principle for meeting rigor in a qualitative research study was dependability, credibility, transferability, and confirmability (Grieb, Eder, Smith, & Calhoun, 2015). These four techniques measured reliability and validity.

Dependability

Dependability tested the trustworthiness and consistency of a research study. Dependability ensured that other researchers could use the same data to generate similar patterns (Hammarberg, Kirkman, & de Lacey, 2016). Dependability could also be achieved when a researcher used the same data and got the same outcome (Morse, 2015). As the researcher, I ensured dependability by using the same interview protocol (see Appendix D) to ask all the participants the same questions in the same chronological order. Connelly (2016) stated that an audit trail is one of the procedures used to ensure dependability. I used my reflective journal to document any concerns during the research study. Use of the journal also helped me to identify patterns and themes.

Noble and Smith (2015) purported that consistency and trustworthiness of a study was contingent on the researcher keeping a decision trail. I used my reflective journal to document any issues or decisions during the process which ensured clarity and transparency. Maintaining a decision trail also helped in ensuring trustworthiness by making the researcher's decision clear and transparent (Noble & Smith, 2015). The trustworthiness of a study was dependent on the participants providing truthful and complete answers to the interview questions (Morse, 2015). I did so by asking the same questions to the participants in chronological order. The participants were allowed to choose the preferred choice of where the interview was held. I explained to them why and how the research process would be done to enhance trustworthiness.

Additionally, I informed them that all responses would be confidential and stored on a memory stick that would be locked up in a location only accessible by me. The

consistency of the participant's responses was done through member checking (Burda et al., 2016). The member checking was done by having participants review the transcript responses to ensure that the data collected through the interview were correct and truthful.

Credibility

The credibility of a qualitative research study relied on the researcher defending the honesty of their work (Hammarberg et al., 2016). Hussein (2015) described data triangulation as a strategy that employed multiple sources to validate data in a research study. I compared the themes that were identified from interviewees and analyzed the organizational documents, as well as with the field notes and decision trail from my reflective journal. Using triangulation of multiple sources such as semi-structured interviews and comparing it with organizational documents, verified the research findings. I let the research participants reviewed and evaluated the interview transcript to ensure my interpretation was correct and they made the appropriate modifications before continuing with the analysis of the remaining transcript. The member checking had been referred to as one of the most accurate strategies to validity participants' responses to interview questions (Grieb et al., 2015). The member checking strategy ensured that responses were believable and truthful. The member checking and data triangulation worked simultaneously to ensure the credibility of research studies (Lub, 2015). The member checking strategy helped minimize personal biases and enhanced the credibility of the study. I also avoided personal biases by maintaining an audit trail using a reflective

journal to document issues or decisions about the research study. Maintaining an audit trail using a reflective journal improved the rigor of the study.

Transferability

Transferability was a form of external validity, which generalized the research findings of a study to a different setting or group (Cope, 2014; Henry & Foss, 2015). I accomplished transferability through data collection, in-depth analysis of rich and comprehensive data from participants during interviews, and organizational documents. Leung (2015) advocated that comparable criteria used to assess the rigor of a study ought to likewise apply to generalizability. I accomplished this by using the same interview questions in the same chronological order for each research participant. Member checking was done by sharing the transcript of the data findings from the interviews with each participant to determine if they felt the transcript represented their views and experiences. Member checking also enhanced data saturation. Data saturation was achieved when no new data, themes, or codes were identified during member checking (Fusch & Ness, 2015). The transferability of this study was done by generating rich, in-depth, and comprehensive data from the research study that was applied to a comparable setting or group.

Confirmability

Confirmability enhanced the objectivity of the research study by using an audit trail to maintain transparency and validity of the study (Morse, 2015). I kept track of all my observations, concerns, and decisions during the research study in my reflective journal to establish transparency. Audit trails served as a blueprint for the research study,

which outlined the process used by the researcher (Auger, 2016). Therefore, the use of this blueprint made the study replicable in a different setting and population. This audit trail also represented the participant's responses and not the researcher's biases or viewpoints (Cope, 2014). Ang et al. (2016) described the audit trail as the key technique for determining confirmability. The researcher's notes in the reflective journal kept track of the steps conducted during the research study and established objectivity (Connelly, 2016). Additionally, the notes in my reflective journal would be used by future researchers to gain insight into how and why decisions were made during this research study.

Transition and Summary

In Section 2, I restated the purpose statement. I also described in detail the role of the researcher participants, target population, ethical research, data collection instruments and techniques, data organization techniques and analysis, as well as data reliability and validity. This qualitative study employed the use of a case study to explore the security strategies DBAs used to prevent data breaches in private IaaS cloud computing. Data collection was accomplished from the face-to-face semi-structured interviews and analysis of organizational documents to identify security strategies that were successful in preventing data breaches in cloud computing.

Section 3 will use the techniques used from this chapter to present the findings from the data collected and interpreted, application of the findings to the IT professional practice, implications of the findings for social change, the recommendation for actions and further research, my reflection of the study, and a strong concluding statement.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative multiple case study was to identify strategies DBAs use to secure data in private IaaS cloud computing. I collected the data for this study from semistructured interviews I conducted with DBAs in two IT organizations in Baltimore, Maryland. I also reviewed organizational documents provided by the DBAs, my field notes, and a reflective journal I kept. The DBAs all had experience in securing data in private cloud computing, as well as mitigating data breaches in the cloud. Section 3 includes the presentation of findings, applications to professional practice, implications for social change, recommendations for action, recommendations for further research, reflections, and the conclusion of the study.

Four major themes emerged from this study: (a) the importance of well-defined security measures in cloud computing, (b) measures to address security issues in cloud computing, (c) the limitations of existing security controls in cloud computing, and (d) future and potential security solutions for DBAs working in cloud computing. These four major themes are consistent with the trends revealed in the literature review (e.g., Cusack & Ghazizadeh, 2016; Flores et al., 2014; Schniederjans & Hales, 2016; Sindhu & Mushtaque, 2014; Sookhak et al., 2018), and the results from the study support my use of the DIT (Christensen, 2006; Goldstein, 2015) as the conceptual framework. The four major themes are described and explored in the next section.

Presentation of the Findings

The central research question for this study was, what were strategies database administrators used to secure data in private Infrastructure as a Service (IaaS) cloud computing? The four major themes illustrate potential strategies DBAs used to secure data in private IaaS cloud computing. Tables 2-5 include the frequency of responses tagged for the subthemes of each theme. Each table consists of columns indicating the frequency of participants who made significant contributions to the theme and the organizational documents that corroborated the data gathered from the semistructured interviews.

The participants in the study were DBAs with supervisory responsibilities and who had vast experience in cloud computing security strategies. A DBA's role includes storing and organizing data and maintaining a successful database environment by ensuring data are secure from unauthorized access (see Cusack & Ghazizadeh, 2016) Eight DBAs agreed to participate in this study, four from each case. However, only six DBAs consented to be interviewed, three from each case. The seventh and eighth participants consented to participate but were unavailable for the interview. Two of the participants had 20 years' and 23 years' experience, respectively, in IT security and over 10 years each of cloud computing experience. The other four participants had between 8 and 11 years' experience in IT security and over 5 years' experience in cloud computing. The participants were all men, and no bias was identified as the research interview questions were non-gender-sensitive.

I achieved data saturation after interviewing Participant 5 as no new themes or codes were identified or emerged when Participant 6 was interviewed. I used methodological triangulation to analyze the two major sources of data, which were the semistructured interviews and seven organizational documents (HIPAA Security Rules; United States [US] Digital Guideline NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations; Information Security Policies: Data Breaches Response Policy; Information Security Policies: Third-Party Security Management; Information Security Policies: Security Incident Management Policy; Information Security Policies: Access Control Policy; and Business Associate Agreement). Six of the seven documents were focused on security policies such as data breach response policy, security incident management policy, third-party security management policy, and access control policy. Additionally, all the participants referred me to the online Health Insurance Portability and Accountability Act (HIPAA) Security Rules and the United States (US) Digital Identity Guideline NIST 800-63B security policies and procedures because of proprietary information policies.

I also used other materials such as my field notes and reflective journal that comprised of critical issues raised during the interviews. The field notes and reflective journals were beneficial in the data triangulation process. The reason for triangulation was to provide a confluence of evidence to breed credibility (see Lub, 2015). Validating my findings over the informational index diminished the effect of potential bias because I gathered data through semistructured interviews and organizational documents. Additionally, after each interview, member checking of interviews was done by

presenting summaries of the initial interviews to each DBA and IT security professional for review and confirmation of accuracy. Member checking was done 1 or 2 days postinterview by telephone or e-mail. I read the participant's responses to each participant to ensure validity, accuracy, and credibility. The use of member checking allowed each participant to modify or make changes if I captured or interpreted the interview transcript incorrectly, as well as secure data saturation. The use of member checking and other validation techniques yielded knowledge that DBAs can use to develop successful security strategies to prevent data breaches in IaaS cloud computing and build trust in consumers and improve system performance.

Theme 1: Importance of Well-Defined Security Measures in Cloud Computing

The importance of well-defined security measures in private IaaS cloud computing emerged as the first theme from the data analysis of this study and was addressed by all the participants. The findings support how well-defined security measures, when used in cloud computing, are associated with the protection of the database. This first theme contained several subthemes mentioned by the participants and in the organizational documents. The four pivotal subthemes were as follows:

- authentication;
- encryption;
- authorization; and
- data integrity and confidentiality.

Based on participant data, these four subthemes are required for DBAs to secure data in cloud computing. Table 2 shows four pivotal subthemes for Theme 1 and includes the

frequency (number) of participants who implemented these strategies to secure data in private IaaS cloud computing. Table 2 also shows the number of supporting documents associated with each subtheme.

Table 2

Frequency of First Major Theme

Source of data collection	Authentication	Authorization	Encryption (*f*)	Data integrity and confidentiality (*f*)
Participants	5	3	5	2
Documents	7	5	7	3

Note. f = frequency.

Authentication. The participants spoke about how critical authentication was in securing data in private IaaS cloud computing. The responses from all the participants showed that they implemented authentication strategies as the first step to ensure securing data in private IaaS cloud computing. The responses from all five participants indicated that authentication, when used as a security strategy by DBAs, ensured the security of data and improved data quality. These views of the participants were consistent with the findings of Sudha (2015). Sudha's (2015) findings supported the participants' responses by ensuring that users' information is shielded from unapproved access by other users' and are given access rights to data they own. Participants 1, 2, 4, and 5 noted that they used multifactor authentication to grant users access to data stored in private IaaS cloud computing. Participant 2 indicated that authentication of users was verified through identity management systems, which is supported by Han, Yang, Wang, Mu, and Liu

(2018), who found that multifactor authentication wins the support of customers for its high-security benefits by improving the security of the user's data. Moreover, the use of multifactor authentication is more reliable than using most complex passwords, and this makes it critical to prevent database breaches. Simon (2019) added that two-factor authentication serves as an added line of protection, is a better way to protect data than the use of a stringent password, and is critical to blocking hacks and assaults to customer' personal information. In comparing the two cases used, two out of the three participants from each organization agreed that multifactor authentication is the first step to prevent unauthorized access to data stored in the cloud, which would prevent data breaches in cloud computing.

In reviewing the seven documents provided by the IT organizations (HIPAA Security Rules, United States (US) Digital Guideline NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Information Security Policies: Data Breaches Response Policy, Information Security Policies: Third-Party Security Management, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy, Business Associate Agreement), I used content analysis by audio recording all the semistructured interviews. I also transcribed each interview, recorded my observations and any issues in my field notes and reflective journal. I found examples of the use of multifactor authentication policies and procedures to address specific types of security incidents that may involve the accidental disclosure of PII to unauthorized third-parties. The seven documents were security documents that provided guidelines on how to address data

breaches, manage third-party security of data, password guidelines, and security policies, how to report and manage incident occurrences in the organizations, and how to provide access to users of the database. The seven documents also defined the requirements for reporting and responding to incidents related to the handling of sensitive information. In their experiences, the six participants indicated that they followed these policies to secure data in private IaaS cloud computing. The organizational documents provided by the participants also demonstrated their knowledge and understanding of the requirements to ensure securing data of customers in private IaaS cloud computing. Participants 1, 2, 3, and 4 emphasized that DBAs had to comply with HIPAA mandates or standards to secure PII in private IaaS cloud computing. These findings also supported the first theme of this study.

The findings of this study support previous research. Wang et al. (2018) emphasized that authentication of users served as the first line of defense to secure data in the cloud and prevent data compromise. Zhou et al. 2017 acknowledged the importance of authentication in cloud computing protects PII. They argued that the authentication protocol served as the cornerstone of security protocol and has been widely used in electronic banking, online shopping, video conference, and electronic voting. Therefore, Zhou et al. (2017) argument supported the findings of this study. In their experience, Participants 1, 2, 3, 4, and 5, verified the importance of using multifactor authentication to identify users accessing data in private IaaS cloud computing.

Current security regulations such as HIPAA encouraged the use of basic security controls such as multifactor authentication to secure data in cloud computing (Gantt,

2014). Participant 1indicated that the use of multifactor authentication is used by complying with HIPAA PII standards and mandates. Participant 2 further explained that he used the Identity Authentication Management (IAM) tool to allow users to access data in private IaaS cloud computing. Participant 3 indicated, “we have the legal rights to make sure the database is accessed using multifactor authentication”. Ramachandran and Chang (2016) confirmed that IAM is a security tool used in managing users’ passwords and permission for access to certain services in the cloud. Participant 4 explained the strategies of multifactor authentication by adhering to HIPAA mandates and standards. Participant 5 indicated that multifactor authentication is done thorough multiple systems that validate the user’s identity before accessing the data in private IaaS cloud computing. Simon (2019) viewed multifactor authentication as challenging to manage due to security concerns related to using unscripted SMS text messages on a cell phone. Heatherly (2016) emphasized the significance of multifactor authentication as well-defined security measures that secure the privacy and data integrity of customers’ data. He explained that this authentication mechanism is achieved successfully by using something they know (password) and something they possess (personal identification verification card or a fob) (Heatherly, 2016). This authentication mechanism also supported the findings of Theme 1. All five participants considered using multifactor authentication that validates all users’ access to the database as one of the major features of the importance of well-defined security measures in cloud computing.

The conceptual framework of this research project was the DIT. These findings emphasized the importance of well-defined security measures in cloud computing and

supported the DIT framework. The findings are consistent with how low-end disruptive technology such as cloud computing has forced organizations to change their business logic. This change in business logic is done by organizations remaining competitive by improving products and system performance in the continuously evolving technological age by exploiting the disruption. Goldstein (2015) supported the improving products and stated that disruptive innovation is an ordinarily substandard development that in the long run improves and swarms better products because it is less expensive, progressively advantageous, and for some customers, adequate. The experience of all the participants provided an understanding of using well-defined security measures like authentication in cloud computing to secure data in cloud computing and ensure that the security risks of data breaches are minimized. The DBAs have embraced DIT and in turn, implemented well-defined security measures to safeguard data in cloud computing and improve the efficiency and performance of their databases. The findings of the importance of well-defined security measures support DIT. These findings have made managers and DBAs embrace DIT as an opportunity and position the potentials of the organization toward change (Kranz et al., 2016; Osiyevskyy & Dewald, 2015). Furthermore, to establish a secure database, DBAs emphasized that authentication improves the productivity of data security in cloud computing (Li & Wang, 2019). Once DBAs understand that authentication can prevent data breaches, they can support and assist IT organizations with securing data in IaaS cloud computing.

