2020

Strategies Administrators Use to Mitigate Cloud Computing Data Threats and Breaches

Wanda Cotton
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Wanda F. Cotton

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. Diane Dusick, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Jaime Klein, Committee Member, Doctor of Business Administration Faculty

Dr. Judith Blando, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2020

Abstract

Strategies Administrators Use to Mitigate Cloud Computing Data Threats and Breaches

by

Wanda F. Cotton

MS, University of Phoenix, 2008

BS, Saint Augustine's University, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2020

Abstract

Cloud computing has changed the information technology (IT) infrastructure of U. S. organizations, generating new threats and breaches in data security. Organization leaders estimated the costs from data breaches at approximately $8.5 billion annually, so reducing data breaches can potentially save organizations billions annually. Grounded in the integrated enterprise risk management framework, the purpose of this qualitative multiple case study was to explore strategies 4 IT administrators in central North Carolina use to mitigate data security threats and breaches. Data collection included archival documents (e.g., data security plans and organization newsletters), journal notes, and semistructured face-to-face interviews. Using thematic analysis and Yin's 5 phases of analysis led to three core themes: reliance on third-party risk management services, employee education, and best practices. A key recommendation is that IT administrators and organization leaders collaborate to align IT functions with organizational objectives to sustain competitive advantage. Applying the findings in this study may help IT administrators develop best practices to mitigate data security threats and breaches in cloud computing environments. The implications for positive social change include the potential to reduce occurrences of data and identity theft, the financial risk for organizations, and financial loss for individuals and community members.

Strategies Administrators Use to Mitigate Cloud Computing Data Threats and Breaches

by

Wanda F. Cotton

MS, University of Phoenix, 2008

BS, Saint Augustine's University, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2020

Acknowledgments

All praise, glory, and honor belong to the Father, Son, and Holy Ghost for leading and sustaining me throughout this doctoral journey. I never would have made it without God's consistent guidance and unconditional love. Thanks to my children, Montrell and Shatisa, for supporting me.Thank you to everyone who prepared countless dinners as I burned the midnight oil (e.g., John Oliver, Diane Goode, and Pam Palmer). To the Newbills for providing room and board during my residency, thank you for your genuine acts of kindness. Dr. Dusick, Dr. Klein, and Dr. Blando, thank you for supporting me and for sharing your academic wisdom. Dr. Dusick, you continually encouraged me to approach the doctoral process one day at a time, which made this journey very doable. Thank you Jill Kapszak for your unwaivering support and encouragement.

Finally, to my mom, whom I endearingly refer to as Ms. Wilkerson, if I had 10 thousand tongues, I could not thank you enough for the love you have shown me throughout this journey. I can only hope to be one iota of the lady you are. You are undoubtedly the classiest, wisest, and most unselfish lady I know. Ms. Wilkerson, you are the epitome of everything lovely in this world. I have watched you overcome insurmountable odds that would have caused the average person to throw in the towel. However, you never complained, and you always managed to look beyond your circumstances and find words of encouragement for me. Please know that you inspire me, and I am proud of you. I am so proud to be your daughter. I love you dearly, Ms. Wilkerson.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

On a global level, many organization leaders are discovering ways to streamline business processes by implementing information technology (IT) systems (Caniëls, Lenaerts, & Gelderman, 2015). By using these systems, organization leaders can (a) expand business operations; (b) create business value; and (c) establish, recover, and maintain customer and stakeholder relationships (Caniëls et al., 2015). Although organization leaders have invested significant amounts of money to acquire and update IT resources (Mithas & Rust, 2016), many IT administrators find it challenging to use these resources to alleviate data security vulnerabilities (Chen, Lin, & Chuang, 2016; Mithas & Rust, 2016). As the frequency of data breaches increases, organization leaders must train IT administrators to implement effective safety solutions to reduce data security risks.

Background of the Problem

Improving data security and reducing data threats and breaches are significant concerns for organization leaders. IT administrators are essential to protect sensitive data of organizations (Reece & Stahl, 2014). IT administrators emphasize preventing internal network threats, which are usually caused by disgruntled employees and human error (DeSouza & Valverde, 2016), rather than identifying and preventing external risks caused by unauthorized users (Reece & Stahl, 2014). Although minimizing internal data breaches is increasingly important (DeSouza & Valverde, 2016), organization leaders must allocate equal funding to train IT administrators to identify signs of data security compromise (Rid & Buchanan, 2015) and protect sensitive data from external threats (Reece & Stahl, 2014). The increased reliance on innovative technology to sustain

competitive advantage requires IT administrators to have the expertise to develop strategies to address increasingly complex cyberattacks.

Unauthorized users rely on advances in technology to gain illegal access to confidential data. In 2016, the average cost to U.S. organizations for a single data breach incident was approximately $200,000, and the total yearly cost was $8.5 billion (Romanosky, 2016). Data security is a complex process, and organization leaders require IT administrators to implement strategies to securely store, distribute, and access confidential data (Singh & Teng, 2015).

IT professionals use data management systems, such as cloud computing, to fulfill organization leaders' and consumers' demands for online access to acquire, store, and distribute data (Colesca, 2015). Because cloud computing vendors manage users' data off-site, concerns such as (a) privacy, (b) identity theft, (c) authentication, and (d) data access rank among the top user concerns. Despite the increasing interest in data security breaches, few researchers have explored how data security professionals in the IT industry minimize data compromises in their respective organizations (DeSouza & Valverde, 2016). The objective of this qualitative multiple case study was to explore strategies IT administrators use to mitigate data security threats and breaches in technology organizations.

Problem Statement

Cloud computing has changed the IT infrastructure of U.S. organizations, generating new threats and breaches in data security (Kumar, Raj, & Jelciana, 2018; Nazim & Ashgher, 2015). Economists estimated the total costs from data security

breaches at approximately $8.5 billion yearly (Romanosky, 2016). The general business problem was that losses resulting from data security breaches put organizations at financial risk. The specific business problem was that some IT administrators lack strategies to address data security threats and breaches in cloud computing.

Purpose Statement

The purpose of this multiple case study was to explore strategies IT administrators use to mitigate data security threats and breaches in cloud computing. The target population was IT administrators at three IT organizations with 1,000 to 3,000 employees in central North Carolina who had successfully implemented such strategies. One implication for social change derived from implementing strategies to reduce the effects of data threats and breaches on individuals and communities to improve the views of data security before and after a crisis occurs.

Nature of the Study

Researchers select a research design that relates to the intent of their study. Qualitative researchers seek to understand how a small group of selected participants interpret and make sense of their lived experiences in their natural environments (Katz, Saadon-Grosmana, & Arzya, 2017). Quantitative researchers examine data to (a) evaluate error rates, (b) establish the statistical reliability and validity of findings, and (c) provide numerical conclusions (Claydon, 2015). I did not use a mixed-methods approach because researchers use the method to collect and analyze both quantitative and qualitative data (see Palinkas et al., 2015). I did not incorporate quantitative data in this study. Because a qualitative method requires researchers to explore a phenomenon in more depth than that

provided by quantitative analysis (Cronin, 2014), a qualitative method was more suitable for this study.

I considered the phenomenological design, which researchers use to examine individuals' emotional and social experiences (Zlatev, 2016), but that was not the intent of this study. I also considered the ethnographic design, which researchers use to examine participants' experiences with social and cultural phenomena (Rapport, Clement, Doel, & Hutchings, 2015). The ethnographic design was not suitable for this study because exploring participants' experiences with social and cultural events was not the intent of this study. Researchers use the narrative inquiry design to explore phenomena from psychological, historic, and cultural viewpoints (Walsh et al., 2015; Wang & Geale, 2015), which was not the intent of this study.

The multiple case study design entails researchers implementing various data collection techniques to investigate a particular phenomenon with participants at various research sites (Cronin, 2014). The multiple case study design was suitable for this study because researchers use the design to replicate findings and explore variations within data between cases (Yin, 2015). Researchers also use the multiple case study design to evaluate program or workplace strategies (Yin, 2015), which was the intent of this study.

Research Question

The central research question for this study was the following: What strategies do IT administrators use to mitigate data security threats and breaches in cloud computing?

Interview Questions

I used the following questions in semistructured interviews to answer the research question:

1. What strategies have you used to identify data security risks in cloud computing?
2. What strategies have you used to assess IT systems for data security vulnerabilities in cloud computing?
3. What strategies have you used to respond to potential and realized data security threats and breaches in cloud computing?
4. What strategies have you found work best to mitigate data security risks in cloud computing?
5. What types of crises communication strategies have you used to communicate with authorized users to mitigate data security threats and breaches in cloud computing?
6. What strategies have you used to align business objectives with IT security functions to mitigate data security threats and breaches in cloud computing?
7. What strategies have you used to recover from careless data security threats and breaches in cloud computing in the past?
8. What else would you like to share regarding strategies you have used to mitigate data threats and breaches in cloud computing?

Conceptual Framework

A conceptual framework provides insight for (a) constructing qualitative research

questions, (b) outlining the proposal, and (c) aligning the study (Green, 2014). The underlying conceptual framework for this study was the Committee of Sponsoring Organizations of the Treadway Commission's (COSO, 2004) integrated enterprise risk management (ERM) framework. COSO consists of a group of administrators from five private institutions who develop regulations and frameworks pertaining to ERM, internal control, and fraud prevention (COSO, 2013).

The integrated ERM framework comprises eight integrated constructs: (a) internal environment, (b) objective setting, (c) event identification, (d) risk assessment, (e) risk response, (f) control activities, (g) information and communication, and (h) monitoring. COSO (2004) developed the integrated ERM framework to help IT professionals manage enterprise risks associated with data security. Applying the ERM framework could help IT administrators (a) assess risk to develop and improve risk response resolutions, and (b) establish strategies to identify and control activities that cause vulnerabilities in security systems. Because of the continued incidence of data security failure in organizations, implementing the ERM framework could educate organization leaders regarding the significance of IT administrators and organization leaders collaborating to enhance performance and sustainability. Gordon (2016) posited that ERM includes assessing and aligning business functions with IT functions to mitigate risks, which decreases the probability of interruptions in business continuity.

Operational Definitions

Data security: Data security entails applying digital safety mechanisms to prevent unauthorized users from accessing and corrupting IT infrastructures, databases, and Internet domains (Saidani, Shibani, & Alawadi, 2013).

Data security breach: Data security breaches occur when unauthorized users successfully compromise data by illegally (a) inspecting, (b) accessing, (c) stealing, or (d) distributing confidential data (Saidani et al., 2013). Some forms of data breach incidents may include medical records, personal identification numbers, and confidential employment or academic data (Saidani et al., 2013).

Data security threat: Data security threats are incidents caused by attackers who could pose harm by compromising confidential data (Balasubramanian & Mala, 2015).

Information technology administrator: Information technology administrators include chief information officers, chief information security officers, chief security officers, and information technology directors and managers (Hooper & McKissack, 2016).

Infrastructure as a service (IaaS): IT software vendors use IaaS programs to provide on-demand management systems so that consumers can access, monitor, and manage their IT infrastructures from remote sites (Lal & Bharadwaj, 2016).

Multitenant: Multitenant refers to multiple clients in various organizations sharing third-party cloud computing software services on a domain hosted by third-party vendors (Kabbedijk, Bezemer, Jansen, & Zaidman, 2015).

Platform as a service (PaaS): IT software vendors use PaaS programs to develop

the life cycle of software through development, testing, and distribution in centralized off-site or on-site locations (Lal & Bharadwaj, 2016).

Software as a service (SaaS): IT software vendors use SaaS programs to maintain data storage, networking, and server performance off-site (Lal & Bharadwaj, 2016).

Vulnerability: Vulnerability refers to any application, strategy, or design failure wherein unauthorized users (a) incite system malfunctions, (b) access confidential data, or (c) gain extended access to confidential data. Unlike threats, which are speculative, vulnerabilities occur, and the actions lead to unauthorized users successfully mishandling confidential data (Balasubramanian & Mala, 2015).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are researchers' unsubstantiated assessments regarding a phenomenon; if assumptions are omitted from the research, the study would be irrelevant (Gardner & Johnson, 2015; Gioia, Corley, & Hamilton, 2013). I assumed that participants would provide honest answers regarding data security failure. I also assumed that participants would have sufficient knowledge to answer the interview questions. Another assumption was the collected data would provide sufficient insight to answer the research question.

Limitations

Limitations are probable weaknesses in a study (Gioia et al., 2013; Marshall & Rossman, 2016). Limitations may also limit the scope of the findings in the study (Marshall & Rossman, 2016). One limitation of the study was the results were limited by

participants' knowledge of the subject. Another limitation was the study findings were limited by the honesty and candor of participants' responses. The third limitation was that participants' responses were limited to IT administrators at IT organizations in central North Carolina.

Delimitations

Delimitations are the parameters researchers implement to define the scope and boundaries of the study (Leedy & Ormrod, 2015). I delimited the study to strategies IT administrators use to mitigate data security threats and breaches in cloud computing. I also delimited the study to IT administrators with at least 3 years of experience successfully mitigating data threats and breaches. Finally, I delimited the cases to IT organizations in central North Carolina with 1,000 to 3,000 employees.

Significance of the Study

Organizations increasingly experience data security threats that challenge business sustainability. Integrating new technology such as cloud computing to streamline business operations presents opportunities and risks (Hussein & Khalid, 2016). This study was significant because the findings may be a resource to help close the knowledge gap for IT administrators regarding best practices for managing and mitigating data security threats and breaches in cloud computing environments.

Contribution to Business Practice

Data security is a major concern for IT professionals in all business sectors (Wamba, Akter, Edwards, Chopin, & Gnanzou, 2015). The findings in this study may facilitate organization leaders providing data security professionals with the requisite

training to (a) identify, (b) assess, and (c) respond to data vulnerabilities to maintain business operations before, during, and after data attacks. Organization leaders have increased their IT budgets to improve data security best practices to identify and mitigate risks (Wamba et al., 2015). The findings in this study may also motivate IT and business administrators to form alliances to mitigate data security threats and breaches collectively.

Implications for Social Change

Approximately 81% of all data compromises occur because of identity theft (Chou, 2016). One implication for social change involves reducing the effects of data security threats and breaches on individuals and communities. Subsequent implications for social change include (a) fewer compromises of individuals' personal information, (b) reduced financial risks for organizations, and (c) reduced financial loss for individuals and communities. Identifying best practices IT administrators use to mitigate data security threats and breaches may help organization leaders minimize risks to business performance and sustainability and enhance community relations.

A Review of the Professional and Academic Literature

The objective of this qualitative multiple case study was to explore strategies IT administrators at technology organizations in central North Carolina have used to mitigate data threats and breaches. The literature review was a presentation of scholarly research regarding data security threats and breaches in cloud computing. The literature review included a synthesis of studies to provide a comprehensive analysis of data security. The contents of the literature review were (a) integrated ERM framework, (b)

risk management frameworks, (c) cloud computing, (d) cloud computing adoption, (e) cloud computing governance, (f) data security, (g) data security breaches, (h) data security governance, (i) data security regulations, and (j) data security standards.

The literature review included a critical examination and synthesis of data security and cloud computing literature. I used the following databases to retrieve scholarly and peer-reviewed literature for this study: (a) ABI/INFORM Complete, (b) ACM Digital Library, (c) Business Source Complete, (d) Computers and Applied Sciences Complete, (e) Google Scholar, (f) IEEE Xplore Digital Library, and (g) ProQuest Computing. The leading search terms were *cloud adoption*, *cloud computing*, *cloud governance*, *cloud regulations*, *cloud security*, *data breaches*, *data governance*, *data security*, *data threats*, *information administrators*, *information professionals*, *information security*, and *information technology*.

I defined the literature content based on the criteria of (a) peer-reviewed texts, (b) material published 2013 or later, (c) relevance to the main tenets of COSO's (2004) ERM integrated framework, and (d) relevance to the research question. Of the 256 references used in the literature review, 248 (97%) were peer-reviewed sources and 246 (96%) were published between 2013 and 2019, which was within 5 or fewer years of my anticipated graduation date. Older sources consisted of seminal works and works from theory literature. Researchers contended that risk management frameworks and organizations, such as IT Infrastructure Library, International Organization for Standardization(ISO), National Institute of Standards and Technology (NIST), and operationally critical threat, asset and vulnerability evaluation , help IT administrators establish and control data

security practices (Ahmad, Maynard, & Park, 2014; Jouini, Rabai, & Aissa, 2014; Zarei & Sadoughi, 2016). The integrated ERM framework comprises the elements described in these recognized models. The integrated ERM framework was a suitable conceptual framework for this study because the framework provided a comprehensive guide for IT administrators to explore the scope of data security in cloud computing. In the following section, I explain the constructs of the integrated ERM framework.

Integrated ERM Framework

COSO (2004) developed the integrated ERM framework to help IT professionals manage enterprise risks associated with data security. ERM refers to organization leaders planning, establishing, leading, and controlling the activities in an organization to reduce the effects of risk on resources (Meidell & Kaarboe, 2017). Conversely, Gordon (2016) posited that ERM refers to assessing and aligning business functions with IT functions to mitigate risks, which decreases the probability of interruptions in business continuity. The eight constructs of the integrated ERM framework, (a) internal environment, (b) objective setting, (c) event identification, (d) risk assessment, (e) risk response, (f) control activities, (g) information and communication, and (h) monitoring, function to guide organization leaders' decision-making regarding managing data security risks (COSO, 2004).

Internal environment. An organization leader develops ERM practices in the internal environment by developing strategies to control risks and perceptions of risks as well as establish a risk appetite (COSO, 2004). Implementing measures to control risks is necessary to reduce perceptions of uncertainty given the increased incidents of data

compromises (Pitsis, Sankaran, Gudergan, & Clegg, 2014). Identifying a risk appetite, or the degree of risk leaders will accept in the process of trying to achieve goals, reveals the ERM philosophy and operating style within the internal environment in organizations (Liu & Wang, 2014). Communicating the significance of ERM to divisions across the organization is necessary for leaders to control risks and improve perceptions of risks.

Objective setting. ERM entails organization leaders establishing processes to set objectives so that the preferred objectives reinforce and align with organizations' business culture and risk appetite (COSO, 2013). Developing set objectives allows leaders to identify potential risks that cause disruptions in business operations (COSO, 2004). Practitioners and researchers call for organization leaders to establish mandatory polices to align business objectives with IT practices to create business value (Coltman, Tallon, Sharma, & Queiroz, 2015; Reynolds & Yetton, 2015) and enhance risk management and business performance (Reynolds & Yetton, 2015). Objective setting should begin at the executive committee level where board members (a) establish business objectives, (b) communicate the objectives organizationwide, and (c) adapt the objectives into policies that align with IT risk management practices (COSO, 2013).

Event identification. Event identification involves identifying internal or external events that might interrupt business performance (COSO, 2004). Administrators must distinguish between (a) events that pose risks, (b) events that create opportunities, and (c) events that may apply to both categories (Al-Musawi, Al-Badi, & Ali, 2015). Four strategies exist to help IT and business administrators identify disruptive events: (a) performing ongoing risks assessments, (b) obtaining third-party risks assessments, (c)

establishing internal risk task forces, and (d) creating event and incident databases to track prior event patterns (Al-Musawi et al., 2015). Opponents of incident reporting systems (e.g., Schulz et al., 2016) asserted that event assessments are ineffective because criteria for classifying disruptive events are vague, and users often lack the expertise to perform risk assessments.