Authorization. Heatherly (2016) defined authorization as the permission rights provided to users to access databases. He emphasized the importance of the varying

authorization levels to secure data (Heatherly, 2016). Participants 1 and 2 responses supported Heatherly's view. Participants 1 and 2 explained the importance of authorization as a well-defined security measure in cloud computing. The responses from the two participants and analysis of the five organizational documents (Information Security Policies: Data Breaches Response Policy, Information Security Policies: Third-Party Security Management, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy, Business Associate Agreement) signified that authorization minimized human threats. Cusack and Ghazizadeh (2016) indicated that authorization is based on users' access control. Participant 1 opined that authorization is a layered approach to security focused on roles and permission. Participant 2 also reiterated that authorization provides permission of roles to control internal threats. Participant 5 also emphasized that authorization is based on read and write access permission roles. The responses from participants indicated that a robust authorization mechanism secures data in cloud computing. This finding was consistent with the literature by Foresti et al. (2018). Foresti et al. (2018) indicated that authorization is permitted through regulatory access rights, which allows users to access varying portions of the data, as well as maintaining privacy and confidentiality. For example, participant 1 indicated that "if Person A wants to access the data from my database, I would give it a token that grants its access to do a specific function, and if they need more than one type of access, I will give it different tokens based upon that permission level". Participant 2 indicated that "user authorization may be secured by IAM tool Cyberport. Every time a user logs into the database, IAM manages the

authentication and authorization rules". Participant 3 said that they provided read and write access to users only to specified programs. Though the responses from the participants in both cases varied, it still supported the findings of the study that authorization is a pivotal strategy required to secure data in IaaS cloud computing. The DBAs in their responses from both cases valued the use of authorization to secure data in cloud computing.

These findings support the DIT framework for this study in that DBAs should develop robust identity management infrastructure to ensure that the permission rights are granted or removed based on the user's roles and relationship to the organization (Jathanna & Jagli, 2015). This theme is consistent with the DIT and supports the findings, the purpose of this study, and answers the research question. The participants voiced that authorization is a security strategy that works best to prevent data breaches in cloud computing infrastructure by safeguarding customer data. Organizational documents had policies and procedures focused on permission rights for enforcing authorization on data to minimize data breaches in cloud computing (Foresti et al., 2018). Previous research supports these findings of access rights such as deletion, provisioning, and disabling of accounts based on the organization's approval process.

Encryption. The third subtheme was encryption. Encryption is a security strategy used to scramble or decode data utilizing access approaches characterized by traits (Ramu, 2018). When asked what the DBAs experience in database security in cloud computing was, Participants 1, 3, 4, 5, and 6 acknowledged that encryption was an important strategy used to prevent unauthorized access to data in cloud computing. The

approach of using encryption varied among the participants. Participant 1 indicated that "encryption was a one-way hash or can be used as a reversible hash depending on the project severity". He also added that "encryption was used for data at rest or in transport when it left the protected zone". Participant 3 indicated that encryption is one of the multiple levels of protection against data breaches. Participant 3 indicated that using encryption is pivotal in securing data, however, concerns about how complex encryption may limit securing data. This ties my findings with similar findings by Hadavi, Jalili, Damiani, and Cimato (2015) where they found that complex encryption can be challenging when storing data in the cloud while maintaining privacy. Moreover, encryption safeguards data integrity, but its intricacy has seriously restricted its reasonable use (Hadavi et al., 2015). Participant 4 further described the encryption of data as a complex process to scramble data while using an encryption key. Participant 5 purported that encryption of data is one of the first steps used by DBAs to secure PII and minimize data breaches. Previous research by Jho, Chang, Hong, and Seo (2016) confirmed the findings for the first theme. Jho et al. (2016) indicated that another strategy of maintaining data security and privacy is by using encryption. These findings of well-developed encryption warrant the confidentiality of the data, which was consistent with the responses from participants 1, 3, 4, and 5 of the study. Two out of the three participants in case one and all three participants in case two emphasized that encryption is an important security strategy to prevent data breaches in cloud computing. However, Participant 3 added that encryption uses multiple levels of protection and expressed

concern about complex encryption. One of the participants from the two cases reported that encryption is the first step to secure PII and minimize data breaches.

I reviewed and analyzed the organizational documents (Information Security Policies: Data Breaches Response Policy, Information Security Policies: Third-Party Security Management, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy, Business Associate Agreement) to ensure it supported the participants' responses of using encryption. All participants verified that DBAs followed a solid policy and procedure to encrypt data in transport and at rest to secure data in private IaaS cloud computing. These findings also reinforced the first theme of this study. The participants corroborated that their policies and procedures for encryption were guided by the NIST Cryptographic Algorithm and Module Validation Programs. These findings were supported by Lankford (2019), who indicated that Federal Information Processing Standards (FIPS) 140-2 is the means to certify an encryption algorithm. Tankard (2017) confirmed the findings in the organizational documents that all PII in the IaaS cloud computing should be encrypted to prevent data breaches. As a DIT, cloud computing technology as a new product has improved system performance making it appealing to large organizations that initially viewed it as a mediocre product (Crockett et al., 2013). Therefore, encryption is a pivotal security strategy used by DBAs to secure data in private IaaS cloud computing and this minimizes data breaches.

As related to the DIT framework, the findings of this study suggested that cloud computing as a DIT changed the business process of the entire organization making data

secure and more accessible to organizations anywhere anytime, which supports the findings of Goldstein (2015). Christensen (1997) opined that the disruptive innovation theory supports innovations spawns' evolution, and this enhances performance in the current IT environment. With well-defined security strategies like encryption, DBAs will secure data in cloud computing and this will the improve performance of their system. The first theme supports one of King and Baatartogtokh's (2015) summarized four key elements that the DIT is based on the notion "that incumbents in a market are improving along a path of sustaining innovation". These findings are tied with the use of encryption as a strategy to sustain innovation by securing data in the cloud, which minimizes data breaches.

Data integrity and privacy. The fourth subtheme identified is data integrity and privacy/confidentiality. Data integrity and privacy align with DIT because cloud computing storage disrupts the way organizations now store data. However, storing data have made organizations give up data management to third-party CSPs and this may compromise data integrity and privacy with the use of multiple cloud tenants. Multitenancy is now a problem in cloud computing because to save costs, organizations share memory, database, and resources in the same area and this creates a potential of data integrity and privacy being compromised (Jathanna & Jagli, 2015). With the emergence of IT and cloud computing, data integrity and privacy of customers sensitive or PII information is now pivotal (Dhasarathan, Thirumal, & Ponnurangam, 2015). Two of the six participants emphasized the importance of data integrity and privacy of PII. Participant 1 indicated that "protecting data privacy in private IaaS cloud computing is a

major concern of customers". He also added that he complied with mandates for the projects or received them depending on the data whether it was federal or healthcare data. In the experience of Participant 2, maintaining data integrity and privacy was achieved by adhering to the HIPAA rules and regulations of securing PII. Review of the three organizational documents and my field notes verified that the security policies of these organizations were centered on HIPAA and NIST privacy requirements to maintain data integrity and privacy by using security measures such as multifactor authentication, encryption, and authorization. A research study by Sudha (2015) supported the participants' experiences by stating that reasonable security requirements in place which addresses authentication, data anonymity, and user privacy will enhance data integrity and privacy of customers' PII. Gootman (2016) noted that using a multifactor authentication process such as a strong password and a PIV card will minimize the risk of hackers gaining access to PII. The findings showed that only two out of three participants from one case reported using data integrity and privacy.

Findings align with the result of Christensen (1997) because the use of cloud computing by organizations has achieved its performance trajectory due to disruption in the IT market. Despite all the security challenges, the findings of this study show that organizations have developed security measures to safeguard data in private IaaS cloud computing. The importance of these well-defined security measures have led to market disruption, which researchers noted happens when the performance trajectory of the cloud computing product has spanned the performance trajectory and is now adopted by conventional organizations (Christensen, 1997; Surya, Mathew, & Lehner, 2014). Storing

data in cloud computing has disrupted the business logic of organizations traditionally storing data in physical data centers (see Kumar & Vardhan, 2018). Christensen (2007) expressed that firms are aware of the innovations; however, their business plans do not permit the organizations to seek innovation when it initially emerges because it will take away scarce resources from their business focus required to contend against its competitors.

Theme 2: Measures to Address Security Controls in Cloud Computing

Measures to address security controls in private IaaS cloud computing emerged as the second theme from the data analysis of this study, and it was addressed by all the participants. The findings showed that when DBAs used measures to address security controls in cloud computing, it safeguards the database from data breaches in cloud computing. This second theme contained several subthemes mentioned by the participants and in the organizational documents. The findings identified six key subthemes:

- firewall installation;
- data Monitoring/Data auditing;
- analysis of Existing data;
- running security patches;
- use of cookie;
- IP tracking.

The data in Table 3 lists the subthemes for measures to address security controls in cloud computing. The research study participants identified these subthemes based on

their experiences from various projects in different organizations. Table 3 also reflected the frequency (number) of participants who indicated that these factors were beneficial for enhanced system performance. Table 3 also shows the number of supporting documents associated with each subtheme.

Table 3

Frequency of Second Major Theme

Source of data collection	Firewall installation *(f)*	Database monitoring and auditing *(f*	Analysis of the existing data *(f)*	Running security patches on monthly basis *(f*	Use of cookies *(f)*	IP tracking *(f)*
Participants	5	5	5	1	1	1
Documents	7	3	7	3	2	0

Note. f = frequency.

Firewall installation. Firewall installation was a common security control subtheme used by almost all of the participants to secure data in private IaaS cloud computing. Table 3 shows the six important components of the measures to address security controls in cloud computing. Table 3 indicates the frequency (number) of participants who indicated these components of measures to address security controls in cloud computing. All participants mentioned that they have implemented firewalls as the gateway to secure data in cloud computing. Participant 1 indicated that the firewall was the first security control used when users attempted access to the three-tier architecture. Participant 2 and 3 further emphasized the use of a firewall to firewall used as loops for

the actual network login, so when one firewall is hacked, another firewall is set up with a different network. Participant 2 mentioned that his organization used Palo Alto firewall network protection. Onag (2018) found that the Palo Alto firewall is an innovative firewall network that has incorporated cloud security into its main features. Participant 4 also described a firewall as a network security for cloud computing to minimize data breaches. Participant 5 also mentioned that firewalls are pivotal as the first line of defense in preventing data breaches in cloud computing. Table 3 also shows the number of supporting documents that contained these measures to address security controls in cloud computing. All documents recommended the use of firewalls. The findings indicate that firewall installation was an effective security control measure used by DBAs to secure data in cloud computing. This supported Jaidi who described a firewall as a security strategy that served as a gatekeeper of system entryways by checking approaching parcels using security filtering rules to identify authorized parcels (2019). Zia and Ali (2018) also emphasized that firewall installation is a security gateway that screens the system traffic dependent on certain guidelines. The findings indicated that DBAs used firewalls installation as a security control to effectively secure the entryways of data from unauthorized access. Simpson and Foltz (2017) also concurred that firewalls served as a screening tool for network ports to secure its boundaries and endpoints. Participants from both cases shared the commonality that firewalls were a means of securing data in IaaS cloud computing. One out of three participants from each case emphasized that the firewall is the first line of defense or the first step in security control, while participants from one case referred to a firewall as a safety loop.

My analysis of organizational documents and review of the participants' responses indicated that firewall installation was a critical measure used to address security control, which led to a secure database and improved system performance. In reviewing the organizational documents, including the security policies and procedures, I found that firewall installation contributed to effectively safeguarding data stored in cloud computing. Based on the DIT conceptual framework of this study, the findings demonstrated that the DIT model reached Christensen's "performance trajectories" because cloud computing performance has improved the way organizations do business since data are no longer stored in traditional physical datacenters and it is now stored in the cloud (Surya et al., 2014). One of the four key elements of the theory of disruption as evident by King and Baatartogtokh (2015) implied that incumbents in the market are improving along a performance trajectory of sustaining innovation. Furthermore, Table 3 shows the frequency of supporting documents that contained information about these components.

Database monitoring/auditing. Database monitoring/auditing is the second subtheme used by DBAs to ensure the safety of data in cloud computing from data breaches. All participants from both cases responded that they implemented database monitoring/auditing to track the traffic flow of users' access to the database. Participant 1 indicated that database monitoring/auditing is done "when a user attempts to access the database, their password and role are verified based on the permission given. Once permission is validated, then a query goes through the database and allows the user access to the specified data that they have permission to access". Contributing to the

security control of database monitoring/auditing, Participant 2 noted that "setting up end-to-end monitoring and real-time monitoring of the database, allowed them to flag any suspicious activities noticed and implemented a solution. According to Participant 2, this process of flagging suspicious activities in the database provides an important advantage of making it possible to trace the activity and minimize database breach. Participant 4 indicated that he used "active monitoring and alert, and endpoint management software to identify suspicious access to the database". Participant 5 echoed the statements of the previous participants that database monitoring/auditing is a well-defined security control, but indicated that giving administrative access to leaders in organizations can be a potential for loss or breach of data. Participant 4 indicated that the standard auditing used in his organization is transactional. Participant 6 noted that data monitoring was used to verify users' roles accessing the database. Regardless of the commonality that all participants from both cases used data monitoring and auditing, DBAs' responsibility is to ensure the safety of data in cloud computing from data breaches. One participant from one case stated that data monitoring and auditing track suspicious activities in IaaS cloud computing, while another participant voiced concern about giving administrative rights to leaders can be a potential for loss of data or data breaches. Despite the difference in the size of the cases, the responses of the DBAs varied at times based on their focus of interest such as giving administrative rights access to leaders or flagging suspicious activities in the data stored in IaaS cloud computing.

My analysis of the three documents (Information Security Policies: Data Breaches Response Policy, Security Incident Management Policy, Information Security Policies:

Access Control Policy) confirmed the usage of database monitoring/auditing as a well-defined security strategies to prevent database breaches in private IaaS cloud computing. These organizational documents also supported the findings that user roles were assigned to users per DBAs based on their roles in the organization. Contributions by Tipton, Forkey, and Choi (2016) supported the findings of database monitoring and auditing allowed DBAs to restrict access to the database to the right users while preventing access to the database to unauthorized users. The data identified in these documents collaborated with the responses from all participants. Therefore, the study supported the DIT conceptual framework that guided this study. The role of the DBAs is to monitor database traffic by determining if the user accessing the system is a legitimate user and can access the data (Zhou et al., 2017). Wang et al. (2018) reported that database monitoring/auditing software implements audit controls, which logs and examines users' activities to the database to minimize malicious attacks to data in the cloud. This ensured that the user seeking access is authorized and verified to access the database (Wang et al., 2018). Cloud computing is a disruptive innovation technology for traditional IT organizations (Bohnsack & Pinkse, 2017); this conflicts with the original organizational logic of storing data in traditional physical data centers because data are stored remotely in the cloud (Bohnsack & Pinkse, 2017). These findings aligned with the DIT framework because the customers have made the switch to the new way of storing data in the cloud which supports the results of Bohnsack and Pinkse (2017) who found acceptance of cloud computing when cloud computing performance has approved to an acceptable level.