Risk assessment. Researchers use the concepts risk assessment and risk management interchangeably, and the processes involve evaluating, predicting, and categorizing risks based on significance (COSO, 2004). Assessing risk based on the likelihood of an occurrence and potential effect on business performance helps IT administrators evaluate and hone risk assessment procedures (Alebrahim, Hatebur, Fassbender, Goeke, & Côté, 2015). Other key aspects of risk assessment include (a) defining the nature of risks, (b) developing strategies and standards to reduce risks, and (c) identifying stakeholders and their roles in minimizing risks (Alebrahim et al., 2015). Because communication among stakeholders during crises may be complex, establishing risk assessment standards early may help stakeholders understand their roles in mitigating risks prior to crises.

Risk assessment is a significant part of risk management (Aven, 2016) and IT administrators should use risk assessment data to facilitate decision-making at the (a) organization level, (b) business performance level, and (c) IT level (Hansson & Aven, 2014). Bernstein (1996) noted that the basis of risks and risk assessments date back approximately 2,400 years ago when the Athenians introduced their concept of performing risk assessments prior to making decisions. The concept of risk assessment

and risk management from a scientific approach emerged during the 1970s (Bernstein, 1996). Risk management is an ongoing process, and IT administrators should continually evaluate the efficacy of risk management processes (Aven, 2016). The findings in Bernstein's study derived from exploring strategies IT administrators used to mitigate data security threats and breaches, which provided best practices to perform risk assessments and respond to risks.

Risk response. Risk response involves establishing response strategies that align with the risk appetite within the organization (COSO, 2004). Administrators select strategies such as (a) accepting, (b) avoiding, (c) reducing, and (d) sharing risks to respond to data threats and breaches (COSO, 2013). Accepting risks involves identifying potential risks and handling incidents as they occur (Kholidy, Erradi, Abdelwahed, & Baiardi, 2016). Avoiding risks involves withdrawing from events that cause potential risks or restructuring the response approach to achieve business objectives (Kholidy et al., 2016). Reducing risks involves implementing strategies to minimize the likelihood of risks occurring (Kholidy et al., 2016). IT administrators are responsible for collecting and assessing data to respond to risks. Sharing information with all divisions to determine who is qualified to handle risks makes all divisions in the organization accountable for managing risks (Kholidy et al., 2016). Risk responses should be prearranged and relevant to the significance of risk to help IT administrators control how risks affect business performance.

Control activities. Control activities represent the guidelines and processes that indicate how organization leaders execute directives. Control activities include such

practices as (a) data security approvals, (b) sanctions, (c) certifications, (d) reconciliations, and (e) audits (COSO, 2004). Administrators use control activities to prevent threat and compromise activities that could cause data security failure. COSO's (2004) control activities phase comprises many traditional controls: (a) preventive, (b) detective, (c) manual, and (d) automated.

Preventive controls refer to procedures IT administrators use to prevent risks before they occur (COSO, 2004). Examples of preventive controls are (a) applying encrypted passwords, (b) establishing off-site backup database facilities, and (c) creating recovery plans to regain business operability in the event of data security failure (COSO, 2004). Organization leaders who combine risk-centered prevention planning and control processes to mitigate risk, as opposed to focusing on decreasing risk costs, achieve higher business value (COSO, 2004).

Detective controls consist of guidelines IT administrators use to identify risks after they occur (COSO, 2004), which causes delays in responding to risks (Frazer, 2016). The purpose of implementing risk controls is to minimize loss resources and ensure business operability (COSO, 2004). Lapses in response time can prolong the time it takes to recover from risks (Frazer, 2016). Examples of detective controls include (a) performance reviews to assess the effectiveness of systems against achieving business objectives, and (b) reconciliations to compare various data to identify discrepancies to take corrective actions (Frazer, 2016).

Manual controls are processes that individuals manage and initiate as opposed to automated system controls (COSO, 2004). Examples of manual controls are (a) manual

audits, (b) manual data reconciliations, (c) manual reporting to record and document vulnerabilities after audits, and (d) manual performance reviews (COSO, 2004). Manual controls are vulnerable to risks because of lack of employee expertise and training as well as potential human error (COSO, 2004). IT-related manual controls refer to joint manual and automated activities (Benedek, 2016), and provide an upgrade alternative when IT administrators cannot implement automated controls exclusively because of cost restraints (Benedek, 2016). Organization leaders can decrease risks with IT-related manual controls by assigning tasks to experienced IT personnel to confirm the accuracy and extensiveness of the automated data (Benedek, 2016).

Automated controls are processes implemented and performed electronically such as (a) automated systems audits, (b) automated reporting, and (c) automated database maintenance (COSO, 2004). Automated controls are advantageous because administrators use them to perform ongoing system audits and procedural reviews (COSO, 2013). Conversely, Elgammal, Turetken, Van den Heuvel, and Papazoglou (2016) asserted that automated controls might be disadvantageous because of inexperienced IT administrators and outdated systems. In agreement with COSO (2004), Benedek (2016) contended that automated controls are reliable and help IT administrators improve the consistency and predictability of manual controls, which improves IT operations and reduce risk costs.

Information and communication. The information and communication process involves identifying, collecting, and communicating information relative to risk vulnerabilities in data security in a style and timeframe that allows IT administrators to

educate members across divisions in the organization so they can perform their respective responsibilities (COSO, 2004). Evaluating the sources of internal and external information is necessary to confirm that data are an accurate account of business objectives and IT operations (COSO, 2004; Pham, Pham, Brennan, & Richardson, 2017). Rae, Sands, and Subramaniam (2017) linked three aspects of information and communication (e.g., information accuracy, information sharing and education, and information transparency) with control activities. Rae et al. also linked two other aspects of information and communication (e.g., effective communication and regular feedback) with risk assessment. Communicating relevant risk management information to divisions across organizations makes individuals accountable for identifying, responding to, and monitoring risks (COSO, 2004).

Monitoring. Monitoring refers to testing systems to determine whether risk management strategies remain effective and relevant (COSO, 2004). Continuous monitoring is necessary because (a) innovations in IT, (b) updated data security regulations, and (c) evolving business objectives require timelier and more functional systems and controls to protect sensitive data (COSO, 2004). Regularly monitoring authorized users' access to sensitive data helps IT administrators (a) identify who is responsible for managing and administering data and (b) assess their competence to perform such tasks (Siponen, Mahmood, & Pahnila, 2014). An essential part of risk management is defining how frequently to monitor risk indicators and identifying the individuals responsible for doing so (Siponen et al., 2014). Defining the aspects of the monitoring process should be a team effort.

Using the integrated ERM framework to evaluate stakeholders' perceptions concerning data security could reveal different perspectives regarding what constitutes secure business and IT environments. Al-Musawi et al. (2015) applied the integrated ERM framework to explore how end users in private and public organizations managed risks in cloud computing environments. Al-Musawi et al. found that identifying and communicating risks to upper management prior to adopting cloud services was effective for proactively mitigating risks. The findings also indicated that improving staff awareness by providing data security and risk management training were suitable measures to prevent data security failure in cloud environments (Al-Musawi et al., 2015).

Al-Musawi et al.'s (2015) findings revealed that organization leaders relied on detailed, though disorganized, frameworks to address data security failure. Al-Musawi et al. recommended that business leaders could address security vulnerabilities by implementing the integrated ERM framework, which outlines an integrated system of multiple constructs that guides leaders in transitioning from traditional on-site IT services to cloud services in multitenant environments. Organization leaders in Al-Musawi et al.'s study agreed that the best responses to data security failure were avoiding and controlling risks.

In another study, Almgren (2014) applied COSO's (2004) integrated ERM framework to explore how organization leaders analyzed risks and interruptions to business continuity in the cloud. Almgren posited that the key to solving data security failure in the cloud involved finding responses that (a) identify risks, (b) reduce the

probability of risks occurring, and (c) help organization leaders identify the amount of acceptable risk to achieve business objectives. Almgren found that event identification, risk assessment, and risk response helped organization leaders perceive risk events as opportunities to increase risk management awareness.

Risk Management Frameworks

Researchers applied risk management frameworks and theories to explore data security in cloud computing (e.g., Hanus & Wu, 2016; Ibrahimovic & Franke, 2017; Park, Shin, & Song, 2016). To justify implementing cloud services, IT administrators must implement risk management systems that provide relevant strategies to assess, manage, and secure data (Islam, Fenz, Weippl, & Kalloniatis, 2016). The following section described the protection motivation theory, risk IT framework, and risk management framework, which were alternative conceptual frameworks I considered using as the basis for this study.

Protection motivation theory. I considered Rogers's (1975) protection motivation theory as the conceptual framework for this study. Rogers originally introduced the protection motivation theory as a social cognitive model to predict individuals' behavior. In 1983, Rogers applied the protection motivation theory to understand how individuals react to and cope with threats in data security. Safa et al. (2015) attributed Rogers's (1983) seminal research as the impetus for additional behavioral research in data security.

The two constructs of the protection motivation theory are threat appraisal and coping appraisal (Rogers, 1983). Threat appraisal refers to how individuals perceive and

assess the severity of risks that occur from vulnerabilities in data security (Rogers, 1983). These risks can threaten accessibility, reliability, and confidentiality of data (Safa et al., 2015).

Coping appraisal refers to how well individuals cope with data security threats or risks (Rogers, 1983). Studies regarding how individuals react during impending threats depict how individuals perceive and cope with risks (Rogers, 1983). Researchers use protection motivation theory to explain and predict individuals' motives for engaging in actions to protect virtual and physical resources in organizations (Jansen, Veenstra, Zuurveen, & Stol, 2016; Tapsuwan, Mankad, Greenhill, & Tucker, 2017).

Jansen et al. (2016) used the protection motivation theory to expound on users' motives for implementing protective practices in data security. Jansen et al. purported that coping appraisal motivated users to adopt protective data security practices when they (a) perceived a technique was effective, (b) felt competent enough to use computer equipment, (c) had a positive perception regarding data security protection, and (d) took ownership for data security. In opposition to Jansen et al. (2016), Ifinedo (2014) posited that coping appraisal motivated users to (a) consider the consequences of their actions prior to responding to threats and risks, (b) consider the degree of potential damage and incurred cost from threats and risks, and (c) comply with established data security standards. To mitigate risks, IT administrators must reinforce data security practices by implementing strategies that help them identify, assess, and respond to data threats and breaches (Ifinedo (2014).

Researchers noted that IT administrators are integrating IT solutions to streamline

operation practices, which makes organizations vulnerable to data security failure (Caniëls et al., 2015; Chen et al., 2016; Lohrke, Frownfelter-Lohrke, & Ketchen, 2016; Mithas & Rust, 2016). Best practices in data security require IT administrators to implement strategies, guidelines, and technologies consistent with business operation practices (Posey, Roberts, Lowry, & Hightower, 2014; Singh & Teng, 2015). The practices must be user-friendly enough that users can integrate and interpret the guidelines to identify probable security threats in the workplace (Chen, Lin, & Yen, 2014).

The protection motivation theory provides a framework for understanding what motivates users to cope with and appraise the severity of data security threats and breaches (Rogers, 1983). The intent of this study was to identify and explore strategies IT administrators have successfully implemented to mitigate data security threats and breaches. The protection motivation theory was irrelevant to this study.

Risk management framework. The National Institute of Standards and Technology (NIST) developed the risk management framework in 2010. NIST is a governing agency that sets regulations and best practices for the information and communications technology industry (Yimam & Fernandez, 2016). The risk management framework is an assessment tool that provides a controlled, yet flexible basis for exploring and defining security controls to alleviate threats and risks that occur because of dilemmas in data security (NIST, 2018).

The constructs of the risk management framework are (a) categorization, (b) selection, (c) implementation, (d) assessment, (e) authorization, and (f) monitoring

(NIST, 2018). Cyber criminals are using complex techniques to access confidential data in organizations (NIST, 2018). IT administrators must implement wide-ranging safety techniques because any vulnerable area in operations is a possible threat to data security (NIST, 2018).

Categorization involves maintaining a record of information systems and the data processed, stored, and transferred by systems after performing impact analysis to determine the risks associated with implementing new systems (NIST, 2018). Selection includes adopting standard security controls to operate information systems based on impact analysis (NIST, 2018). IT administrators should amend the controls based on an assessment of organization practices (NIST, 2018). Assessment refers to evaluating security controls to determine (a) how accurately users implement the controls, (b) if the controls are functioning as envisioned, and (c) if the controls are creating outcomes according to system and security requirements (NIST, 2018).

Authorization refers to approving information system tasks based on evidence that the risks to (a) organization operations and resources, (b) people, and (c) external stakeholders are acceptable (NIST, 2018). Monitoring risk involves assessing risks long-term (Joos, Piotroski, & Srinivasan, 2016) and involves periodically evaluating risk assessment processes to determine if IT professionals need training to enhance their risk management skillset (NIST, 2018). The risk management framework is inclusive and consists of best practices for IT administrators to assess risk compliance controls (NIST, 2018.

NIST (2010) created the risk management framework to help federal organizations in the U.S. to implement new IT systems. Meszaros and Buchalcevova (2017) questioned the effectiveness of the framework because of the time consuming process of continuous assessing and monitoring information systems and security controls. Meszaros and Buchalcevova noted that an effective risk management framework provides guidelines for selecting security controls based on the results of assessing and monitoring threat and risk vulnerabilities.

Kalaimannan and Gupta (2017) contradicted Meszaros and Buchalcevova's (2017) views and noted that monitoring provides an added level of systems reinforcement, which allows system owners to address emerging internal vulnerabilities as they occur rather than after external attacks ensue. Kalaimannan and Gupta likewise asserted that, without adequate research and training, NIST's (2010) framework is inconvenient because the complex security controls can overwhelm novices and prevent organization leaders from adopting the framework. The risk management framework is widely accepted, which has led to a market for numerous publications and training tools to instruct system owners (Kalaimannan & Gupta, 2017).

Mendelson and Mendelson (2017) applied the risk management framework in practice to explore how third-party vendors in the United Kingdom have legal access to consumers' sensitive data without restrictions. Mendelson and Mendelson noted that study participants, which consisted of international software engineers, purported that (a) continuous systems monitoring, (b) keeping accurate records of data transfers, and (c) limiting the use of *live* data while testing systems provided controls to improve data

security. Kalaimannan and Gupta (2017) also posited that the complexity of applying the risk management framework in practice was problematic for novice users.

The risk management framework provides a model for assessing data security failure (NIST, 2010). IT professionals implement the framework to create, assess, and maintain risk management controls for information and communication technology compliance (NIST, 2018). Because the intent of this study was to explore strategies IT administrators have successfully used to mitigate data security threats and breaches, the risk management framework was inappropriate for this study.

Risk IT framework. Information Systems Audit and Control Association (ISACA), comprised of 112 colleagues from 18 countries, collaborated with approximately 1,700 IT professionals to create the risk IT framework (ISACA, 2012). The objective of the risk IT framework is to help organization leaders bridge the gap in awareness between ERM and IT risk management practices (ISACA, 2012). The constructs of the risk IT framework are (a) risk governance, (b) risk evaluation, and (c) risk response (ISACA, 2012).

Risk governance involves integrating IT risk management controls with ERM controls to handle risks based on a cost and profit analysis (ISACA, 2012). Risk evaluation refers to identifying and assessing IT-associated risks and opportunities for profit and presenting the findings in a business format (ISACA, 2012). Risk response involves addressing IT-associated risk concerns, opportunities, and incidents from a cost-effective perspective and in a manner that aligns with business objectives (ISACA, 2012). IT risk management is a fundamental element of data security, and IT administrators

must implement strategies to mitigate threats and promote risk awareness organizationwide (ISACA, 2012).

Hatefi and Fasanghari (2015) applied the risk IT framework in practice to explore strategies IT administrators use to improve ERM and data security risk awareness when implementing new IT projects. Project risk management involves implementing strategies to improve the project performance by (a) methodically identifying and evaluating risks, and (b) developing strategies to minimize or avoid risks and create business value. IT administrators in Hatefi and Fasanghari's study findings revealed that IT administrators implemented the risk IT framework to capitalize on opportunities to protect IT assets (e.g., data, hardware, and software) and obtain the maximum return on IT investments. The risk IT framework provides a model to help organization leaders accept and manage tolerable degrees of risks and character damage to pursue a return on investment (ISACA, 2012), which was not the intent of this study. The risk IT framework was inappropriate for this study.

Irrespective of which risk management framework (or combination of frameworks) IT administrators select to reduce data threats and breaches, there is a significant caution. The constructs within the framework should align with business and IT operations, as well as local, state, and national IT compliance regulations (Al-Ruithe, Benkhelifa, & Hameed, 2018). Because IT compliance regulations differ at the local and national levels, establishing a data governance framework consistent with IT and business requirements helps administrators establish a system of accountability to identify individuals responsible for securing, distributing, and using data in organizations (Al-

Ruithe, et al., 2018).

Cloud Computing

Cloud computing is an online data management system wherein third-party vendors lease comprehensive cloud services to consumers (Avram, 2014). NIST (2018) recognized five significant features of cloud computing: (a) on-demand availability, (b) broad network access, (c) resource sharing, (d) scalable services, and (e) monitored services. IT administrators use cloud services to manage data capabilities, as well as improve sustainability and competitive advantage (Lal & Bharadwaj, 2016). Cloud services also reduce IT costs and improve business agility (Talluri, 2016; Tsai & Hung, 2014).

Compliance, manageability, and effective data security practices are three capabilities essential to creating business value (Lal & Bharadwaj, 2016). The three common cloud models are (a) SaaS, (b) PaaS, and (c) IaaS (Kushida, Murray, & Zysman, 2015; Lal & Bharadwaj, 2016). SaaS refers to applications delivered to end users online as a service (Lal & Bharadwaj, 2016). SaaS applications are advantageous because end users implement SaaS programs to operate existing Internet applications and systems (Lal & Bharadwaj, 2016), which eliminates the need to run applications on separate computers. One disadvantage of using SaaS is the lack of end user manageability privileges (Sharma, Singh, Singh, & Kaur, 2016). Examples of SaaS providers are Citrix, GoToMeeting, and Facebook (Lal & Bharadwaj, 2016).

PaaS services are services end users implement to create tailor-made development and deployment platform applications (Kushida et al., 2015). End users implement PaaS

services to customize cloud applications with existing software codes (Kushida et al., 2015). PaaS providers deliver applications on public domains, which is disadvantageous to private businesses that cannot customize the services to meet their respective needs (Sharma et al., 2016). Examples of PaaS providers are Windows Azure, Force.com, and Google App Engine (Kushida et al., 2015).

IaaS service providers deliver server, storage, and network capabilities as a service (Kushida et al., 2015). IaaS solutions allow end users to operate multiple hardware and software applications on designated cloud hardware. One disadvantage of IaaS applications is the lack of service provider technical support (Sharma et al., 2016). Examples of IaaS providers are Amazon EC2, Windows Azure, and Rackspace (Kushida et al., 2015).

Adopting cloud services and outsourcing IT functions to manage software applications is prevailing in organizations (Fung, 2016). Yet, research and toolkits that help IT administrators map applications to particular cloud deployment models are sparse (Fung, 2016). Deployment models depict how users gain access to cloud services (Fung, 2016). The four common cloud deployment models are (a) public cloud, (b) private cloud (c) community cloud, and (d) hybrid cloud (Islam & Rahaman, 2016). Organization leaders should invest in cloud deployment models based on (e) business requirements, (a) compatibility with existing applications, and (b) the degree of support necessary to operate the models successfully (Islam & Rahaman, 2016).