Analyzing the existing database. The analysis of existing databases is the third

subtheme used by DBAs to ensure that the information or data held in private IaaS cloud computing systems is protected from data breaches. For IT organizations, analyzing data for vulnerability is pivotal. Chennam and Lakshmi (2016) indicated that the primary objective of storing data in the cloud is to safeguard the data from unauthorized access by external and internal users. The findings from Participant 1 and Participant 2 supported the safeguarding of data by unauthorized users by using a standard process. This process involved scanning the logs and application events to determine who accessed the database, what changes were made to the database, what network connections and ports to the database were manipulated in 24 hours, and if a threat is identified, then database monitoring solutions are implemented. Participant 3 indicated that an alert is received if the database is manipulated. Participant 4 says security checks are in place to find out why data are downloaded on to the DBAs laptops and why? Participant 5 echoed Participants 1, 2, and 3 statements that security scans analyzed the database by checking all code systems, all files, and passwords not encrypted. These findings determined weak code or vulnerability, and this allowed the DBAs to take steps to secure the database from vulnerability or threats. The findings were supported by Ghazi, Masood, Rauf, Shibli, and Hassan (2016) who were cited in the professional and academic review. Ghazi et al. (2016) noted that analyzing the existing database includes auditing, which analyzed users' actions to track suspicious activities of the database. The findings supported the third subtheme, which aligned with the disruptive innovation theory (Christensen, 1997). The DIT framework influenced organizations to change their business logic from storing data in traditional physical data centers to storing data in the cloud. Over time, cloud

computing initially supported by entrants organizations have shifted the way incumbent organizations that supported the physical storing of the database in data centers now store data (Danneels, 2004**).** This storing of data in the private IaaS cloud computing involved security strategies to prevent data breaches and enhanced system performance was consistent with the theme of this study. All the DBAs from one case and two out of the three DBAs in the second case concurred that analyzing the data ensures the safety of data in private IaaS cloud computing from data breaches. DBAs should use this measure to address security controls in cloud computing.

In reviewing the organizational documents (Information Security Policies: Data Breaches Response Policy, Security Incident Management Policy, Information Security Policies: Access Control Policy) provided by the organizations, I identified that the focus was on safeguarding data from data breaches. This safeguarding of data, enhanced trust in customers to store their data in the cloud and improved database integrity and performance. Effective safeguard of data using security measures such as analyzing the database, was consistent with the findings from Participants 1, 2, 3, 4, and 5. These findings were supported by Kumar and Vardhan (2018). Kumar and Vardhan (2018) highlighted that large organizations have now shifted to using cloud computing from using physical data centers due to the requirement of high-cost traditional computing infrastructure and the procurement and maintenance of IT resources. Consistent with the theme was the study by Shen, Liu, Liu, He, and Sun (2017). Shen et al. (2017) indicated that storing data in the cloud minimizes storage burden and relieves organizations from hardware maintenance; however, this poses security challenges. Analyzing the database

and auditing protocols were cited by Shen et al. (2017) as one of the strategies to minimize data breaches. The findings also aligned with the DIT framework for this study. Based on the DIT model, cloud computing as a new business model has disrupted the traditional way of organizations storing data from the traditional physical infrastructures storage to storing data in the cloud (Christensen & Raynor, 2003).

Running security patches. Running security patches monthly is the fourth subtheme used by DBAs to ensure the safety of data in cloud computing from data breaches in private IaaS cloud computing. Haber (2015) indicated that installing the latest security patches helped decrease vulnerabilities in cloud computing. Participant 3 indicated that his DBA experience involved applying recent security patches in cloud computing to minimize data breaches. Participant 3 also indicated that these security patches are applied as a precautionary approach either monthly or quarterly. This finding supported the theme of the study and aligned with the DIT conceptual framework. Only Participant 3 mentioned applying security patches to minimize data from breaches in cloud computing. The views of Participant 3 were supported by Avery and Wallrabenstein (2018), cited in the professional and academic literature, emphasizing that using traditional preventive measures such as security patches initially will minimize data breaches from happening. A recent study by researchers Adamski, Kurowski, Mika, Piatek, and Weglarz (2017) denoted that security patches signify an occurrence, which can be treated as the protection against vulnerability and minimized the database in cloud computing from data breaches. The research reinforced the responses from Participant 3 when asked what security measures were in place when database breaches were

encountered. Findings from Participant 3 and the organizational security documents were aligned with the DIT framework. Not only did the findings align with the organizational documents, but it also supported the research question of what are strategies DBAs use to secure data in private IaaS cloud computing. Therefore, running security patches is a well-defined security control measures used to secure data in private IaaS cloud computing. Despite cloud computing is a disruptive innovation technology, it has improved along a performance trajectory of sustaining innovation (King & Baatartogtokh, 2015). Ironically, only one participant reported the use of running security patches on a monthly basis from one of the cases. I find the use of running security patches on a monthly basis as a unique strategy that was not mentioned by any of the five participants that DBAs can use to minimize data breaches in IaaS cloud computing.

Use of cookies. The use of cookies is the fifth subtheme used by DBAs to ensure the safety of data in private IaaS cloud computing from data breaches. The use of cookies is a security control used to track unauthorized users' access to data in cloud computing (Samarasinghe & Mannan, 2019**)**. Participant 2 was the only participant who mentioned that cookies were used as a security control in safeguarding data in the cloud. Participant 2's response was aligned with the research study by Samarasinghe and Mannan (2019). Supporting Participant 2's views was the study by Mazel, Garnier, and Fakuda (2019). Mazel et al. (2019) stressed that the use of cookies tracked user identification and this helped enhance data collection. Also supporting the use of cookies was a study by Bugliesi, Calzavara, Focardi, and Khan (2015). Bugliesi et al. (2015) indicated that a cookie encodes user sessions, which allowed malicious activities of the database to be

tracked. Only one participant from one case supported the use of cookies as a measure to address security controls in cloud computing. DBAs should consider using cookies as a security control to prevent data breaches in cloud computing.

In reviewing the three documents provided by the organizations, I found that the documents addressed steps to follow whenever unauthorized system access was suspected or identified, and immediate action must be taken to terminate the system access. The information from the records of the organizations was consistent with the existing literature (Ramachandran & Chang, 2016). Ramachandran and Chang (2016) also emphasized that security policies should be modified at regular intervals and employees are provided routine and formal training on security. Fostering training on security updates is critical to minimizing data breaches. Participant 2 mentioned that training staff on security awareness is pivotal about how to minimize potential threats and data breaches. Participant 2's view was consistent with literature by Ghafir et al. (2018) that integrating security awareness tasks into daily assignments of employees help maintained and utilized the information garnered in training. This security awareness training, in turn, will minimize data breaches in cloud computing that will enhance DBAs knowledge of security strategies that they can use to prevent data breaches in IaaS cloud computing.

The findings of the researchers supported the fifth theme and also aligned with the DIT framework that guided this study (Christensen, 1997). Also, supporting the findings was the research of Ghafir et al. (2018), who noted that cloud computing is a low-end disruptive innovation technology that slowly outperformed existing technology. As noted

in this study, data are now stored in the cloud instead of in the traditional physical data centers. With the security challenges in cloud computing such as data breaches, DBAs may use this fifth theme as a security control to minimize data breaches.

IP tracking. IP tracking is the sixth subtheme used by DBAs to ensure the safety of data in private IaaS cloud computing from data breaches. IP tracking is a new method of tracking IP addresses to identify unauthorized access to data in cloud computing. Supporting this finding was research by Jin, Guo, Dutta, Bidmeshki, and Makris (2017), who noted that tracking data flow is a powerful approach for preventing sensitive information from reaching untrusted sites. The statement was consistent with Participant 5's views. This participant indicated that "there are several security companies out there that trace signals, where do they come from, where are they going to as an example". Researchers like Mansoori, Welchi, Choo, Maxion, and Hashemi (2017), on the other hand, confirmed that IP tracking is a security control used to screen users' access to databases, which enabled the site to give or deny users' particular access rights. The findings of this study explored the notion of tracking database users who are authorized to legitimately access data stored in cloud computing. This IP tracking of unauthorized users helped DBAs minimize data breaches in cloud computing. Only one participant from both cases reported using IP tracking as a measure to address security controls in IaaS cloud computing. The use of IP tracking by DBAs will be beneficial to prevent data breaches in IaaS cloud computing.

The goal of these security controls is to help minimize data breaches and data thefts, which would slow down the system performance of the databases. Also supporting

the theme of this study was Adamski et al. (2017), who concurred with the study findings that attacks and thefts of data altered and compromised the system performance of the database. Cloud computing as a disruptive innovative technology brings with it many security challenges and DBAs have to implement security strategies in place to minimize data breaches and secure data of their customers to build trust. Improved use of the performance trajectory of cloud computing as a DIT has shifted the IT organizations to move to use data to produce maximum efficiency (Rizvi, Karpinski, Kelly, & Walker, 2015).

Theme 3: Limitations of Existing Security Controls in Cloud Computing

The third theme to emerge from the findings of this study is the limitations of existing security controls in cloud computing. This third theme developed from the participants' responses, the data analyzed from the organizational documents, and the findings from previous research studies. Table 4 lists the frequency and significance placed upon the limitations of existing security controls in cloud computing as described by the participants and clarified within the provided organizational documents. Table 4 depicted four important subthemes that were evident from this study and the frequency (number) of participants who indicated these limitations of existing security controls in cloud computing were essential to secure data in cloud computing. The frequencies are not mutually exclusive, meaning that two or more of these subthemes may be included in one document.

Table 4

Frequency of Third Major Theme

Source of data collection	Stringent passwords *(f)*	Human factor *(f)*	Secure sockets layer *(f)*	Standardizing security approach *(f)*
Participants	3	4	3	5
Documents	7	3	7	3

Note. f = frequency.

Stringent passwords. Stringent passwords have been the least effective means of protecting access by organizations and it is also the least effective way to safeguard data from data breaches. Participant 1, when asked what were the least effective security measures used in preventing cloud computing data breaches, responded that "stringent password controls used by the system are fine, those are secure. But if you make your password policy too stringent for the user, the user is just going to write it down and stick it up on their monitor". Participant 3 noted that "passwords should be changed every 60 days and the DBAs forcefully push the change". Participant 4 indicated that his organization focuses more on multifactor authentication instead of using stringent passwords. This feedback from the DBAs ties my study findings with findings from a similar study by Wei, Jiang, Zhang, and Ma (2017), who found that strong secure authentication is required to protect users' privacy. This finding also supports the works of Greengard (2015) in the literature review that proposed the need of consumers wanting more robust protections instead of using stringent passwords. Further, Greengard (2015) believes that a password is a rendition of skeleton keys and organizations cannot keep on

going down the path of failure. Two out of three of the participants in one case expressed concern about the limitations of stringent passwords and this may expose data stored in the cloud to vulnerability. The two participants recommend that passwords must be changed forcefully every 60 days and the DBAs are responsible for this forceful push of the 60 days change generated from the system. However, one participant from one of the cases emphasized that his organization was more focused on the use of multi-factor authentication instead of the use of stringent passwords.

Methodological triangulation was achieved by reviewing the organizational documents that supported the subtheme. As shown in Table 4, all the seven documents (HIPAA Security Rules, United States (US) Digital Guideline NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Information Security Policies: Data Breaches Response Policy, Information Security Policies: Third-Party Security Management, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy, Business Associate Agreement) addressed standards for the security of sensitive data, training of employees on the various types of security incidents that may trigger a data breach, and the process to follow when unauthorized system access is suspected or triggered. My analysis of the organizational documents and participants' answers show that the security of data in cloud computing is pivotal in an organization, which leads to enhanced system performance and builds trust in customers.

As pivotal to the DIT framework for this study, the research findings for this third theme showed that the performance trajectory of cloud computing has changed the

business logic in IT organizations. Weeks (2015) asserted that as new technology develops, it improves over time, and this meets the need of the large organizations in the business. Therefore, in the long run, the existing organizations are forced to change the way they conduct business as the disruption addressed the issues of the emerging market (Weeks, 2015). With continuous monitoring and adjustments, organizations have made strategic adjustments over time to change their business logic (Chen et al., 2016) by adopting storing data in the cloud instead of in traditional physical data centers.

Human factors or errors. With data now being stored in the cloud, the human factor is the second subtheme of the limitations of existing security controls in private IaaS cloud computing. In designing IT systems, human factors or errors should be considered as a challenge to prevent database security breaches. Participant 1 indicated that "in dealing with security on its own and you don't take into account human behavior, agencies or organizations will define policies that sound secure in the real world, but the problem is no one will conform to them in the manner they think they were intended". Participant 1 further explained that he had one project were the password sequence had twenty-plus characters and it involved so many symbols and weird characters that no one was going to remember it. He made it easier for the program to figure the complex password. Participant 1 also opined that human-centered design is the key to an organization's security policy. Participant 2 noted that the human factor results in limitations of existing security controls because it is an internal threat that is ineffective to prevent cloud computing data breaches. Participant 4, when asked what are your concerns in implementing security measures and what has the organization done to

rectify these concerns, responded that human errors are the leading cause of unauthorized access to data in cloud computing. Participant 5 also affirmed that human factors are the cause of most unauthorized access to PII. The results from this study supported the work by Sharma, Javadi, Si, and Sun (2016), who alluded that human errors are due to inexperience, and believed that social engineering is the root cause of human errors. Previous studies by Ghafir et al. (2018), also supported the second theme because, through social engineering, hackers can compromise database security through users' interactions. Safa, Solms, and Futcher (2016) further indicated that the human factor is a threat to data security. Two participants from each case concurred that human error is the leading threat to data security breaches. The findings of the researchers supported the second theme and are aligned with the DIT framework that guided this study. DIT not only enhances the performance of the database when adopted by organizations, but it also improves cost savings due to business logic change from using traditional physical storage like servers to storing data in the cloud (Ramachandran & Chang, 2016). DBAs should focus on successful security strategies such as multifactor authentication that would minimize the use of too stringent passwords that would minimize human errors.

Three documents (Information Security Policies: Data Breaches Response Policy, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy) were used in achieving methodological triangulation to enhance the reliability and validity of this theme. These documents as shown in Table 4 focuses on security policies and procedures when data breaches occur. In reviewing these three documents, methodological triangulation showed security

strategies DBAs used. The documents guide DBAs on security awareness for effectively safeguarding data from data breaches. These documents support the theme and agree with the conceptual framework for this study because cloud computing has changed the business logic of how organizations now store data and protecting data in the cloud needs robust strategies to prevent data breaches. DBAs have to ensure that purposeful updates through staff training on security awareness are critical to minimize human errors.

Secure Sockets Layer (SSL). The secure sockets layer is the third subtheme of the limitations of existing security controls in private IaaS cloud computing of this study findings. SSL is important and aligns with DIT because it protects data in the cloud when it is transported to prevent data breaches since cloud computing data storage has security challenges that may compromise data integrity. Three out of the five participants responded that their concern in implementing security measures in cloud computing is SSL. The theme emerged from the responses of three participants and my analysis of all the seven documents provided by the organization. Methodological triangulation was achieved with five out of the seven organizations' documents.

Findings from the participants indicated that SSL certificates are required to protect sensitive data. This finding supports Shahzad (2014) who indicated that SSL certificates are pivotal in protecting sensitive data. Participant 1 noted that different levels of SSLs certificates are generated to authorize users' access to specific databases. Without this authorized SSL, data in transit may experience a middle man attack. Participant 3 specifically noted the importance of connecting to the database that SSL certificates are used and authorizing agencies are asked to sign the certificates and

provide the level of access it requires for each user. Participant 4 further emphasized that SSL is a certificate of authority that is system generated. Participant 4 also explained that his organization does not have SSL, but they can use open SSL to generate the certificates. This finding is consistent with the conceptual framework for this study because cloud computing an evolving disruptive innovation brings with it many challenges such as data security that needs to be addressed to minimize data breaches. In the review of professional and academic literature, Ghazi et al. (2016) proposed that SSL is a strategy to protect encrypted data in transit so that the right person receives the data in the correct form. Singh and Chatterjee (2017) indicated that a middle man attack to the data occurs in transit due to a lack of security configuration of an SSL. Participants 1, 3, and 4 confirmed that for the overall data exchange, an SSL certificate must be in place to minimize data breaches. This finding aligned with Tipton et al. (2016). Tipton et al. (2016) noted that it is important for SSL certificates to be in place to secure data exchange. Two out of three participants from one case specified the use of SSL, while only one participant from the second case stated the use of SSL. The DBAs can use SSL to secure data when in transit to ensure it retains its correct form and prevent data loss.