Public cloud refers to open-access services (e.g., Google) controlled by cloud providers (Islam & Rahaman, 2016). Private cloud signifies systems tailor-made for a

single organization and maintained by the cloud provider (Islam & Rahaman, 2016). Community cloud refers to services where groups of similar organizations (e.g., hospitals, banks, and utility companies) establish information by sharing cloud infrastructures (Islam & Rahaman, 2016). Hybrid cloud includes a combination of two or more public or private cloud models (Islam & Rahaman, 2016). As cloud adoption has increased, cloud providers have expanded the line of deployment models to help meet users' specific IT needs (Islam & Rahaman, 2016).

In 2013, cloud computing emerged as a model projected to revolutionize the mainstream ways in which vendors provided computing services to customers (Sultan, 2013). Cloud adoption rates increased because of advantages such as (a) cost-effectiveness, (b) scalability, (c) efficiency and (d) reduced operation and maintenance costs (Cioca & Ivascu, 2014; Sridhar, 2016)). The findings in Wang, Wood, Abdul-Rahman, and Lee's (2015) study revealed that integrating cloud services in IT projects could reduce delays in meeting deadlines and improve the scope of projects. IT project managers, despite the advantages of using cloud services, expressed apprehensions regarding disadvantages such as (a) lack of data confidentiality, and (b) inconsistencies in U. S. and global regulations and governance policies (Wang et al., 2015).

In 2016, International Trade Administration (ITA) researchers predicted that organization leaders would invest approximately $191 billion on cloud services by 2020. The prediction represented a 20% increase above the 2014 proposed expansion rate, which indicated there was a surge in cloud adoption (ITA, 2016). Researchers in the International Data Corporation predicted investments in cloud computing to surpass the

$107 billion mark by 2017, doubling the $47.4 billion prediction for 2013 (ITA, 2016). In 2015, the cost-effectiveness of cloud services, along with the need to store, monitor, and evaluate large volumes of data, caused organization leaders to adopt cloud services at scale (Chou, 2016).

Hashem et al. (2015) supported Sultan's (2013) projection and described cloud computing as a revolutionary alternative to traditional on-site IT services. Contrary to Sultan's projection, Avram (2014) indicated that because of disadvantages such as service providers' viability and lack of transparency, organization leaders should only consider cloud adoption after exploring factors such as (a) how well cloud services work with existing IT functions, and (b) cost-effectiveness in relation to organization size and staff expertise. Riungu-Kalliosaari, Taipale, Smolander, and Richardson (2016) introduced a 5-phase cloud adoption toolkit to help organization leaders make informed decisions about adopting cloud services.

Cloud Computing Adoption

Cloud service providers deliver on-demand computing services (e.g., SaaS, IaaS, and PaaS), which IT administrators in developed and developing countries use to expand service supply and performance in organizations (Senyo, Effah, & Addae, 2016). Samimi, Ledary, and Samimi (2015) indicated that cloud adoption rates in developing countries were 50% to 70% lower than rates in developed countries. The percentages could be higher because employees in developing countries seldom share experiences regarding failed cloud adoption processes (Samimi et al., 2015). Contrary to Samimi et al. (2015), Ika and Saint-Macary (2014) noted that cloud adoption rates were lower in

developing countries because IT administrators lacked strategies to influence organization leaders' decision-making regarding the advantages of cloud adoption.

A plethora of literature exists regarding cloud adoption in developing countries (e.g., Carcary, Doherty, & Conway, 2014; Dillon & Vossen, 2015; Ratten, 2014; Senarathna, Yeoh, Warren, & Salzman, 2016; and Tang & Liu, 2015). Dillon and Vossen (2015), Ratten (2014), and Tang and Liu (2015) posited that organizations' geographic location and data security failure were determinants for cloud adoption in developing countries. Conversely, Senarathna et al. (2016) indicated that lack of affordable internet and telephone access influenced organization leaders' propensities to decline cloud adoption in developing countries.

Carcary et al. (2014) also posited that cultural differences and geographic location played roles in organization leaders' inclinations to decline cloud adoption in developing countries. Ratten (2014) asserted that exploring cloud adoption in diverse regions could improve organization leaders' perspectives regarding cloud adoption in developing countries. COSO (2004) indicated that the internal environment in organizations, which includes diverse cultural perspectives, defines how organization leaders assess risks and make decisions about adopting new services and products.

The cloud concept is a comparatively new phenomenon, and cloud adoption research is still in an evolving phase (Buyya et al., 2019; El-Gazzar, Hustad, & Olsen, 2016; Vithayathil, 2018). IT administrators have expressed a growing interest in cloud services to perform complex business tasks (Buyya et al., 2019; Kappelman, McLean, Luftman, & Johnson, 2013). In 2012, IT analysts recognized cloud computing as the third

most influential IT investment and the fifth most prominent global technology (Kappelman et al., 2013). Buyya et al. (2019) projected that investments in cloud services would increase from $70 billion in 2015 to approximately $203 billion in 2020.

IT administrators are managing complex data security and governance processes (Kappelman et al., 2013). The leading cloud adoption concerns among organization leaders and IT administrators in developed and developing countries are (a) data security threats and breaches, (b) vague legal criteria for cloud adoption, and (c) conflicting global governing practices (Kappelman et al., 2013; Lee, 2019). Although no single governance framework incorporates every available IT control, combined, the frameworks help IT administrators address essential aspects of data security governance (Zafar et al., 2017).

Cloud Computing Governance

Cloud computing governance involves implementing detailed guidelines for using cloud services (Prasad & Green, 2015). IT administrators use cloud computing governance principles to secure data located on remote IT infrastructures (Prasad & Green, 2015). Because the cloud is the leading method for providing computing services globally, legislative and regulatory governance models are gaining more notoriety from increasing incidents of data security failure (Brender & Markov, 2013; Prasad & Green, 2015). Organization leaders are implementing governance strategies to (a) align IT objectives with sustainability goals, and (b) assess and manage risks in a timely manner (Prasad & Green, 2015). Although some of the governance concerns such as (a) data security compliance, (b) access authentication, and (c) confidentiality are common features in computing, unique features in cloud computing such as multitenancy and

resource sharing exacerbates the impact of such concerns (Prasad & Green, 2015).

Organization leaders understand the landscape of IT risks in traditional computing systems (Yousif, Edsall, Krebbers, Pappe, & Khalidi, 2014). Leaders implement governance standards such as (a) the cooperative ISO and international electrotechnical commission, (b) control objectives for information and related technologies, and (c) the payment card industry data security standard, to manage IT functions in cloud computing (Yousif et al., 2014). By 2012, approximately two-thirds of the Financial Times Stock Exchange 100 Index organizations were either completely or moderately compliant with the ISO/IEC 27,000 system of security controls (ISO, 2014).

Yousif et al. (2014) asserted that adhering to governance controls is a creditable approach to mitigating data security failure. Prasetyo and Surendro (2015) purported that complying with controls alone does not guarantee data security. Organization leaders must adopt user-friendly data governance models that align with IT and business operations to mitigate data security threats and breaches (Prasetyo & Surendro, 2015). El-Gazzar et al. (2016) posited that IT administrators often lack IT governance strategies and skills to manage and secure cloud services, which makes upper management hesitant about adopting cloud services.

The links between acceptable and prohibited practices in cloud computing remain ambiguous (Verma & Bhattacharyya, 2017). Traditional data security regulations, as well as predictable business profiles, are becoming unsustainable in the cloud (Kim et al., 2014). Implementing cloud services requires organization leaders to assess governance models to adopt IT risk management controls that align with business and IT practices

(Kim et al., 2014). Mathur and Purohit (2017) also asserted that conventional governance controls are no longer viable in multitenant cloud environments.

Data Security

Data security involves protecting IT systems against security threats and breaches that compromise the accessibility, reliability, and privacy of data (Savola, 2014). Security and privacy are the challenges that prevent cloud adoption in practice (Wei et al., 2014). Unlike traditional computing models, where end users manage data storage and data manipulation, cloud computing involves service providers acquiring full control of managing data and systems (Savola, 2014; Wei et al., 2014). Because of end- users' limited access to managing and controlling data security, data are vulnerable to attacks (Wei et al., 2014).

Researchers study cloud data security challenges and issues from perspectives such as (a) data confidentiality, (b) data integrity, and (c) network security (DeSouza & Valverde, 2016; Kumarga & Sireesha, 2014; Rao & Ramana, 2016). Because of the increasing number of data breach incidents, IT administrators should implement extensive data security measures in cloud environments (Gordon, 2016). IT administrators need to understand how to align Administrators can apply the integrated ERM framework to link ERM practices with business objectives to enhance risk management practices (COSO, 2004).

Data confidentiality is essential for end users to store private or sensitive data (Xia et al. 2016). Because of the rise in adoption of cloud services, IT administrators are motivated to outsource data to cloud platforms because of cost-effective data

management services (Bajaj & Sion, 2014; Xia, Wang, Sun, & Wang, 2016). Xia et al. (2016) suggested that IT administrators should encrypt sensitive data prior to outsourcing to maintain data confidentiality to make it hard for unauthorized users to access data with traditional passwords.

Contrary to Xia et al. (2016), Hadden and Mahdy (2016) asserted that combining data encryption and fragmentation improves data confidentiality in cloud services. Fragmentation refers to partitioning data to multiple platforms among several cloud providers (Hadden & Mahdy, 2016). Acquiring support from multiple cloud providers enhances data confidentiality and security (Hadden & Mahdy, 2016).

Data integrity is a fundamental element in IT system operations (Rao & Ramana, 2016). Data integrity refers to protecting data from illegal deletion, adaptation, or assembly (Rao & Ramana, 2016). By contrast, Kumarga and Sireesha (2014) indicated that data integrity refers to how accurate and reliable data are after two or more updates. Rao and Ramana and Kumarga and Sireesha agreed that cloud service providers are obligated to monitor users' access and rights to IT resources, which ensures that confidential data and services are less susceptible to unauthorized and fraudulent activities. Reece and Stahl (2014) added that IT administrators play significant roles in securing confidential data; yet IT administrators' lack of knowledge of cloud computing and network security discourages organization leaders from adopting cloud platforms.