Standardizing security approach. The standardizing security approach is the fourth subtheme of the limitations of existing security controls in private IaaS cloud computing. The responses from 5 participants and analysis from 3 organizational documents showed that the standardizing security approach is a limitation of existing security controls in cloud computing. Participant 1 indicated that DBAs complied with mandates provided by the organization or they receive the mandates depending on the

type of data they are working with such as PII. Participant 3 noted that in his 10 years' DBA experience, he had not seen standard security protocols in place to prevent data security breaches. Participant 3 added that some organizations may have their own customized standard protocol for their security system to prevent data security breaches. Participant 4 also confirmed that there is no standard security protocol in place to prevent database security breaches, and DBAs in his organization comply with laws or regulatory bodies like HIPPA and ISSO 2702 or 2701. Participant 5 also supported that there is no standard security protocol and he added that there is "a delay in the federal posture when new technologies are adopted". Participant 6 described steps taken to prevent database security breaches such as blocking suspicious IP address and data encryption, and was unable to confirm if there is a standard security protocol in place to prevent data security breaches. The literature reviewed showed that there are no standard security protocols in place. However, DBAs have to adhere to the security protocols that the organizations they work for use such as HIPPA, NIST or ISSO 2702 or 2701.

The three organizational documents reviewed aligned with the 5 participants' responses that DBAs complied with regulatory bodies like ISO 2702/2701, HIPPA and NIST or customized security policies internal to the organizations. Recent literature supports the findings of this theme that there are no standardized security policies in cloud computing to prevent data breaches (Hashem et al., 2015). These findings are aligned with Togan (2015), who noted that a lack of standardization of security solutions for cloud infrastructures has led to some organizations not implementing cloud

computing. Existing research is consistent with the findings from previous studies and the participants in my study regarding the existing security controls in cloud computing.

Security is a pivotal challenge when storing data in cloud computing and the responses from the participants alluded to the lack of standardized security controls in cloud computing. The framework supported the findings as DIT promoted redefining marketplace expectations by physically changing the traditional way of storing sensitive data in cloud computing (Yu et al., 2017). Despite the lack of standardization in cloud computing, the literature supports the participants' responses, and security remains a challenge. DBAs need to develop well-defined security strategies to prevent database breaches in cloud computing.

Theme 4: Future and Potential Security Measures Solutions in Cloud Computing

The fourth theme to emerge from the data collection and analysis was the future and potential security measures solutions in private IaaS cloud computing. This fourth theme developed from the participants' responses, the data analyzed from the organizational documents, and the findings from previous research studies. Table 5 lists the frequency and significance placed upon the future and potential security measures solutions in cloud computing as described by the participant and clarified within the provided organizational documents. Table 5 depicts three important subthemes, which were evident from this study and the frequency (number) of participants who indicated that the future and potential security measures solutions in cloud computing were essential to secure data in cloud computing.

Table 5

Frequency of Fourth Major Theme

Source of data collection	Security iterative living process (*f)*)	Leadership (*f*)	Delay in adopting new technology (*f*)
Participants	1	3	1
Documents	7	3	7

Note. f = frequency.

Security iterative living process. The security iterative living process is the first subtheme of the future and potential security measures solutions in private IaaS cloud computing. Ramachandran and Chang (2016) noted that the use of cloud storage and social networks have transformed IT social collaborations and communications of people. However, data security continues to remain a challenge and an iterative process when organizations store their data in the cloud. Among the 6 participants that participated in this study, only Participant 1 believed that security is an iterative process. Participant 1 indicated that the biggest concern is that "the old way of conducting business before cloud computing was once you get security right at the beginning, no vulnerabilities will ever happen". Participant 1 also emphasized that security in cloud computing is an iterative process that requires continuous upgrades and changes in the future to be effective to adapt to the real world discovered exploits. Only one participant from one case reported security as an iterative living process. The remaining 5 participants did not provide any input about security being an iterative process. With the evolution of cloud

computing, organizations using cloud computing should also change their views about security because cloud computing has now changed the way organizations store data and that poses security challenges. It's the DBAs responsibility to ensure that the security updates are done to stay abreast of the technology advancements to implement successful security strategies.

Table 5 depicts the number of participants who believed that security in cloud computing is an iterative process for future and potential security measures solutions in private IaaS cloud computing, as well as the organizational documents reviewed to align with the study findings. The 7 organizational documents provided focused on security and the process to follow when security breaches occurred. Recent academic literature by Mjihil, Kim, and Haqiq (2016) indicated that with cloud computing evolution, security frameworks should be adapted to support the new features of cloud computing. The use of traditional security solutions is no longer effective for maintaining data privacy in cloud computing (Srivastava, 2017). Shahzad (2014) recognized that traditional security measures such as firewalls to secure data are ineffective against external and internal threats. The study findings aligned with Mjihil et al. (2016) because security in cloud computing is an iterative process requiring future updates and changes. These findings also supported the fourth theme of this study.

My analysis of the organizational documents and participants' responses showed that effective security solutions for cloud computing are an iterative process due to the evolving feature of cloud computing as innovative technology. The conceptual frameworks that guided this study, was the DIT framework (Christensen, 1997), and the

findings of this study supported the framework. As related to the DIT model, the findings of this study suggested cloud computing a disruptive technology has spanned its performance trajectory. Due to this disruptive nature of cloud computing, conventional organizations have now adopted the cloud (Christensen, 1997; Surya et al., 2014). Based on the finding, the first subtheme depicted that security is an iterative process. Therefore, cloud computing has revolutionized the IT social collaborations and communications of people (Ramachandran & Chang, 2016).

Leadership. Leadership is the second subtheme of the future and potential security measures solutions in private IaaS cloud computing. Organizational leaders or authorities play a critical role in how robust and effective security solutions should be in cloud computing. The responses from three participants and my analysis of 3 out of the 7 organizational documents indicated that organizational leaders believed that their IT infrastructures were secure and that their existing security policies are reliable safeguards against data breaches. This finding supports Noguerol and Branch (2018), who found out that organizational leaders do not fully understand security controls and are less likely to enforce security controls, which places the integrity of the data at risk. Participant 5 noted that "organization administrators do not want to assume responsibility and the easiest way to mitigate responsibility is to handover an IT requirement sheet to a DBA and tell them what to do. The person making the request does not care how it is done and it's the DBA's job to figure out the most secure way possible to get it done". This finding was consistent with the contributions by Moon et al. (2018), as cited in the professional and academic literature. Moon et al. (2018) emphasized that security executives are

consistently tested with how to adapt the information needs of the business with the IT security resources. The responses from Participant 5 aligned with Moon et al. (2018) academic literature. DBAs have to openly communicate to organizational leaders the importance and criticality of securing data in the cloud and the robust updating of the system to minimize data breaches.

In contrast, Participant 1 alluded that organizational leaders operate with the notion that "once security is right at the beginning and there are no vulnerabilities, the database is secured". Participant 6 indicated that leadership wants security and do not want to spend money on it. For example, if no data breaches occur, the organizational leaders think their data are secure and security updates are not required. Participant 6 also added that some organizational leaders do not allocate enough money in their budget for data security. This supports Choong et al. (2016), who found that with the increasing challenges of cyber-attacks, the budget allocated for data security remains low because organizational leaders want justification of system breaches, which is hard to justify. With the cost-savings capability that cloud computing brings, organizational leaders should change the way they do business by including the budget cost for cloud computing, which will improve economic performance and make organizations more competitive (Schniederjans & Hales, 2016). The participants' concerns raised about organizational leaderships' lack of support in investing in IT security training and resources may have an impact on employees not fully vesting their time and effort in adhering to security requirements. As indicated by Paliszkiewicz (2019), the commitment of an organization's leadership is pivotal in an employee's behavior and attitude toward

security compliance. The responses from Participant 1, 5, and 6, aligns with the Paliszkiewicz (2019) academic literature. This subtheme aligns with the DIT conceptual framework for this study. Therefore, cloud computing is a disruptive technology that continues to change the way organizations now store data to remain competitive in the IT market. Moreover, leadership should be willing to allocate funds toward securing data stored in cloud computing

Delay in adopting new technology. Delay in adopting new technology is the third subtheme of the future and potential security measures solutions in private IaaS cloud computing. Participant 5 opined that "the federal government is slower in adopting cloud computing due to the security concerns, so that is why there is a delay in the federal posture when they take on new technologies". Participant 5 also indicated that organizational leaders are hesitant to adopt cloud computing due to the lack of standardization and regulations. Ramachandran and Chang (2016) purported that outsourcing of data to cloud service providers may result in increased security concerns such as unauthorized access to data and data security breaches. Setting in place stringent security regulations and governance on cloud computing will build the confidence of organizations and IT executives and leaders to adopt cloud computing (Ramachandran & Chang, 2016). Sharma et al. (2016) supported Participant 5's opinion that cloud computing lacked standardization, which aligned with the response from Participant 5. Only one participant from one case spoke about the delay in adopting new technology as a future and potential security measure solutions in cloud computing. The remaining 5 participants did not provide their experiences about the delay in adopting new technology

by federal organizations. DBAs should stay current with the evolving changes in information technology and keep leadership apprised of new technologies to get a competitive edge.

My review of all the 7 documents provided by the company confirmed the findings from the participants that there is no security standardization in cloud computing. Previous researchers also supported these findings (Mjihil et al., 2016). Mjihil et al. (2016) found that because there is no standardization in cloud computing security, CSPs are introducing new features and techniques to help organizations maintain their cloud architectures, which is increasing consumers' trust in using cloud computing. Taylor (2017) revealed that Data migration from the traditional physical data warehouses to the cloud can be puzzling for government organizations because the organizations' lose control of their data to a third-party and that results in a change in the organizational structure and makeup.

Therefore, the documents, responses, and experiences of one participant from one of the two cases supported the theme of this study and aligned with the DIT framework of Christensen (1997). Shahzad (2014) also indicated that cloud computing a disruptive technology has revolutionized the way organizations' do business because of the potential advantages it provided such as collaboration, agility, scaling, availability, and low-cost savings through efficient computing. Moreover, Barrow et al. (2016) stressed that cloud computing will remain a disruptive technology trend for organizations without standard security controls in place. The results of this study revealed that well-defined

security strategies developed by DBAs are critical to the success of cloud computing use by organizations.

Applications to Professional Practice

This study intended to explore the strategies used to secure data in private IaaS cloud computing by DBAs working in IT settings in Baltimore, Maryland. The findings of this study, in conjunction with an analysis of its conceptual framework and a review of academic literature, added to the existing body of knowledge of security strategies to increase security posture in general and, more specifically, in the area of database breaches. The findings are pertinent to DBAs, IT security professionals, software and hardware developers, chief information officers (CIOs), and IT training professionals to enhance and strengthen the IT infrastructure and promote its operational and technical safety. Participants of this study indicated that their participation would contribute to the enhancement of the limitations of existing security controls in cloud computing.

With the increasing growth of internet use, training and education are required to enhance security awareness and minimize the database security breaches. By providing successful security strategies, other organizations may adopt these successful strategies and enhance customers' trust. Watts (2015) opined that data breaches can be costly and damage an organization's reputation. Watts (2015) added that training and empowering staff to secure data is key to remaining competitive and improving the security stance of the IT organization.

The strategies illustrated by the findings from this study will secure data while also improving the reputation of IT organizations, build confidence and trust in

customers, protect assets, and avoid unsurmountable legal costs in IT organizations. Well-defined security strategies such as authentication, authorization, encryption, and data integrity and confidentiality can be used as best practices for DBAs and IT professionals. These best practices may lead to innovative trends, which may lead to the improvement of the security posture of the organization, as well as the prevention of security breaches. Also, the results of this study are meaningful since they provide a platform for DBAs to improve the existing security strategies and improve the reputation of organizations, thereby keeping it competitive.

Investment by leadership and authority in IT security strategies on an evolving basis will make the IT infrastructure robust and improve data protection. This leadership and authority support may enhance the efficiency and effectiveness of the DBAs in managing and minimizing database breaches.

Implications for Social Change

Exploring well-defined security strategies DBAs may be a significant step to ensure data integrity and minimize data breaches in organizations. From a social change perspective, the findings of this study may be useful to organizational reputation by building trust and confidence in their customers. A reputable organization may result in decreased identity theft and maintain a safe community. These study findings added to the existing knowledge of literature by providing information and knowledge on well-defined security strategies DBAs in IT organizations can use to prevent database breaches in private IaaS cloud computing. The study findings may result in positive social change

as more DBAs successfully implement security strategies that may protect customer sensitive data and build trust in consumers to store data in cloud computing.

Moreover, the findings explained that when DBAs implement well-defined security strategies, which promotes a positive environment and data stored in the cloud will be secured, and customers' data integrity will improve customer satisfaction and system performance. The study findings identified key factors necessary for securing data stored in cloud computing, which will protect PII of customers and protect them from identity theft. In 2015, the Office of Personnel Management (OPM) experienced two massive cybersecurity attacks and PII was stolen (Gootman, 2016). After this OPM attack, concerns have increased from the federal employees, as well as the public about the safety of their PII and is it protected (Gootman, 2016). The study findings provided an exploration and analysis of the security strategies used by DBAs that may positively impact social change by protecting its citizens and customers' PII. Successful security strategies when implemented will enhance the protection of PII, which will benefit society and communities by building confidence and flexibility in customers' use of innovative technology. Thus, customers need to have trust that storing their sensitive data in cloud computing will not adversely impact their lives, and preventing data breaches is a key component to achieving customer trust in storing data in the cloud computing. The well-defined security strategies will protect an individual's data which in turn will promote their well-being and build strong communities and society. These well-defined security strategies will safeguard services such as healthcare and financial institutions. Data breaches when successful, results in disruption of power and customers losing

access to their data in financial and healthcare organizations. There are rising concerns from the communities and society as a whole calling on the government to safeguard customers, patients and citizens' PII (Gootman, 2016). These study findings explored well-defined strategies when implemented will successfully protect data that will benefit communities and society by ensuring that data integrity of healthcare and financial organizations are sustained during data breaches. Fully sustaining and successfully protecting sensitive data of citizens in the community and society during data breaches will enhance IT reputation and posture. Further, this successful use of the well-defined strategies will also promote trust and confidence in customers to use cloud computing to store data in healthcare and financial institutions.

Recommendations for Action

The study findings revealed four key security strategies that DBAs can use during IT security awareness training and implementation. The desire for effective security strategies to prevent database breaches is increasingly pivotal and presents new challenges that must be addressed by DBAs, especially with the evolving technological innovations. Strategies that have shown to be effective from this study for IT practitioners include:

- importance of well-defined security measures in cloud computing;
- measures to address security controls in cloud computing;
- limitations of existing security controls in cloud computing; and
- future and potential security measures solutions in cloud computing.

I recommend that each organization conduct a security gap analysis of their IT security strategies and identify which well-defined strategies worked to prevent data breaches and use these well-defined security strategies as baselines to secure data in cloud computing. The measures to address security controls in cloud computing can be used by IT organizations and stakeholders to create collaborative cloud computing security and compliance programs. The third recommendation is to IT leaders and security professionals are to establish security awareness and compliance in IT organizations and emphasize security awareness through training and constant reinforcement in the workforce. The final recommendation is the buy-in and support of organizational leaders to allocate and invest in IT security programs that will protect data in cloud computing on an evolving basis. These findings were significant and supported current literature on security strategies to prevent database breaches in cloud computing, as well as the organizational documents. Findings from this study are important to organizations storing data in the cloud such as healthcare organizations, banking institutions, retail organizations, and academic communities.

The participants in this study emphasized the importance of well-defined security measures in cloud computing. DBAs must consider that with technology becoming more sophisticated and continuously evolving, new security challenges will emerge that will need to be addressed. With these changes in security challenges, security strategies are not expected to remain the same. DBAs must consider how to keep users informed and aware of the changes in security strategies to minimize database breaches.

Disseminating the findings of this study will take place after receiving CAO approval for this study. A two page summary of the research results will be sent to all six research participants. The study results will also be shared in academic communities through ProQuest database globally to students and scholars. I plan on presenting the study findings in IT security seminars and conferences and publicize my study in peer-reviewed journals.

Recommendations for Further Study

The findings of this study revealed security strategies used by DBAs to prevent data breaches. The limitations of this study were focused primarily in Baltimore, Maryland. Repeating the study in different geographical regions of the United States based on their regulations and security requirements, using a different conceptual framework and methodology will benefit organizations and IT professionals.

This study added to the existing security strategies literature, but additional research is warranted due to the small sample size used of qualified DBAs. Future work may consider the exploration of security strategies with larger sample sizes or larger organizations. Finally, this study has contributed to the body of literature on security strategies on cloud computing, but may also prove beneficial to the healthcare industry, academic communities, and banking sectors.

Finally, this study also recommended some important issues that need to be addressed in the IT marketplace. Based on the literature review and the collected data of this study, recommendations for future research topics were highlighted:

- researchers should explore different encryption approaches to identify the optimal encryption approach that delivers top data security;
- further research needs to explore the barriers preventing leaders from taking proactive security approaches to investing in innovative security strategies that keep them relevant and prevent data breaches in organizations; and
- research should explore the key components to understanding the motivations and triggers of positive behavior change that minimizes external and internal data breaches in organizations.

Reflections

During the research process, my understanding of doctoral-level research developed considerably. I was challenged and amazed by the level of detail and alignment that this research study entailed, and I felt overwhelmed during the data collection and analysis phase. At times I felt like quitting because I had periods of writer's block. In 2015, I became interested in securing data in cloud computing when I became a victim of the massive data breach of the OPM database (Gootman, 2016). As a federal employee, I was a victim of this data breach, and my name, date of birth, address, social security number, and fingerprints were stolen from the OPM database. This identity theft stupendously motivated me with the passion to undertake this study. As an IT professional with over 18 years of experience, I had some bias before conducting this study about IT security strategies. However, I minimized my bias by allowing the participants to express themselves without offering my opinions. My knowledge of the

topic did not bias the study because I used open-ended questions throughout the semistructured interview process, resulting in rich comprehensive data based on the participants' experiences.

I was unaware of how in-depth and time consuming qualitative study was until I delved into the data collection and analysis process. Recruiting participants for my study was a challenge and two out of the eight participants who agreed to participate in my study were unavailable via telephone or e-mail to schedule an interview. Member checking was difficult at first to schedule, but based on my classmates' experiences, I learned that having a quick phone call to the participant proved beneficial instead of another interview for 5-10 minutes. Transcribing the audio-recorded interviews took over two hours for a 20-30 minutes interview due to low voice level and background noise. Analyzing the transcript was also an arduous process because I had to learn how to use qualitative data software. Overall, I was humbled by the interview process and how willing most of the participants were to share their experiences with me. The findings from this study identified well-defined strategies that DBAs can use to prevent database breaches in private IaaS cloud computing.

With this study, I have garnered enough understanding of conducting a qualitative research study that may be used in my next future career. My academic writing skills have also improved since I enrolled at Walden University and I intend to continue building on it. I am now equipped with the academic skillset to venture with confidence in writing research articles on improving security strategies in cloud computing.

Summary and Study Conclusions

Maintaining the security of sensitive data stored in cloud computing is critical to the success of organizations and increases confidence in customers' use of cloud computing. The purpose of this qualitative multiple case study was to explore the strategies DBAs use to secure data in private IaaS cloud computing. The specific IT problem is that some DBAs lack strategies for securing data in private IaaS cloud computing. The case organizations in the study represented critical IT infrastructure in two small business companies in Baltimore, Maryland. This qualitative case study investigated security strategies used for securing data in cloud computing. The study answered the following research question: what are strategies DBAs use to secure data in private IaaS cloud computing? Six out of eight DBAs from two small business companies in Baltimore, Maryland, participated in the semi-structured interviews. Security strategies used by DBAs, illustrated by these findings were:

- importance of well-defined security measures in cloud computing;
- measures to address security controls in cloud computing;
- limitations of existing security controls in cloud computing; and
- future and Potential Security Measures Solutions in Cloud Computing.

There is an ongoing need for data security in cloud computing due to the increase in external threats of sensitive data in cloud computing. Until security issues are settled, organizations should be cautious, guaranteeing that they weigh the security dangers against the advantages of cloud computing, by implementing well-defined controls and strategies (Tankard, 2015). Cloud computing may experience a great rise in its adoption

if all these security challenges are addressed and resolved to increase customers' trust and confidence.

The limitation placed on this study was using a relatively small experienced DBAs from two small business IT organizations in Baltimore, Maryland. The findings from this study were significant and supported by the organizational documents and recent literature on cloud computing security strategies consistent with the DIT framework of this study. As noted in the DIT framework, cloud computing is a disruptive technology and this disruptive trend is due to its security challenges, which need to be addressed and resolved. The findings of this study should have greater applicability to DBAs, as well as other IT organizations that are seeking to use effective security strategies to improve collaboration and increase customers' trust in storing their sensitive data in cloud computing.

References

Adamski, M., Kurowski, K., Mika, M., Piatek, W., & Weglarz, J. (2017). Security aspects in resource management systems in distributed computing environments. *Foundations of Computing & Decision Sciences*, *42*(4), 299–313. doi:10.1515/fcds-2017-0015

Alamoudi, Y., & Alamoudi, W. (2016). Cloud computing - the future of business. *Journal of Information Systems & Planning, 8*(19), 41-60. Retrieved from www.intellectbase.org/journals.php

Aleem, A., & Christopher, R. S. (2013). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime, 20*, 6-24. doi:10.1108/13590791311287337

Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. *International Journal of Information Management*, *37*(6), 639-649. doi:10.1016/j.ijinfomgt.2017.05.008

Ali, M., Bilal, K., Khan, S. U., Veeravalli, B., Li, K., & Zomaya, A. (2018). DROPS: Division and replication of data in cloud for optimal performance and security. *IEEE Transactions on Cloud Computing, 6*(2), 303-315. doi:10.1109/TCC.2015.2400460

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357-383. doi:10.1016/j.ins.2015.01.025

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, 5, 9-11. doi:10.1016/S1353-4858(18)30043-6

Ang, C. K., Embi, M. A., & Yunus, M. M. (2016). Enhancing the quality of the findings of a longitudinal case study: Reviewing trustworthiness via ATLAS. *The Qualitative Report*, *21(*10), 1855-1867. Retrieved from https://nsuworks.nova.edu

Annansingh, F., & Howell, K. (2016). Using phenomenological constructivism (PC) to discuss a mixed method approach in information systems research. *Electronic Journal of Business Research Methods, 14*(1), 39-49. Retrieved from http://www.ejbrm.com

Apolonia, N., Freitag, F., & Navarro, L. (2017). Leveraging deployment models on low-resource devices for cloud services in community networks. *Simulation Modelling Practice and Theory, 77*, 390-406. doi:10.1016/j.simpat.2016.06.008

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

Arki, O., Zitouni, A., & Dib, A. T. E. (2018). A multi-agent security framework for cloud data storage. *Multiagent & Grid Systems, 14*(4), 357–382. doi:10.3233/MGS-180296

Arora, H. D., & Dhiman, A. (2015). Comparative study of generalized quantitative-qualitative inaccuracy fuzzy measures for noiseless coding theorem and 1:1 codes. *International Journal of Mathematics & Mathematical Sciences*, *4*, 20151-20156. doi:10.1155/2015/258675

Artal, R., & Rubenfeld, S. (2017). Ethical issues in research. *Best Practice & Research Clinical Obstetrics & Gynaecology*, *43*, 107-114. doi:10.1016/j.bpobgyn.2016.12.006

Auger, M. D. (2016). Cultural continuity as a determinant of indigenous peoples' health: A metasynthesis of qualitative research in Canada and the United States. *International Indigenous Policy Journal, 7*(4), 1-24. doi:10.18584/iipj.2016.7.4.3

Avery, J., & Wallrabenstein, J. R. (2018). Formally modeling deceptive patches using a game-based approach *Computers & Security*, *75*, 182–190. doi:10.1016/j.cose.2018.02.009

Barnard, M. (2016). How to apply for research ethics committee approval. *Nursing Children and Young People, 28*(6), 16. doi:10.7748/ncyp.28.6.16.s20

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

Barrow, P., Kumari, R., & Manjula, R. (2016). Security in cloud computing for service delivery models: Challenges and solutions. *Journal of Engineering Research and Applications*, *6*(4), 76-85. Retrieved from http://www.ijera.com

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

Belmont Report (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* National Commission for the Protection

of Human Subjects of Biomedical and Behavioral Research. Retrieved from https://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, *15*(2), 219-234. doi:10.1177/1468794112468475

Bhatia, T., & Verma, A. K. (2017). Data security in mobile cloud computing paradigm: A survey, taxonomy and open research issues. *The Journal of Supercomputing, 73*(6), 2558-2631. doi:10.1007/s11227-016-1945-y

Bohnsack, R., & Pinkse, J. (2017). Value propositions for disruptive technologies: Reconfiguration tactics in the case of electric. *California Management Review*, *59*(4), 79-96. doi:10.1177/0008125617717711

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

Brew, A., Boud, D., Lucas, L., & Crawford, K. (2017). Responding to university policies and initiatives: The role of reflexivity in the mid-career academic. *Journal of Higher Education Policy and Management*, *39*(4), 378-389. doi:10.1080/1360080X.2017.1330819

Budzise-Weaver, T., Goodwin, S. P., & Maciel, M. L. (2015). Qualitative coded analysis of undergraduate and graduate student library instruction feedback. *Library Philosophy and Practice; Lincoln, 13*(1), 1-29. Retrieved from http://digitalcommons.unl.edu/libphilprac

Bugliesi, M., Calzavara, S., Focardi, R., & Khan, W. (2015). CookiExt: Patching the browser against session hijacking attacks. *Journal of Computer Security*, *23*(4), 509–537. doi:10.3233/JCS-150529

Burda, M., Van den Akker, M., Van der Horst, F., Lemmens, P., & Knottnerus, J. A. (2016). Collecting and validating experiential expertise is doable but poses methodological challenges. *Journal of Clinical Epidemiology; Elmsford*, *72*(1), 10-15. doi:10.1016/j.jclinepi.2015.10.021

Busse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, *20*(4), 574-609. doi:10.2139/ssrn.2713980

Caldarelli, A., Ferri, L., & Maffe, M. (2017). Expected benefits and perceived risks of cloud computing: An investigation within an Italian setting. *Technology Analysis & Strategic Management, 29*(2), 167–180. doi:10.1080/09537325.2016.1210786

Carter, N., Bryant-Lukosius, D. 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

Carvalho, C., Andrade, R., Castro, M., Coutinho, E. F., & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. *Computers and Electrical Engineering*, *50*, 141-152. doi:10.1016/j.compeleceng.2016.12.030

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811-830. Retrieved from https://nsuworks.nova.edu

Chen, C., Guo, R., & Zhang, J. (2016). The d-day, v-day, and bleak days of a disruptive technology: A new model for ex-ante evaluation of the timing of technology disruption. *European Journal of Operational Research*, *251*(2), 562-574. doi:10.1016/j.ejor.2015.11.023

Chennam, K. K., & Lakshmi, M. A. (2016). Cloud security in crypt database server using fine grained access control. *International Journal of Electrical and Computer Engineering, 6*(3), 915-924. doi:10.11591/ijece.v6i3.8925

Choong, P., Hutton, E., Richardson, P., & Rinaldo, V. (2016). Assessing the cost of security breach: A marketer's perspective. *Journal of Marketing Development and Competitiveness, 11*(1), 59-68. Retrieved from http://www.na-businesspress.com

Chowdhury, M. F. (2015). Coding, sorting and sifting of qualitative data analysis: Debates and discussion. *Quality & Quantity*, *49*(3), 1135-1143. doi:10.1007/s11135-014-0039

Christensen, C. M. (1997). *The innovators dilemma: When new technologies cause great firms to fail.* Boston, MA: Harvard Business School Press.

Christensen, C. M. (2006). The ongoing process of building a theory of disruption. *Journal of Product Innovation Management*, *23*(1), 39. doi:10.1111/j.1540-5885.2005.00180.x

Christensen, C. M. (2011). *The innovator's dilemma: The revolutionary book that will change the way you do Business.* New York, NY: HarperBusiness.

Christensen, C. M., & Raynor, M. (2003). *The innovator's solution.* Boston, MA: Harvard Business School Press.

Christensen, C. M., Raynor, M., & McDonald, R. (2015). What is disruptive innovation? *Harvard Business Review*, *93*(12)*, 44-53*. doi:10.1353/abr.2012.0147

Connelly, L. (2016). Understanding research. Trustworthiness in qualitative research. *MedSurg Nursing*, *25*(6), 435-436. Retrieved from http://www.medsurgnursing.net

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+A178:A179A178:A180

Crockett, D. R., McGee, J. E., & Payne, G. T. (2013). Employing new business divisions to exploit disruptive innovations: The interplay between characteristics of the corporation and those of the venture management team. *Journal of Product Innovation Management, 30*(5), 856–879. doi:10.1111/jpim.12034.