Network security entails applying tools such as firewall applications, anti-virus software, and anti-spyware software to filter incoming content (Schlechtendahl, Kretschmer, Sang, Lechler, & Xu, 2017), which protects users' information against

unauthorized access (Hassan, Lin, Yue, & Wan, 2017). A computer network consists of a group of computers that administrators merge to share resources (Li, Li, Pan, & Zhang, 2015). Access to the Internet is the most shared resource among users on a network (Li et al., 2015). Users also share resources such as data, file servers, and printers (Hassan et al., 2017).

Schlechtendahl et al. (2017) asserted that IT professionals design network security systems to mitigate malicious attacks on users' information. Chu, Chow, Tzeng, Zhou, and Deng (2014) indicated that threats such as (a) insecure Web applications, (b) malware attacks, and (c) data leakages pose threats to network security systems. Although cloud computing is economically advantageous, Chu et al. (2014) purported that inconsistencies in global security standards and laws, as well as lack of assurance for data confidentiality, prevent organization leaders from adopting cloud services on a large scale.

Data Security Standards

Cloud adoption has increased since the initial inception of the product in 2006 (Martínez-Pérez, De La Torre-Díez, & López-Coronado, 2015). Because cloud computing involves using a network of remote servers hosted on the Internet, organization leaders must implement preventative security standards to ensure that collecting, storing, and manipulating users' private information occurs in secure environments (Martínez-Pérez et al., 2015). Mandatory security standards exist to help organization leaders establish best practices to mitigate data security failure (Lee, Geng, & Raghunathan, 2016). The purpose of security standards is to help IT administrators

identify approaches and solutions to mitigate data security challenges in cloud computing (Lee et al., 2016).

Because organization leaders rely on multiple security frameworks to remain compliant with federal, state, and local regulations, IT administrators must comply with established security standards to avoid compliance penalties in the event security breaches occur (Lee, Park, & Yang, 2015). The list of data security standards is extensive, and adopting a specific standard or a combination of diverse standards in multiple frameworks is contingent upon (a) organization size, (b) employees' IT expertise, and (c) the efficacy of existing business strategies and IT security frameworks (Castka & Corbett, 2015; (Prasad & Green, 2015).

There are two categories of data security standards : technology and management (Heatherly, 2016). Technology security standards include strategies IT administrators use to concentrate on the logical (e.g., authorization, authentication, encryption, and passwords) and physical aspects of data security (e.g., inaccessible computers, investigations, or inoperable systems; Heatherly, 2016). Conversely, IT administrators use management security standards to implement strategies to develop and supervise best practices to regulate and protect sensitive data (Heatherly, 2016).

In 2005, ISO developed the ISO/IEC 27001 standard series, which outlines the criteria for (a) establishing, (b) applying, (c) operating, (d) assessing, and (e) enhancing management and IT security practices (Alebrahim, et al., 2015). ISO 27001 consists of security strategies IT administrators and organization leaders use to share information and align IT objectives with business objectives (Alebrahim et al., 2015). The ISO/IEC

27010:2015 international standard, an extension of ISO 27001, includes instructions organization leaders implement to exchange and share sensitive data globally within similar or competing industries (Mok & Ang, 2016). The ISO/IEC 27001:2013 standards, extensions of the initial ISO 27001 standards, are nonspecific and applicable to organizations in all business industries (Choi, Choi, & Kim, 2014).

Data security standards such as the (a) Cloud Security Alliance (CSA), (b) European Network and Information Security Agency, and (c) Information Technology Infrastructure Library outline strategies that allow IT administrators and organization leaders to collaborate to develop processes to mitigate data security vulnerabilities (Ali, Khan, & Vasilakos, 2015). The objective of implementing data security programs is to offer frameworks that allow organization leaders and IT administrators to develop and implement strategies to (a) improve data security awareness, (b) assess systems and processes to identify vulnerabilities, and (c) identify intentional and unintentional threats to enhance data security governance (Ali et al., 2015).

Data Security Governance

Data security governance refers to the guidelines and accountability standards IT administrators implement to establish effective data management policies (Thompson, Ravindran, & Nicosia, 2015). One aspect of data security governance involves identifying stakeholders' roles in the data security governance process (Thompson et al., 2015). Assessing stakeholders' perceptions regarding security governance helps organization leaders judge the efficacy of data security governance plans (COSO, 2004).

Making data security a shared effort among internal and external stakeholders

bolsters buy-in and decreases the likelihood of interruptions in business continuity during crisis (Thompson et al., 2015). Ernst and Young (2013) surveyed 500 IT administrators worldwide who acknowledged a link between effective security governance and business stability. At 20% of the organizations in the Ernst and Young study, IT administrators indicated that establishing a governance plan helped IT administrators identify vulnerabilities in data security early. Organization leaders should integrate IT security governance initiatives with corporate governance initiatives to enhance business operability (Thompson et al., 2015).

IT administrators can enhance data governance policies by (a) proactively identifying and monitoring risks, (b) aligning risk management policies with business practices, (c) responding to risks in a timely manner and (d) assessing risk management strategies to ensure strategies remain relevant and effective (COSO, 2004). Thompson et al. (2015) indicated that data governance controls exist to help IT administrators manage IT functions. Tisdale (2015) asserted that IT administrators lack the expertise to apply governance controls to achieve IT objectives, which could impede business continuity.

Data security governance is a fundamental aspect of enterprise risk management (Carcary et al., 2014). Organization leaders must assess their existing maturity aptitude regarding IT security governance and risk management to identify vulnerable areas that warrant attention (Carcary et al., 2014). Atoum, Otoom, and Abu Ali (2014) asserted that consumers expect organization leaders to govern data security practices and implement strategies to mitigate data compromise. Effective data governance involves identifying and implementing regulations to manage and mitigate data security threats and breaches

(Tisdale, 2015).

Data Security Breaches

Data breaches occur when unauthorized users unintentionally or maliciously compromise sensitive data (Saidani et al., 2013). Data breach victims lose revenue or incur physical or virtual property damage (Saidani et al., 2013). The financial effect is substantially higher during malicious breaches or illegal acts (Ponemon Institute, 2015). Privacy Rights Clearing House (2016) researchers ranked cybercrime as the number one concern for organization leaders.

The three most common forms of data breach are (a) physical theft, which refers to stolen documents, laptops, servers, or computers; (b) skimming, which involves stealing the magnetic strip from credit cards; and (c) cybercrime, which involves such acts as cyber espionage, hacking, Internet attacks, malware, and viruses (Edwards, Hofmeyr, & Forrest, 2016). Hacking accounted for 11.3% of data attacks in September of 2016 (Privacy Rights Clearing House, 2016). Cyber espionage accounted for 4.2% of data attacks in September of 2016 (Privacy Rights Clearing House, 2016). Cyber warfare (e.g., deliberately attacking military IT systems) accounted for 4.2% of the data attacks in September of 2016 (Privacy Rights Clearing House, 2016).

There has been an increased number of data breach incidents since 2008 (Holtfreter & Harrington, 2014). Between 2005 and 2013, there were approximately 4,000 reported cases of data breach incidents in the U.S. (Holtfreter & Harrington, 2014), and the effects of data breach occurrences were substantial for organizations and private consumers (Holtfreter & Harrington, 2014). Economists classify the financial effect of

security breaches as short-term costs incurred only during the time of the breach, and long-term costs incurred for extended periods (Chen, Dong, & Chen, 2016). The magnitude of the short-term and long-term costs could vary based on the form of breach and organization type (Chen et al., 2016).

Organizations and consumers suffer substantial financial loss because of data breaches. Ponemon Institute (2015) researchers revealed that U.S. organizations' losses totaled approximately $5.9 million for every individual data breach incident. Consumers' losses totaled approximately $16 billion after 12.7 million incidents of fraud and compromises in personal data occurred (Ponemon Institute, 2015). In 2018, the average cost of a single data breach incident was $148 million, and it took IT administrators approximately 196 days to identify a breach (Ponemon Institute, 2018). Federal Trade Commission analysts indicated that identity theft was the number one complaint among consumers in 2015 (Ponemon Institute, 2015). Figure 1 illustrates that organizations' losses from data breaches totaled $2.34 million to $3.72 million over a 10-year span (Ponemon Institute, 2015).

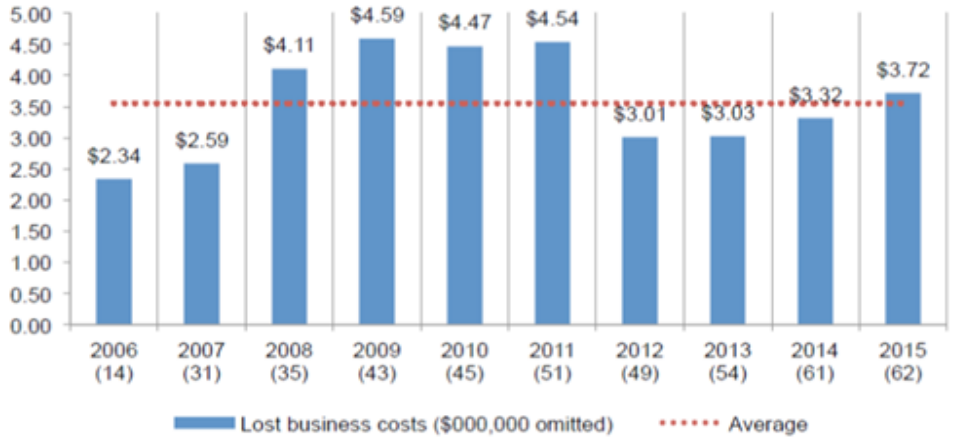

Figure 1. Average organization costs over 10-year span. Retrieved from "2015 Cost of Data Breach Study: United States," From IBM & Ponemon Institute, 2015, Ponemon Institute Research Report, p. 13. Copyright 2015 by Ponemon Institute. Adapted with permission.

Despite all the precautionary actions taken by IT administrators, the increasing numbers of data breaches are not restricted to a specific industry or form of data breach (Sen & Borle, 2015). For example, of the reported data compromises that occurred in the U.S. between 2005 and 2012, 22% of the cases involved incidents with consumers' medical information (Sen & Borle, 2015). During 74 % of the cases, attackers compromised consumers' private information (e.g., social security numbers and driver license numbers; Sen & Borle, 2015). Because of the increased number of attacks against consumers' personal information, consumers have pursued legal actions against organizations to recover financial losses (Romanosky, 2016).

The five leading industries attacked in 2015 were (a) retail, (b) financial, (c) computer software, (d) healthcare, and (e) governmental agencies (Department of Networked Systems and Services [DNSS], 2016). The five leading types of data stolen in 2015 were (a) legal names, (b) social security numbers, (c) residential addresses (d)

financial data, and (e) birthday data (DNSS, 2016). In 2015, attackers compromised data at 60% of SMEs in the U.S. (DNSS, 2016). The numbers of reported cases of data failure indicate the need for additional data security research.

Because of the regularity of data breach occurrences and the economic effect on IT budgetary spending in organizations, IT administrators must be vigilant to identify strategies to recognize data security risks early (Sen & Borle, 2015). Implementing strategies to identify the elements of cybercrime helps IT administrators mitigate security attacks (DNSS, 2016). Organization leaders should inform victims prior to breaches regarding the practices IT administrators have implemented to identify and resolve risks (Modi, Wiles, & Mishra, 2015). Because of the increasing number of data compromises, a study regarding strategies IT administrators use to mitigate threats and breaches may help IT professionals establish best practices to minimize data security failure.

Proactively alerting customers regarding established data security policies can help maintain good customer relations (Modi et al., 2015). Informing consumers about pending or existing breaches in security also reduces the effect of loss when crises occur (Modi et al., 2015). Because data security is a safety initiative that should span across divisions in organizations, organization leaders should encourage employees to remain productive during crises to help manage the effect of risks for shareholders once the public is informed about data breach incidents (Modi et al., 2015).

The unprecedented numbers of data breach incidents in the U.S. has led to public alarm (Risk Based Security, 2015). In 2014, U.S. organizations encountered 1,343 data breaches, which led to 512 million damaged files (Risk Based Security, 2015).

Legislators reacted by ratifying state and federal regulations that made organization leaders responsible for notifying consumers regarding data breaches (Risk Based Security, 2015). Because of the increased dependency on IT, and the increased number of data breaches, IT administrators must implement strategies to identify, mitigate and prevent data compromise (Ben-Asher & Gonzalez, 2015). Organization leaders and IT administrators are responsible for assessing and protecting enterprise systems from vulnerabilities and threats (Ben-Asher & Gonzalez, 2015).

Cloud computing provides opportunities for organization leaders to improve service processes (Kude, Hoehle, & Sykes, 2017). Using cloud services also increases the threat of unauthorized users gaining illegal access to sensitive data (Kude et al., 2017). With the surge in breach incidents, organization leaders have implemented strategies to prevent data breaches (Kude et al., 2017). Contrary to Ben-Asher and Gonzalez (2015), Kude et al. (2017) asserted that IT administrators should implement strategies to handle security breaches once they occur. Kude et al.'s study revealed that compensating consumers after breach incidents restored consumers' loyalty quicker, rather than providing no incentives to consumers.

Opposing Ben-Asher and Gonzalez's (2015) and Kude et al.'s (2017) assertions, Martin and Murphy (2016) posited that even though marketers rely on consumers' personal information to share promotions, marketers have limited awareness regarding the ramifications of inappropriately handling consumers' data. Martin and Murphy also indicated that marketers' lack of data management skills could increase consumers' perceptions of vulnerability because of the increased numbers of data breaches. Kude et

al. (2017) contended that consumers' perceptions of vulnerability increases when organization leaders' fail to make restitution for losses after security breaches occur.

IT professionals perceive that data security failures are avoidable (Chou, 2016). Organization leaders in numerous organizations received criticism from consumers and governing agencies for mismanaging data and neglecting to implement effective security practices (Chou, 2016; Kude et al., 2017). Another factor that attributes to increases in successful security breaches is that IT administrators miss warning signs (e.g., irregular login requests and repeated requests for access to the same files) that, when addressed; prohibit attackers from successfully compromising sensitive data (Chou, 2016). Warnings are futile if IT administrators fail to conduct ongoing system and procedural assessments (Chou, 2016). Dreyfuss and Giat (2018) posited that IT administrators should perform ongoing risk assessments in traditional and cloud computing environments to evaluate security risks,

Many organization leaders fail to implement strategies to mitigate security risks, or allocate funding to make security investments before and after crises (Chou, 2016). The reason is that many organizations are not incurring significant revenue losses or risks from data breaches, because consumers and credit card companies bare the majority of the risks (Chou, 2016). Economic analysts maintained that existing governmental proposals would not correct this imbalanced cost-to-risk dilemma (Chou, 2016). Although the Federal Trade Commission has applied affirmative measures to levy added costs on organizations where business leaders disregard existing security processes, the existing cost-to-risk imbalances caused by security risks remain substantial for consumers

(Chou, 2016).

IT analysts expect that data breach incidents will continue to gain public notoriety because of (a) modifications in compliance and governing controls, and (b) the imbalance in cost-to-risk among organizations and consumers (Martin & Murphy, 2016). Therefore, the potential for IT administrators to participate in the early stages of ERM planning will also increase (Martin & Murphy, 2016). Organization leaders who understand the significance of integrating business practices with IT practices to manage enterprise risks will establish ERM programs that manage data security risks holistically (Atoum et al., 2014). Organization leaders should allocate funding for data security and establish best practices that help curtail the billions of dollars in lost revenue the public incurs annually from data threats and breaches (Atoum et al., 2014).

Transition

Section 1 contains the (a) problem statement; (b) purpose statement; (c) nature of the study; (d) research question; (e) interview questions; (f) operational definitions; (g) assumptions, limitations, and delimitations; and (h) significance of the study. Section 1 also includes the literature review, which includes the following subjects: cloud computing, cloud computing adoption, cloud computing governance, integrated ERM framework, data security, data security breaches, data security governance, data security standards, protection motivation theory, risk IT framework, and risk management framework. Section 1 concludes with an introduction to Section 2.

Section 2: The Project

Section 2 includes an in-depth depiction and rationalization for conducting the research and the methods implemented to increase the reliability and validity of the study. Section 2 starts with a reiteration of the purpose statement, followed by (a) the role of the researcher during data collection, (b) participants' eligibility requirements, (c) the research method and design, (d) population and sampling, (e) ethical research, (f) data collection technique, (g) data collection organization, (h) data analysis, and (i) reliability and validity. Section 2 concludes with an introduction to Section 3.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies IT administrators use to mitigate data security threats and breaches in cloud computing. The target population was four IT administrators at three IT organizations in central North Carolina with 1,000 to 3,000 employees. One implication for social change derived from implementing strategies to reduce the effect of data threats and breaches on individuals, organizations, and community members.

Role of the Researcher

The researcher is responsible for constructing awareness and understanding for the reader while collecting and analyzing data (Kaczynski, Salmona, & Smith, 2013; Morse, Lowery, & Steury, 2014). During qualitative analysis inquiry, researchers should be categorical and flexible (Morse et al., 2014) while attempting to provide a detailed understanding of complex social issues (Kaczynski et al., 2013). Qualitative researchers should also adopt a descriptive way of presenting data, which includes embracing the

idea of the researcher as instrument (Kaczynski et al., 2013), an analogy used by Geertz (1975) to indicate that the researcher is involved with all aspects of the research process at multiple levels.

As the primary data collection instrument, researchers assume multiple roles in qualitative inquiry (Geertz, 1975; Kaczynski et al., 2013; Katz, 2015; Morse et al., 2014; Yin, 2015). First, the researcher identifies a conceptual framework that supports the purpose of the study (Katz, 2015) and reviews the extant literature to link the concepts of the framework with the literature (Yin, 2015). I analyzed and synthesized the extant literature to articulate the rationale for conducting a study pertaining to strategies IT administrators use to mitigate data security threats and breaches.

Second, qualitative researchers strive to understand the core meaning of phenomena by (a) recruiting participants, (b) collecting data, and (c) analyzing and interpreting data (Katz, 2015). Nicholls (2017) purported that qualitative researchers rely on individuals' accounts to substantiate phenomena, rather than the conclusions obtained from large groups. I identified qualified participants to collect relevant data to answer the research question regarding strategies IT administrators use to mitigate data threats and breaches. After collecting data, I drafted an in-depth report to interpret the findings to convey summaries, conclusions, and recommendations for future research.

Research participants are reluctant to share thoughts when they perceive that researchers prefer specific outcomes (Kornbluh, 2015). To gain participants' trust and alleviate skepticism about participating in the study, I (a) established rapport with participants, (b) refrained from guiding participants' responses, and (c) helped

participants understand the research process by explaining the different phases of the study. The research process might be, and generally is, a new experience for participants. Without clearly understanding the purpose and aspects of the study, a participant might question the researcher's ability to be objective and interpret data accurately (Miles & Huberman, 1994).

Researcher bias implies that researchers have preconceived perceptions regarding the study phenomenon (De Massis & Kotlar, 2014). Complete impartiality is neither attainable nor expected in qualitative research (Ahern, 1999). Remaining completely impartial is impossible for researchers to achieve because of factors such as (a) character, (b) socioeconomic status, and (c) values (Greene, 2015). As a researcher, I was responsible for implementing strategies to ensure that my biases did not influence participants' responses.