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons, 59*(6), 605-614. doi:1016/jbushor.2016.08.002

Dan, Y., & Chang Chieh, H. (2010). A reflective review of disruptive innovation theory. *International Journal of Management Reviews*, *12*, 435-452. doi:10.1111/j.1468-2370.2009.00272.x

Danneels, E. (2004). Disruptive technology reconsidered: A critique and research agenda. *Journal of Product Innovation Management*, *21*(4*),* 246-258. doi:10.1111/j.0737-6782.2004.00076.x

Davis, F. (1989). *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* Doctoral Dissertation, Sloan School of Management, M.I.T. Retrieved from https://www.researchgate.net

Davoll, B. (2017). Do you have what it takes to be a world-class DBA? *Database Trends & Applications, 31*(5), 9-10. Retrieved from https://www.dbta.com

Dayıoglu, Z. N., Kiraz, M. S., Birinci, F., & Akın, I. H. (2014). Secure database in cloud computing: CryptDB revisited. *International Journal of Information Security Science, 3*(1), 129-148. Retrieved from http://www.ijiss.org/ijiss/index.php/ijiss

de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). Pracis: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers & Security, 69*, 127-141. doi:10.1016/j.cose.2016.12.01

Demir, Y., Mutlu, G., & Şişman, Y. S. (2018). Exploring the oral communication strategies used by Turkish EFL learners: A mixed methods study. *International Journal of Instruction, 11*(2), 539-554. doi:10.0.50.173/iji.2018.11237

Deng, L., Yang, Z., Du, P., & Song, Y. (2018). A cloud platform for space science mission concurrent design. *Concurrent Engineering-Research and Applications*, *26*(1), 104-116. doi:10.1177/1063293X17724848

Dey, P., & Lehner, O. (2017). Registering ideology in the creation of social entrepreneurs: Intermediary organizations, 'ideal subject' and the promise of enjoyment. *Journal of Business Ethics: JBE, 142*(4), 753-767. doi:10.1007/s10551-016-3112-z

Dhasarathan, C., Thirumal, V., & Ponnurangam, D. (2015). Data privacy breach prevention framework for the cloud service. *Security & Communication Networks, 8*(6), 982–1005. doi:10.1002/sec.1054

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *The Qualitative Report*, *21*(3), 521-528. Retrieved from https://nsuworks.nova.edu

Ecker, J. (2017). A reflexive inquiry on the effect of place on research interviews conducted with homeless and vulnerably housed individual. *Forum: Qualitative Social Research*, *18*(1), n/a. doi:10.17169/fqs-18.1.2706

Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4. doi: 10.11648/j.ajtas.20160501.11

Fador, A. (2014). Innovation and technology acceptance model (TAM): A theoretical approach. *Romanian Journal of Marketing, 2*, 59-65. Retrieved from http://www.revistademarketing.ro

Fagerholm, F., Kuhrmann, M., & Münch, J. (2017). Guidelines for using empirical studies in software engineering education. *PeerJ Computer Science*, *3*(1), 131-166. doi:10.7717/peerj-cs.131

Feder, C. (2018). The effects of disruptive innovations on productivity. *Technological Forecasting & Social Change, 126*, 186-193. doi:10.1016/j.techfore.2017.05.009

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information

security governance and national culture. *Computers & Security*, *43*, 90-110. doi:10.1016/j.cose.2014.03.004

Foley, T., Boyle, S., Jennings, A., & Smithson, W. H. (2017). "We're certainly not in our comfort zone": A qualitative study of GPs dementia-care educational needs. *BMC Family Practice, 18*(1), 1-10. doi:10.1186/s12875-017-0639-8

Foresti, S., Paraboschi, S., Pelosi, G., & Samarati, P. (2018). Enforcing authorizations while protecting. *Journal of Computer Security*, *26*, 143–175. doi:10.3233/JCS-171004

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

Gale, S. F. (2018). Under lock and key. *PM Network, 32*(10), 54–61. Retrieved from https://pmi.org

Gantt, G., Jr. (2014). Hacking health care: Authentication security in the age of meaningful use. *Journal of Law and Health (Online), 27*(2), 232-258. Retrieved from https://engagedscholarship.csuohio.edu/jlh/

Garg, N., & Bawa, S. (2016). Comparative analysis of cloud data integrity auditing protocols. *Journal of Network & Computer Applications*, *66*, 17–32. doi:10.1016/j.jnca.2016.03.010

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, *20*(11), 1772. doi:10.4135/9781412950589.n885

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S.,… Jabbar, S. & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, *74*(10), 4986. doi:10.1007/s11227-018-2337-2

Ghazi, Y., Masood, R., Rauf, A., Shibli, M. A., & Hassan, O. (2016). DB-SECaaS: A cloud-based protection system for document-oriented no SQL databases. *Eurasip Journal on Information Security, 16*(1), 1-17. doi:10.1186/s13635-016-0040-5

Goldstein, E. R. (2015). The undoing of disruption: Clayton Christensen and his critics. *The Chronicle of Higher Education,* (5), 6-9. Retrieved from https://www.chronicleofhigherdeucation.com

Goodell, L., Stage, V., & Cooke, N. (2016). Practical qualitative research strategies: Training interviewers and coders. *Journal of Nutrition Education and Behavior*, *48*(6), 578-585. doi: 10.1016/j.jneb.2016.06.001

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research, 11*(4), 517-525. doi:10.1080/19361610.2016.1211876

Goyal, S. (2014). Public vs. private vs. hybrid vs. community - cloud computing: A critical review. *International Journal of Computer Network and Information Security*, *6*(3), 20-29. doi:10.5815/ijcnis.2014.03.03

Greengard, S. (2015). Why passwords are skeleton keys of the 21st century. *CIO Insight*, 2. Retrieved from https://www.cioinsight.com

Grieb, S. D., Eder, M. M., Smith, K. C., & Calhoun, K. T. D. (2015). Qualitative research and community-based participatory research: Considerations for effective

dissemination in the peer-reviewed literature. *Progress in Community Health Partnerships*, *9*(2), 275-282. doi:10.1353/cpr.2015.0041

Griffiths, T. L., Daniels, D., Austerweil, J. L., & Tenenbaum, J. B. (2018). Subjective randomness as statistical inference. *Cognitive Psychology*, *103*, 85-109. doi:10.1016/j.cogpsych.2018.02.003

Guttentag, D. (2015). Airbnb: disruptive innovation and the rise of an informal tourism accommodation sector. *Current Issues in Tourism*, *18*(12), 1192-1217. doi:10.1080/13683500.2013.827159

Haber, M. (2015). Protecting Data in the Cloud. *Risk Management*, *62*(10), 8–9. Retrieved from https://www.RIMS.org/

Hadavi, M., Jalili, R., Damiani, E., & Cimato, S. (2015). Security and searchability in secret sharing-based data outsourcing. *International Journal of Information Security, 14*(6), 513–529. doi:10.1007/s10207-015-0277-x

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction, 31*(3), 498-501. doi:10.1093/humrep/dev334

Han, Z., Yang, L., Wang, S., Mu, S., & Liu, Q. (2018). Efficient multifactor two-server authenticated scheme under mobile cloud computing. *Wireless Communications & Mobile Computing*, 1-14. doi:10.1155/2018/9149730

Hang, C. C., Garnsey, E., & Ruan, Y. (2015). Opportunities for disruption. *Technovation*, *39-40*(1), 83-93. doi:10.1016/j.technovation.2014.11.005

Hannaford, L. (2017). Motivation in group assessment: A phenomenological approach to post-graduate group assessment. *Assessment & Evaluation in Higher Education*, *42*(5), 823-836. doi:10.1080/02602938.2016.1195787

Hanson, L., Haas, M., Bronfort, G., Vavrek, D., Schulz, C., Leininger, B., … Neradilek, M. (2016). Dose-response of spinal manipulation for cervicogenic headache: study protocol for a randomized controlled trial. *Chiropractic & Manual Therapies*, *24*(1), 1-12. doi:10.1186/s12998-016-0105-z

Happel-Parkins, A., & Azim, K. A. (2017). She said, she said: Interruptive narratives of pregnancy and childbirth. *Forum: Qualitative Social Research*, *18*(2), 1-18. doi:10.17169/fqs-18.2.2718

Hashem, I., Yaqoob, I., Anuar, N., Mokhtar, S., Gani, A., & Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47*, 98-115. doi:10.1016/j.is.2014.07.006

He, L., Huang, F., Zhang, J., Liu, B., Chen, C., Zhang, Z., … Yang, Y., & Lu, W. (2016). Dynamic secure interconnection for security enhancement in cloud computing. *International Journal of Computers Communications & Control, 11*(3), 348-357. doi:10.15837/ijccc.2016.3.504

Heatherly, R. (2016). Privacy and security within biobanking: The role of information technology. *Journal of Law, Medicine & Ethics, 44*(1), 156-160. doi:10.1177/1073110516644206

Hege, I., Dietl, A., Kiesewetter, J., Schelling, J., & Kiesewetter, I. (2018). How to tell a patient's story? Influence of the case narrative design on the clinical reasoning

process in virtual patients. *Medical Teacher*, 1-7. doi:10.1080/0142159x.2018.1441985

Henry, C., & Foss, L. (2015). Case sensitive? A review of the literature on the use of case method in entrepreneurship research. *International Journal of Entrepreneurial Behaviour & Research*, *21*(3), 389-409. doi:10.1108/ijebr-03-2014-0054

Hesse-biber, S. (2016). Qualitative or mixed methods research inquiry approaches: Some loose guidelines for publishing in sex roles. *Sex Roles*, *74(*1), 6-9. doi:10.1007/s11199-015-0568-8

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: An example from practice. *Nurse Researcher, 22*(5), 8. doi:10.7748/nr.22.5.8.e1307

Hoyland, S., Hollund, J. G., & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education, 49*(2), 224-232. doi:10.1111/medu.12622

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work*, *4*(1), 1-12. Retrieved from https://journals.uis.no/index.php/JCSW

Ibrahim, N., & Edgley, A. (2015). Embedding researcher's reflexive accounts within the analysis of a semi-structured qualitative interview. *The Qualitative Report*, *20*(10), 1671-1681. Retrieved from https://nsuworks.nova.edu

Igbal, S., Kiah, S., Anuar, L. M., Daghighi, N. B., Wahid, B., Wahab, A., … Khan, S. (2016). Service delivery models of cloud computing: security issues and open

challenges. *International Journal of Applied Engineering Research, 9*(22), 4726-4750. doi:10.1002/sec.1585

Jaidi, F. (2019). A quantified trust-risk assessment approach for enhancing firewalls-filtering services. *Journal of Information Assurance & Security, 14*(2), 30–39. Retrieved from https://www.mirlabs.net/jias/index.html

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, *5*(4), 87. doi:10.4103/0976-0105.141942

Jathanna, R., & Jagli, D. (2015). Cloud computing and security issues. *International Journal of Engineering Research and Application, 7*(6), 31-38. Retrieved from https://www.ijera.com

Jho, N. S., Chang, K. Y., Hong, D., & Seo, C. (2016). Symmetric searchable encryption with efficient range query using multi-layered linked chains. *Journal of Supercomputing*, *72*(11), 4233–4246. doi:10.1007/s11227-015-1497-6

Jian, S., Dengzhi, L., Qi, L., Debiao, H., & Xingming, S. (2017). An enhanced cloud data storage auditing protocol providing strong security and efficiency for smart city. *Journal of Information Science & Engineering*, *33*(4), 923-938. doi:10.6688/JISE.2017.33.4

Jim, R. (2013). Multifactor authentication: Its time has come. *Technology Innovation Management Review,* 51-58. Retrieved from https://timreview.ca

Jin, J., Guo, X., Dutta, R. G., Bidmeshki, M. M., & Makris, Y. (2017). Data secrecy protection through information flow tracking in proof-carrying hardware IP - Part

I: Framework fundamentals. *IEEE Transactions on Information Forensics and Security, 12*(10), 2416-2429. doi:10.1109/TIFS.2017.2707323

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management, 34(*6), 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications, 111*, 120-141. doi:10.1016/j.comcom.2017.07.006

Kallio, H., Pietila, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72(12),* 2954-2965. doi:10.1111/jan.13031

Kaltenecker, N., Hess, T., & Huesig, S. (2015). Managing potentially disruptive innovations in software companies: Transforming from on-premises to the on-demand. *Journal of Strategic Information Systems*, *24,* 234-250. doi:10.1016/j.jsis.2015.08.006

Kim, S. Y., & Miller, F. G. (2015). Informed consent for pragmatic trials: the integrated consent Model. *The New England Journal of Medicine*, *370*(8), 769-772. doi:10.1056/nejmhle1312508

King, A. A., & Baatartogtokh, B. (2015). How useful is the theory of disruptive innovation? *MIT Sloan Management Review*, *57*(1), 77-90. doi:10.1017/CBO9781107415324.004

Kline, T. J. B. (2017). Sample issues, methodological implications, and best practices. *Canadian Journal of Behavioural Sciences, 49*(2), 71-77. doi:10.1037/cbs0000054

Kranz, J. J., Hanelt, A., & Kolbe, L. M. (2016). Understanding the influence of absorptive capacity and ambidexterity on the process of business model change – the case of on-premise and cloud-computing software. *Information Systems Journal*, *26*(5), 477-517. doi:10.1111/isj.12102

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology. *Journal of Parapsychology*, *79*(2), 219-233. Retrieved from https://www.parapsych.org

Kumar, M., & Vardhan, M. (2018). Data confidentiality and integrity preserving outsourcing algorithm for matrix chain multiplication over malicious cloud server. *Journal of Intelligent and Fuzzy Systems, 34*(3), 1251-1263. doi:10.3233/JIFS-169422

Kumaril, K., & Mrunalini, M. (2018). A survey on big data security: Issues, challenges and techniques. *International Journal of System and Software Engineering, 6*(2), 24-36. doi:10.29042/2018-3290-3293

Lankford, E. (2019). NIST cryptographic algorithm and module validation programs: validating new encryption schemes. *ISSA Journal, 17*(5), 37–40. Retrieved from https:// www.members.issa.org`

Larrinaga, O. V. (2017). Is it desirable, necessary and possible to perform research using case studies? *Cuadernos De Gestión*, *17*(1), 147-171. doi:10.5295/cdg.140516ov

Lepore, J. (2014). The disruption machine. *The New Yorker, 90*, 30–36. Retrieved from https://newyorker.com

Leung, 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

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*(4), 473-475. doi:10.1177/1524839915580941

Li, J., & Wang, J. (2019). Security storage of sensitive information in cloud computing data center. *International Journal of Performability Engineering*, *15*(3), 1023-1032. doi:10.23940/ijpe.19.03.p32.10231032

Li, J., Wang, Y., Liu, X., Xu, Y., & Cui, T. (2018). Academic adaptation among international students from East Asian countries: A consensual qualitative research. *Journal of International Students*, *194*(1), 2162-3104. doi:10.5281/zenodo.1134289

Liu, C., Yang, C., Zhang, X., & Chen, J. (2015). External integrity verification for outsourced big data in cloud and IoT: A big picture. *Future Generation Computer Systems, 49,* 58-67. doi:10.1016/j.future.2014.08.007

Lloyd, J., & Hopkins, P. (2015). Using interviews to research body size: Methodological and ethical considerations. *Area, 47*(3), 305-310. doi:10.1111/area.12199

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods, 14*(5), 1-8. doi:10.1177/1609406915621406

Lucas, S. R. (2014). Beyond the existence proof: Ontological conditions, epistemological implications, and in-depth interview research. *Quality & Quantity*, *48*(1), 387-408. doi:10.1007/s11135-012-9775-3

Madni, S. H. H., Latiff, M. S. A., Coulibaly, Y., & Abdulhamid, S. M. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities. *Journal of Network and Computer Applications, 68*, 173-200. doi:10.1016/j.jnca.2016.04.016

Mahtoa, R. V., Belousovab, O., & Ahluwalia, S. (2017). Abundance – A new window on how disruptive innovation occurs. *Technological Forecasting & Social Change,*1-8. doi:10.1016/j.techfore.2017.09.008

Maluf, D. A., Sudhaakar, R. S., & Choo, K. R. (2018). Trust errosion: Dealing with unknown-unknowns in cloud security. *IEEE Cloud Computing, 5*(4), 24-32. doi:10.1109/MCC.2018.043221011

Mansoori, M., Welchi, I., Choo, K. R., Maxion, R. A., & Hashemi, S. E. (2017). Real-world IP and network tracking measurement study of malicious websites with HAZOP. *International Journal of Computers and Applications, 39*(2), 106-121. doi:10.1080/1206212X.2017.1283910

Manvi, S. S., & Krishna, G. (2014). Resource management for infrastructure as a service (IaaS) in cloud computing: A survey. *Journal of Network and Computer Applications. 41*, 424-44. doi:10.1016/j.jnca.2013.10.004

Marion, T. J., Eddleston, K. A., Friar, J. H., & Deeds, D. (2015). The evolution of interorganizational relationships in emerging ventures: An ethnographic study within the new product development process. *Journal of Business Venturing*, *30*(1), 167-184. doi:10.1016/j.jbusvent.2014.07.003

Marks, L. D. (2015). A pragmatic, step-by-step guide for qualitative methods: Capturing the disaster and long-term recovery stories of Katrina and Rita. *Current Psychology: A Journal for Diverse Perspectives on Diverse Psychological Issues*, *34*(3), 494-505. doi:10.1007/s12144-015-9342-x

Mazel, J., Garnier, R., & Fakuda, K. (2019). A comparison of web privacy protection techniques. *Computer Communications, 144,* 1562-174. doi:10.1016/j.comcom.2019.04.005

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2*, 1-12. doi:10.1177/2333393615597674

McKendrick, J. (2015). Database administrators expanding their horizons. *Database Trends & Applications 29*(2), 1-3. Retrieved from http://www.dbta.com

McKendrick, J. (2018). Managing the hybrid future: From databases to clouds. *Database Trends & Applications, 32*(1), 12–14. Retrieved from http://www.dbta.com

McMurtry, J. (2012). Behind global system collapse: The life-blind structure of economic rationality. *Journal of Business Ethics*, *108*, 49-60. doi:10.1007/s10551-011-1086-4

Mell, P., & Grance, T. (2010). The NIST definition of cloud computing. *Communications of the ACM*, *53*(6), 1-2. Retrieved from https://cacm.acm.org

Miracle, V. A. (2016). The Belmont Report: The triple crown of research ethics. *Dimensions of Critical Care Nursing, 35*(4), 223-228. doi:10.1097/DCC.000000000000

Mjihil, O., Kim, D. S., & Haqiq, A. (2016). Security assessment framework for multi-tenant cloud with nested virtualization. *Journal of Information Assurance & Security*, *11*(5), 283–292. Retrieved from https://www.mirlabs.org/jias

Modi, C. N., & Acha, K. (2016). Virtualization layer security challenges and intrusion detection / prevention systems in cloud computing: A comprehensive review. *Journal of SuperComputing, 73*, 1192-1234. doi:10.1007/s11227-016-1805-9

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23-48. doi:10.26458/jedep.v7i1.571

Molina-Azorín, J. F., & López-Gamero, M. D. (2016). Mixed methods studies in environmental management research: Prevalence, purposes and designs. *Business Strategy and the Environment, 25*(2), 134-148. doi:10.1002/bse.1862

Moon, Y. J., Choi, M., & Armstrong, D. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean

governmental organizations. *International Journal of Information Management, 40*, 54-66. doi:10.1016/j.ijinfomgt.2018.01.001

Moore, J. E., Uka, S., Vogel, J. P., Timmings, C., Rashid, S., Gülmezoglu, M. A., & Straus, S. E. (2016). Navigating barriers: Two-year follow up on recommendations to improve the use of material health guidelines in Kosovo. *BMC Public Health*, *16*(1). 1-14. doi:10.1186/s12889-016-3641-5

Morar, P., Read, J., Arora, S., Hart, A., Warusavitarne, J., Green, J., … Faiz, O. (2015). Defining the optimal design of the inflammatory bowel disease multidisciplinary team: results from a multicentre qualitative expert-based study. *Frontline Gastroenterology*, *6*(4), 290-297. doi:10.1136/flgastro-2014-100549

Morse, J. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212-1222. doi:10.1177/1049732315588501

Moyano, F., Fernandez-Gago, C., & Lopez, J. (2013). A framework for enabling trust requirements in social cloud applications. *Requirements Engineering*, *18*, 321-341. doi:10.1007/s00766-013-0171-x

Nagy, D., Schuessler, J., & Dubinsky, A. (2016). Defining and identifying disruptive innovations. *Industrial Marketing Management, 57,* 119-126. *doi:*10.1016/j.indmarman.2015.11.017

Neumann, P. G. (2014). Risks and myths of cloud computing and cloud storage. *Communications of the ACM*, *57*(10), 25-27. doi:10.1145/2661049

Nigra, M., & Dimitrijevic, B. (2018). Is radical innovation in architecture crucial to sustainability? Lessons from three Scottish contemporary buildings. *Architectural Engineering and Design Management*, *14*(4), 272-291. doi:10.1080/17452007.2018.1465392

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34-35. doi:10.1136/eb-2015-102054

Noblin, A., Cortelyou-War, K., & Servan, R. M. (2015). Cloud computing and patient engagement. *Podiatry Management, 30*(2), 65-70. Retrieved from http://www.podiatry.com

Noguerol, L. O., & Branch, R. (2018). Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study. *Journal of Economic Development, Management, IT, Finance & Marketing*, *10*(2), 7–35. https://gsmi-ijgb.com

Oates, J. (2015). Use of Skype in interviews: The impact of the medium in a study of mental health nurses. *Nurse Researcher*. *22*(4), 13-17. doi:10.7748/nr.22.4.13.e1318

Olson, J. D., McAllister, C., Grinnell, L. D., Walters, K. G., & Appunn, F. (2016). Applying constant comparative method with multiple investigators and inter-coder reliability. *The Qualitative Report, 21*(1), 26-42. Retrieved from https://nsuworks.nova.edu

Onag, G. (2018). Palo Alto Networks make firewalls smarter. *ComputerWorld Hong Kong, 25*, 1-2. Retrieved from https://www.cw.com.hk

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

Orange, A. (2016). Encouraging reflexive practices in doctoral students through research journals. *The Qualitative Report, 21*(12), 2176-2190. Retrieved from https://nsuworks.nova.edu

Osiyevskyy, O., & Dewald, J. (2015). Explorative versus exploitative business model change: The cognitive antecedents of firm-level responses to disruptive innovation. *Strategic Entrepreneurship Journal, 9*(1), 58-78. doi:10.1002/sej.1192

Padgett, D., & Mulvey, M. S. (2007). Differentiation via technology: Strategic positioning of services following the introduction of disruptive technology. *Journal of Retailing*, *83*(4), 375-391. doi:10.1016/j.jretai.2007.03.010

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 and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544. doi:10.1007/s10488-013-0528-y

Paliszkiewicz, J. (2019). Information Security Policy Compliance: Leadership and Trust. *Journal of Computer Information Systems*, *59*(3), 211-217. doi:10.1080/08874417.2019.1571459

Parisha, P., Khanna, P., Sharma, P., & Rizvi, S. (2017). Hash function based data partitioning in cloud computing for secured cloud storage. *International Journal*

of Engineering Research and Applications, 7(7), 1-6. doi:10.9790/9622-0707100106

Parisha, P. K., Puneet, S., & Sheenu, R. (2017). Data partitioning technique in cloud: a survey on limitation and benefits. *International Journal of Engineering Research and Applications*, *7*(7), 1-6. doi:10.9790/9622-0707100106

Paulus, T., Woods, M., Atkins, D. P., & Macklin, R. (2017). The discourse of QDAS: Reporting practices of ATLAS.ti and NVivo users with implications for best practices. *International Journal of Social Research Methodology*, *20*(1), 35-47. doi:10.1080/13645579.2015.1102454

Pelin, Y., & Soner, Y. (2015). Theoretical Frameworks, Methods, and Procedures for Conducting Phenomenological Studies in Educational Settings. *Turkish Online Journal of Qualitative Inquiry*, *6*(1), 1-20. doi:10.17569/tojqi.59813

Pérez, L., Dos, S. P., & Cambra-Fierro, J. (2017). Taking advantage of disruptive innovation through changes in value networks: Insights from the space industry. *Supply Chain Management, 22*(2), 97-106. doi:10.1108/SCM-01-2017-0017

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. A consideration of two very different issues in the use of interviews to collect research data. *Nurse Researcher*, *22*(4), 6-7. doi:10.7748/nr.22.4.6.s2

Peticca-Harris, A., DeGama, N., & Elias, S. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*, *19*(3), 376–401. doi:10.1177/1094428116629218

Pfeiler, W. A., Buffington, M. L., Rao, S., & Sutters, J. (2017). Research is... results: From a national survey. *Art Education*, *70*(2), 8-15. doi:10.1080/00043125.2017.1274179

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management, 36*(4), 618-625. doi:10.1016/j.ijinfomgt.2016.03.005

Ramu, G. (2018). A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter. *Education and Information Technologies, 23*(5), 2213-2233. doi:10.1007/s10639-018-9713-7

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

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, 204-209. doi:10.1016/j.procs.2015.04.171

Rashid, M., Caine, V., & Goez, H. (2015). The encounters and challenges of ethnography as a methodology in health research. *International Journal of Qualitative Methods, 14*(5), 1-16. doi:10.1177/1609406915621421

Reich, J. A. (2015). Old methods and new technologies: Social media and shifts in power in qualitative research. *Ethnography*, *16*(4), 394-415. doi:10/1177/1466138114552949

Reid, S., & Mash, B. (2014). African primary care research: Qualitative interviewing in primary care. *African Journal of Primary Health Care & Family Medicine, 6*(1), 1-6. doi:10.4102/phcfm.v6i1.632

Reinhardt, R., & Gurtner, S. (2015). Differences between early adopters of disruptive and sustaining innovations. *Journal of Business Research*, *68*(1), 137-145. doi:10.1016/0148-2963(86)90041-x

Rizvi, S., Karpinski, K., Kelly, B., & Walker, T. (2015). Utilizing third party auditing to manage trust in the cloud. *Procedia Computer Science, 61*, 191-197. doi:10.1016/j.procs.2015.09.192

Rodik, P., & Primorac, J. (2015). To use or not to use: Computer-assisted qualitative data analysis software usage among early-career sociologists in Croatia. *Forum*: *Qualitative Social Research*, *16*(1), 1-21. Retrieved from http://www.qualitative-research.net

Rogers, E. M. (1962). *Diffusion of innovations*. New York, NY: Free Press.

Rogers, E. M. (2004). A prospective and retrospective look at the diffusion model. *Journal of Health Communication*, *9,* 13-19. doi:10.1080/10810730490271449

Rogers, O., & Cliff, D. (2012). A financial brokerage model for cloud computing. *Journal of Cloud Computing*, *1*, 2-12. doi:10.1186/2192-113X-1-2

Roy, K., Zvonkovic, A., Goldberg, A., Sharp, E., & LaRossa, R. (2015). Sampling richness and qualitative integrity: Challenges for research with families. *Journal of Marriage and Family*, *77*(1), 243-260. doi:10.1111/jomf.12147

Rubin, A., & Babbie, E. (2016). Empowerment series: *Research methods for social work* (9th ed.). Boston, MA: Cengage Learning.

Rubóczki, E. S., & Rajnai, Z. (2015). Moving towards cloud security. *Interdisciplinary Description of Complex Systems, 13*(1), 9-14. doi:10.7906/indecs.13.1.2

Safa, N. S., Solms, R. V., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud and Security, 2*, 15-18. doi:10.1016/S1361-3723(16)30017-3

Samarasinghe, N., & Mannan, M. (2019). Towards a global perspective on web tracking. *Computers & Security*, *87*, 1-13. doi:10.1016/j.cose.2019.101569

Sanjari, M., Bahramnezhad, F., Fomani, F., Shoghi, M., & Cheraghi, M. (2014). Ethical challenges of researchers in qualitative studies: the necessity to develop a specific guideline. *Journal of Medical Ethics & History of Medicine*, *7*(14), 1-6. doi:10.1177/0969733007086018

Schmidt, G. M., & Druehl, C. T. (2008). When is a disruptive innovation disruptive? *Journal of Product Innovation Management*, *24*(4), 347-369. doi:10.1111/j.1540-5885.2008.00306.x

Schniederjans, D. G., & Hales, D. N. (2016). Cloud computing and its impact on economic and environmental performance: A transaction cost economics perspective. *Decision Support Systems, 86*, 73-82. doi:10.1016/j.dss.2016.03.009

Shahzad, F. (2014). State-of-the-art survey on cloud computing security challenges, approaches, and solutions. *Procedia Computer Science*, *37*, 357-362. doi:10.1016/j.procs.2014.08.053

Shaikh, R., & Sasikumar, M. (2015). Data classification for achieving security in cloud computing. *Procedia Computer Science*, *45*, 493-498. doi:10.1016/j.procs.2015.03.087

Shana, Z. Z., & Abulibdeh, E. E. (2017). Cloud computing issues for higher education: Theory of acceptance model. *International Journal of Emerging Technologies in Learning*, *12*(11), 168-184. doi:10.3991/ijet.v12.i11.7473

Shao, Z., Yang, B., Zhang, W., Zhao, Y., Wu, Z., & Miao, M. (2015). Secure medical information sharing in cloud computing. *Technology and Health Care*, *23,* S133-S137. doi:10.3233/THC-150945

Sharma, Y., Javadi, B., Si, W., & Sun, D. (2016). Reliability and energy efficiency in cloud computing systems: Survey and taxonomy. *Journal of Network and Computer Applications, 74,* 66-85. doi:10.1016/j.jnca.2016.08.010

Shen, J., Liu, D., Liu, Q., He, D., & Sun, X. (2017). An enhanced cloud data storage auditing protocol providing strong security and efficiency for smart city indicated that storing data in cloud minimizes storage burden. *Journal of Information Science and Engineering, 33*(4), 923-938. doi:10.6688/JISE.2017.33.4.4

Silva, L., 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

Simon, M. (2019). Two-factor authentication: How to choose the right level of security for every account. *PC World, 7*(5), 91-98. Retrieved from https://www.pcworld.com

Simpson, W. R., & Foltz, K. E. (2017). Ports and Protocols Extended Control for Security. *IAENG International Journal of Computer Science, 44*(2), 72–85. Retrieved from http://www.iaeng.org/IJCS

Sims, L. (2016). Legal publishing: Establishing context through the lens of disruptive innovation. *Legal Reference Services Quarterly*, *35*(3), 195-213. doi:10.1080/0270319X.2016.1227203

Sindhu, R., & Mushtaque, M. (2014). A new innovation on user's level security for storage data in cloud computing. *International Journal of Grid & Distributed Computing*, *7*, 213-219. doi:10.14257/ijgdc.2014.7.3.22

Singh, A., & Chatterjee, K. (2017). Review: Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, 79*, 88-115. doi:10.1016/j.jnca.2016.11.027

Song, J., Li, T., Wang, Z., & Zhu, Z. (2013). Study on energy-consumption regularities of cloud computing systems by a novel evaluation model. *Computing Archives for Informatics and Numerical Computation, 95*, 269-287. doi:10.1007/s00607-012-0218-8

Soni, A., & Hasan, M. (2017). Pricing schemes in cloud computing: A review. *International Journal of Advanced Computer Research, 7*(29), 60-70. doi:10.19101/ IJACR.2017.729001

Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S. U., Buyya, R., … & Zomaya, A. Y. (2015). Remote data auditing in cloud computing environments: A

survey, taxonomy, and open issues. *ACM Computing Surveys, 47*(4), 1-34. doi:10.1145/2764465

Sookhak, M., Yu, R. F., & Zomaya, A. Y. (2018). Auditing big data storage in cloud computing using divide and conquer tables. *IEEE Transactions on Parallel and Distributed Systems, 29*(5), 999-1012. doi:10.1109/TPDS.2017.2784423

Spillane, A., Larkin, C., Corcoran, P., Matvienko-Sikar, K., & Arensman, E. (2017). What are the physical and psychological health effects of suicide bereavement on family members? Protocol for an observational and interview mixed-methods study in Ireland. *BMJ Open*, *7*(3), 1-8. doi:10.1136/bmjopen-2016-014707

Srivastava, H., & Kumar, S. A. (2015). Control framework for secure cloud computing. *Journal of Information Security*, *6*, 12-23. doi:10.4236/jis.2015.61002

Srivastava, R. (2017). Assessment of cloud computing security risks for E-governance infrastructure. *Journal of Network and Information Security*, *5*(2), 1-8. Retrieved from http://www.publishingindia.com/jnis

Stewart, H., & Gapp, R. (2017). Exploring the alchemy of qualitative management research: seeking trustworthiness, credibility, and rigor through crystallization. *The Qualitative Report*, *22*(1), 1-19. Retrieved from https://nsuworks.nova.edu

Stockman, C. (2015). Achieving a doctorate through mixed methods research. *The Electronic Journal of Business Research Methods*, *13*(2), 74-84. Retrieved from http://www.ejbrm.com

Streitfeld, D. (2014). Even early adopters see major flaws in the cloud. The New York Times, F8. Retrieved from http://www.nytimes.com

Subha, T., & Jayashri, S. (2017). Public auditing scheme for data storage security in cloud computing. *Journal of Information Science & Engineering*, *33*(3), 773–787. doi: 10.6688/JISE.2017.33.3.11

Sudha, M. (2015). Efficiency of security privacy in cloud computing. *International Journal of Advanced Research in Computer Science, 6*(8), 21-28. Retrieved from http://www.ijarcs.info

Sultan, N. (2015). Reflective thoughts on the potential and challenges on wearable technology for healthcare provision and medical education. *International Journal of Information Management, 35*, 521-526. doi:10.1016/j.ijinfomgt.2015.04.010

Supriya, M., Sangeeta, K., & Patra, G. K. (2016). Trustworthy cloud service provider selection using multi-criteria decision-making methods. *Engineering Letters*, *24*(1), 1-10. Retrieved from http://www.engineeringletters.com

Surya, K., Mathew, S. K., & Lehner, F. (2014). Innovation and the cloud: A review of literature. *CMIT 2014 - 2014 IEEE International Conference on Management of Innovation and Technology,* 193-198. doi:10.1109/ICMIT.2014.6942424

Takahashi, N., Shintaku, J., & Ohkawa, H. (2013). Is technological trajectory disruptive? *Annals of Business Administrative Science*, *12*(1), 1-12. doi:10.7880/abas.12.1

Tankard, C. (2015). The security issues of the Internet of things. *Computer Fraud and Security,* 1, 11-14. doi:10.1016/S1361-3723(15)30084-1

Tankard, C. (2017). Encryption as the cornerstone of big data security. *Network Security,* (3), 5-7. doi:10.1016/S1353-4858(17)30025-9

Taylor, J. (2017). Going public: Using the cloud to improve project delivery. *Information Systems Management, 34*(2), 105-116. doi:10.1080/10580530.2017.1288521

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36*, 1-9. doi:10.1016/j.jocs.2016.11.011

Tellis, G. J. (2006). Disruptive technology or visionary leadership? *Journal of Product Innovation Management, 23*, 34–38. doi:10.1111/j.1540-5885.2005.00179.x

Than, K., Tin, K. N., La, T., Thant, K. S., Myint, T., Beeson, J. G., ... Morgan, A. (2018). The potential of task shifting selected maternal interventions to auxiliary midwives in Myanmar: A mixed-method study. *BMC Public Health*, *18*(1), 1-10. doi: 10.1186/s12889-017-5020-2

Thomas, D. R. (2017). Feedback from research participants: are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*(1), 23-41, doi:10.1080/14780887.2016.1219435

Tian, H., Nan, F., Chang, C. C., Huang, Y., Lu, J., & Du, Y. (2019). Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. *Journal of Network and Computer Applications, 127*, 59-69. doi:10.1016/j.jnca.2018.12.004

Tinkler, L., Smith, V., Yiannakou, Y., & Robinson, L. (2018). Professional identity and the clinical research nurse: A qualitative study exploring issues having an impact on participant recruitment in research. *Journal of Advanced Nursing*, *74*(2), 318-328. doi:10.1111/jan.13409

Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward proper authentication methods in electronic medical record access compliant to HIPAA and C . I .A . *Triangle, 1996*, 1–9. doi:10.1007/s10916-016-0465-x

Togan, M. (2015). Aspects of security standards for cloud computing. *MTA Review, 25*(1), 31-44. Retrieved from https://www.worldcat.org/title/mta-review/oclc/882231145

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers and Education*, *106*, A1-A9. doi:10.1016/j.compedu.2016.12.002

Vecchiato, R. (2017). Disruptive innovation, managerial cognition, technology competition outcomes. *Technology Forecasting and Social Change*, *116*, 116-128. doi:10.1016/j.techfore.2016.10.068

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*, 186–204. doi:10.1287/mnsc.46.2.186.11926

Vicary, S., Young, A., & Hicks, S. (2017). A reflective journal as learning process and contribution to quality and validity in interpretative phenomenological analysis. *Qualitative Social Work*, *16*(4), 550-565. doi:10.1177/1473325016635244

Wang, C., Ding, K., Li, B., Zhao, Y., Xu, G., Guo, Y., … & Wang, P. (2018). An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment. *Wireless Communications & Mobile Computin*g, 1–13. doi:10.1155/2018/3048697

Wang, C., & Geale, S. (2015). The power of story: Narrative inquiry as a methodology in nursing research. *International Journal of Nursing Sciences, 2*(2), 195-198. doi:10.1016/j.ijnss.2015.04.014

Wang, R. (2017). Research on data security technology based on cloud storage. *Procedia Engineering, 174*, 1340-1355. doi:10.1016/j.proeng.2017.01.286

Watkins, D. C. (2017). Rapid and rigorous qualitative data analysis: The "RADaR" technique for applied research. *International Journal of Qualitative Method*s, *16*(1), 1-9. doi:10.1177/1609406917712131

Watts, S. (2015). Five seconds to protect your business. *Computer Fraud and Security, 9*, 18-19. doi:10.1016/S1361-3723(15)30086-5

Weeks, M. R. (2015). Is disruption theory wearing new clothes or just naked? Analyzing recent critiques of disruptive innovation theory. *Innovation: Management, Policy & Practice*, *17*(4), 417-428. doi:10.1080/14479338.2015.1061896

Wei, F., Jiang, Q., Zhang, R., & Ma, C. (2017). A Privacy-preserving multi-factor authenticated key exchange protocol with provable security for cloud computing. *Journal of Information Science & Engineering*, *33*(4), 907–921. doi:10.6688/JISE.2017.33.4.3

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624. doi:10.1016/j.bushor.2015.06.005

Werfs, M., Baxter, G., Allison, I. K., & Sommerville, I. (2013). Migrating software products to the cloud: An adaptive STS perspective. *Journal of International*

Technology and Information Management, 22(3), 37-54. Retrieved from https://iima.org

Xiang, S., & Zhu, Z. (2019). Dynamic access control of encrypted data in cloud computing environment. *International Journal of Performability Engineering, 15*(3), 969-976. doi:10.23940/ijpe.19.03.p26.969976

Xu, Z., Wu, L., Khurram, M., Choo, K. R., & He, D. (2017). A secure and efficient public auditing scheme using RSA algorithm for cloud storage. *Journal of SuperComputing, 73*, 5285–5309. doi:10.1007/s11227-017-2085-8

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology, 88*(2), 225-231. Retrieved from https://www.asrt.org

Ye, K., & Ng, M. (2019). Intelligent encryption algorithm for cloud computing user behavior featured data. *Journal of Intelligent & Fuzzy Systems, 35*, 4309-4317. doi:103233/JIFS-169751

Yesilyurt, M., & Yalman, Y. (2016). New approach for ensuring cloud computing security: Using data hiding methods. *Sādhanā, 41*(11), 1289-1298. doi:10.1007/s12046-016-0558-8

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., … Mukherjee, N. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*(1), 10-19. doi:10.1111/2041-210x.12828

Yu, Y., Cao, R. Q., & Schniederjans, D. (2017). Cloud computing and its impact on service level: A multi-agent simulation model. *International Journal of Production Research*, *55*(15), 4341-4353. doi:10.1080/00207543.2016.1251624

Yuvaj, M. (2015). Cloud computing software and solutions for libraries: a comparative study. *Journal of Electronic Resources in Medical Libraries*, *12*(1), 25-41. doi:10.1080/15424065.2014.1003479

Zamawe, F. (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

Zhang, Q., Yang, L. T., & Chen, Z. (2016). Privacy preserving deep computation model on cloud for big data feature learning. *IEEE Transactions on Computers, 65*(5), 1351-1362. doi:10.1109/TC.2015.2470255

Zhang, W., Wulan, G., Zhai, J., Xu, L., Zhao, D., Liu, X., … Zhou, J. (2018). An intelligent power distribution service architecture using cloud computing and deep learning techniques. *Journal of Network and Computer Applications*, *103,* 239-248. doi:10.1016/j.jnca.2017.09.001

Zhou, J., Sun, L., Song, M., & Song, J. (2017). Anonymous limited-use-proof entity authentication protocol. *Wireless Personal Communications, 96*(1), 1065–1082. doi:10.1007/s11277-017-4221-4

Zia, M., & Ali, R. (2018). Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls. *PLoS ONE, 13*(12), 1–11. doi:10.1371/journal.pone.0208857

Zissis, D., & Lekkas, D. (2012). *Future Generation Computer Systems, 28*(3), 583-592. doi 10.1016/j.future.2010.12.006

Appendix A: E-mail Granting Permission to Use Table

Request to receive permission to use the table in the article "Opportunities for disruption".

From: Elizabeth Garnsey <ewg11@hermes.cam.ac.uk> on behalf of Elizabeth Garnsey <e.garnsey@eng.cam.ac.uk>

Sent: Friday, October 5, 2018 12:09:06 PM

To: Alberta Sannie-Ariyibi

Subject: Re: Request to receive permission to use the table in the article "Opportunities for disruption".

Dear Alberta,

You may use an adapted table from this article in your doctoral research.

I wish you good progress.

Regards

Elizabeth

On 4 Oct 2018, at 22:39, Alberta Pratt-Sensie <[e-mail address redacted]

wrote:

Good Day Authors,

My name is Alberta Pratt-Sensie, and I am a doctoral student at Walden University in the United States of America. I am currently writing my Proposal and I would like to use a table in your article:

"Hang, C. C., Garnsey, E., & Ruan, Y. (2015). Opportunities for disruption. Technovation, 39-40(1), 83-93. doi:10.1016/j.technovation.2014.11.005".

I am kindly requesting permission from you to adapt this table in my doctoral study. Please let me know if it is acceptable to you. Thank you so much.

Sincerely,

Alberta Pratt-Sensie

Appendix B: Participant Letter of Invitation

Date: May 23, 2019

Dear Potential Research Participant,

My name is Alberta Sannie-Ariyibi. I am currently a doctoral student at Walden University. I wish to request your participation in my doctoral research study entitled "***Security Strategies to Prevent Data Breaches in IaaS Cloud Computing*.".** The data I will collect from this study will be used to identify strategies database administrators use to prevent data breaches in IaaS cloud computing. As the sole researcher for this study, I will be interviewing participants who have knowledge and experience on strategies used to prevent data breaches in IaaS cloud computing. The purpose of this e-mail is to inform you about the details regarding voluntary participation in my research study, as well as your rights to make an informed decision whether to participate in this study or to refuse to participate.

Participation in this study is completely voluntary. If you agree to participate, you have the right to refuse to answer any questions that make you feel uncomfortable or refuse participation in the study at any phase of this research study, as well as completely withdraw all or part of the information already provided even after the completion of data collection without any prejudice or consequence. There will be no payment for participation in this study. I truly appreciate your time and effort in willingly participating in this study. Attached is a copy of the business letter of invitation for the head of your organization.

Sincerely,

Alberta Pratt-Sensie
[e-mail address redacted]

Appendix C: Business Letter of Invitation

Alberta A. Pratt-Sensie
Doctoral Candidate at Walden University
[e-mail address redacted]

Date: May 23, 2019

To: Business Manager

Dear Sir or Madam,

My name is Alberta A. Sannie-Ariyibi. I am a doctoral candidate at Walden University and I am working to fulfill my doctoral requirements in the Doctor of Information Technology program. My doctoral study is entitled ***Security Strategies to Prevent Data Breaches in IaaS Cloud Computing***. The purpose of my doctoral study is to explore the strategies database administrators use to secure data in private Infrastructure as a Service (IaaS) cloud computing.

Your company was selected as a potential participant in this study based on your professional role and expertise in computer technology and implementing cloud computing. The study will require that I meet with some of your employees who are 28 years or older with an IT work experience of five years or more and three years of cloud computing experience as related to data security in cloud computing. I will also collect nonproprietary information regarding security strategies and processes used by your organization.

The data collected from the potential participants will be kept confidential, and their identity will be protected. All published data from this study will maintain the privacy of the participants and the organization to protect the identity of both the participants and the organization. Minor risks will be associated with this study such as interruption of daily routine work activities, which will include taking time away from work to attend an interview. Participation in this study is voluntary and will not pose any risk to the participant's well-being or safety. Participants may choose to withdraw from this study at any time without retaliation or penalty. Consent to participate in this study will be beneficial to social change because the participant's personal information will be protected and prevent their personal information from being compromised.

Please consider participating in this study and respond to me via email at [redacted] or by returning it via e-mail as an electronic consent.

Thank you very much for your consideration and time!

Sincerely,

Alberta A. Pratt-Sensie
Walden University
Doctoral Candidate

Appendix D: Interview Protocol

A. Thank you for your willingness to participate in the interview process for my doctoral research study. My name is Alberta Sannie-Ariyibi, a doctoral student at Walden University, conducting a study on the Security Strategies Database Administrators use to prevent data breaches in IaaS cloud computing.
B. Participants will be given the consent form to read and review and ask any questions they may have prior to signing the consent form.
C. A copy of the signed consent form will be provided to the participants for their records.
D. Participation in the study will be completely voluntary
E. With the permission of the participant, the audio recorder will be switched on noting the date, time, and location of the interview.
F. The confidentiality and privacy of each participant will be maintained by omitting the name of the participant and the organization from the transcript, as well as any published data findings from the study.
G. The interview will last for 30-60 minutes allowing the participants to respond to 10 questions.
H. Follow-up questions may result from the initial questions to get more in-depth details
I. At the end of the interview, the participants will be thanked for participating in the interview process

J. Participants will be informed that I will contact them in one -two weeks for a follow-up member checking meeting that will last approximately 15 minutes to share the interview transcript with them for their feedback and comments

Semistructured Interview Questions

The following are the interview questions that for my research study.

1. What is your IT background such as education, work experience, etc.?
2. What do you currently know about database breaches and security measures?
3. Have you ever used security measures to prevent database breaches in cloud computing? If so how was this done?
4. How does your existing organization use security measures to prevent data breaches?
5. What solutions does your organization provide with regards to preventing data breaches?
6. What security measures does your organization have in place that were effective in preventing cloud computing data security breaches?
7. If your organization does not have a standard protocol for preventing data security breaches, have you implemented security breaches to prevent cloud computing data security breaches in your organization?
8. What were the least effective security measures used in preventing cloud computing data breaches?

9. With your experience as an IT professional, what obstacles does your organization face with regards to implementing cloud computing security measures, and how was this done?
10. In terms of cloud computing, what are your concerns in implementing security measures, and has the organization done to rectify these concerns?