I used multiple strategies to mitigate my preconceptions regarding data security failure. First, I created a reflective journal to identify and re-evaluate my biases, which helped me bracket any preconceptions. Second, I used an interview protocol (see Appendix A) to collect data in the same manner from all participants. The interview protocol consisted of (a) an introduction statement, (b) a reiteration of the purpose of the study, (c) interview questions that pertained to the research question, and (d) a script of probing and follow-up interview questions, which ensured that the interview process was engaging and conversational.

Researchers should try to make sense of the phenomenon by interpreting participants' responses to understand the scope and depth of their experiences (Noble &

Smith, 2015). Researchers should also refrain from discussing participants' preconceptions to avoid guiding their responses (Chan, Fung, & Chien, 2013). I used member checking to confirm that my interpretations and data analysis reflected participants' responses. Researchers accept member checking as the litmus for establishing reliability in qualitative research (Kornbluh, 2015; Lincoln & Guba, 1985; Patton, 2002). Engaging in the discussion and critiquing researchers' preliminary findings encourages participants to take ownership of the data for possible future use in social change (Fetterman, 1994; Patton, 2008).

I reached data saturation by collecting adequate data to (a) ensure the study was generalizable, (b) confirm that no new data were attainable, and (c) demonstrate there were no new emerging themes. Data saturation is not a generic process; the amount of data needed to reach saturation differs based on the criterion of each study design (Fusch & Ness, 2015). Failure to reach data saturation weakens the validity of the study (Noble & Smith, 2015).

Participants

The impetus for conducting this study was to contribute knowledge that provides awareness about threats and breaches in data security. Identifying IT administrators who were willing to share experiences regarding successful strategies they have used to mitigate data security failure was essential to conducting this study. Eligible study participants had to have at least 3 years of experience applying strategies to successfully identify and mitigate data security failure. Participants also had to agree to share knowledge and answer interview questions pertaining to the research question, as well as

have permission to release applicable documents and artifacts for me to review and evaluate. The subsequent section includes a description of (a) participant criterion for eligibility to contribute to the study, (b) methods for gaining access to participants, and (c) strategies for developing an interactive relationship with participants.

Levitt, Motulsky, Wertz, Morrow, and Ponterotto (2017) indicated that study participants should satisfy the study's eligibility requirements, as well as provide knowledge to satisfy the purpose of the study. The eligibility criteria for the study required that participants have data security expertise and access to documents or artifacts pertinent to the study. I also delimited the study to IT administrators, for example, chief information officers, chief information security officers, chief security officers, and information technology directors and managers) in central North Carolina IT organizations with 1,000 to 3,000 employees, who had at least 3 years of experience successfully implementing strategies to mitigate data security failure.

I excluded IT administrators who did not have at least 3 years of experience implementing strategies to mitigate data security failure or did not operate in decision-making management roles. Data collection included inviting participants to participate in interviews to share their experiences. Describing participants' experiences regarding phenomena, and analyzing data to understand how participants make sense of their experiences are primary aspects of qualitative inquiry (Osbeck, 2014).

I identified participants for the study by conducting an online search to identify IT technical organizations in central North Carolina. Once I received IRB approval (07-24-18-0074368), I contacted multiple management groups in IT organizations by accessing

email addresses and telephone numbers found on their respective public websites. Ethics in research mandates that researchers outline informed consent, privacy, and protection of participant rights prior to recruiting participants (M. Carey, 2019; Peticca-Harris, DeGama, & Elias, 2016). After participants agreed to participate in the study, I sent each participant a consent form via email. I collected the signed consent forms from participants during interview sessions. I assured participants that I would respect their rights throughout the study and conduct an ethical research project.

The term *gatekeeper* refers to the individual responsible for granting researchers access to interact with study participants (Collings, Grace, & Llewellyn, 2016). Negotiating with gatekeepers to recruit study participants involves identifying and recruiting participants and gaining access to research sites (Collings et al., 2016). To gain access to participants, I requested that managers review a letter from me explaining the scope of the study and grant me access to study participants. Next, I requested that managers compile and forward a list of participants, after which I would send out a call for interested participants.

Once I received IRB approval, I contacted community partners to recruit participants. Upon receiving responses from community partners, I followed up with them by emailing a letter of cooperation (see Appendix B) explaining the rationale for the study and the participant eligibility requirements. I began establishing rapport with community partners by requesting to meet participants in person. I asked participants to respond via telephone, email, or by returning the consent form via fax, email, or U.S. mail to indicate their willingness to participate in the study.

To establish rapport, I contacted participants chosen to participate in the study via email or telephone to thank them for agreeing to participate. I conducted interviews in locations selected by and familiar to study participants. Dempsey, Dowling, Larkin, and Murphy (2016) indicated that researchers must conduct interviews that provide in-depth and meaningful data, while simultaneously making participants feel comfortable discussing confidential data with strangers. I obtained permission from gatekeepers to put up *do not disturb* signs in the designated interview locations to make the areas private and quiet for study participants. Prior to starting interview sessions, I tried to make participants feel comfortable by initiating informal and unassuming reciprocal conversations.

Research Method and Design

The intent of this qualitative multiple case study was to explore the successful strategies IT administrators use to mitigate data security threats and breaches. Because qualitative researchers use case studies to describe how individuals make sense of phenomena (Darawsheh, 2014), the qualitative research method and multiple case study design were suitable to understand how IT administrators understood data security failure. The research and design sections include extensions of the research and design justifications described in Section 1.

Research Method

I selected a qualitative method because the approach was suitable to assess how participants related to data security failure. Researchers use the qualitative method to demonstrate the techniques participants implement to make meaning of a phenomenon

(Belk, 2017), which provides in-depth understanding of participants' performance in response to a phenomenon (Dempsey et al., 2016). Researchers perform qualitative inquiries for three interrelated purposes: (a) exploring a phenomenon, (b) reviewing options to mitigate the phenomenon, and (c) exploring new theories regarding the phenomenon (Lewis, 2015). Because qualitative methods include using open-ended questions (Belk, 2017), researchers have the flexibility to ask probing questions, which allows interviewers to identify participants' perspectives as they occur (Gehman et al., 2018). The responses to the interview questions regarding strategies IT administrators use to mitigate data security threats and breaches provided data to answer the research question.

The scope of the study, and a review of the extant literature, justified using a qualitative method to explore constructs within the study. Information and communication technology (ICT) has expanded users' online access and created limitless business opportunities (Soomro, Shah, & Ahmed, 2016). Conversely, using ICT has also created challenges such as (a) modifications in organizational designs, (b) interruptions in data management systems, (c) technological repercussions, and (d) data security threats (Soomro et al., 2016). Traditionally, IT administrators governed data security management using quantitative methods to discover technological solutions to manage data compromise (Siponen et al., 2014). Researchers and practitioners called for IT professionals to implement qualitative methods to minimize data compromise issues (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; B. Phillips, 2013; Siponen et al., 2014).

Scholars are acknowledging the benefits of qualitative methods in researching IT phenomena. Parsons et al. (2014) applied a qualitative approach to study the relationship between 500 Australian workers' awareness and attitudes toward data security processes and guidelines. The findings revealed that participants responded favorably to data security training that outlined the expectations and rationale of data security guidelines (Parsons et al., 2014).

In another study, B. Phillips (2013) employed a qualitative method to assess how data security procedures influenced IT effectiveness. Responses from IT and audit professionals indicated that when management valued the input of IT professionals' perceptions regarding IT security, the joint effort to mitigate data security failure enhanced IT effectiveness (B. Phillips, 2013). The IT professionals also viewed IT value as a litmus test of IT effectiveness (B. Phillips, 2013).

Siponen et al. (2014) used a qualitative approach to examine employees' propensity to adhere to data security guidelines. The findings indicated that (a) threat appraisal (e.g., perception of threat severity); (b) self-efficacy (e.g., perception of ability to mitigate threat); and (c) response efficacy (e.g., extent that response mitigates threat) influenced employees' propensity to observe data security policies (Siponen et al., 2014). In the current study, I used a qualitative method to explore strategies IT administrators use to successfully mitigate data security threats and breaches in cloud computing.

Researchers use a quantitative method to evaluate data by numerical, scientific, or statistical data analysis (Toye, Williamson, Williams, Fairbank, & Lamb, 2016). Unlike qualitative researchers, quantitative researchers rely on data collected from polls,

questionnaires, and surveys; discussions regarding findings are logical and diagnostic but lack contextual depth (Frels & Onwuegbuzie, 2013). Researchers implement the mixed-methods approach to integrate qualitative and quantitative methods as a means of capitalizing on the advantages and counteracting the disadvantages of both research methods (Starr, 2014).

The objective of the current multiple case study involved exploring strategies IT administrators use to successfully mitigate issues related to data security failure. Because researchers use the qualitative method to obtain in-depth descriptions of participants' experiences with phenomena (Katz, 2015), the qualitative method was suitable for this study. Because the intent of this study was not to conduct an experiment or incorporate statistical data with contextual data, the quantitative and mixed-methods approaches were not appropriate for this study.

Research Design

When using a qualitative research design, researchers make knowledge claims consistent with the constructivist perspective (Garneau & Pepin, 2015), which stipulates that researchers describe phenomena using accounts from the experiences of individual participants (Owen, 2014). An effective research design should answer three questions (Crotty, 1998):

1. What knowledge claims will the researcher identify?
2. What research design will the researcher use to convey these claims?
3. How will the researcher collect and analyze data to report these claims?

Although researchers use the findings in single case study designs to provide rich

and convincing descriptions of phenomena, critics contend that single case studies are limited in scope because the findings lack construct validity and replicability (Cronin, 2014; De Massis & Kotlar, 2014). Alternatively, the multiple case study design allows researchers to offer a robust platform for providing diverse perspectives (Houghton, Casey, Shaw, & Murphy, 2013), as well as building on existing theoretical frameworks (Cronin, 2014). Multiple cases facilitate comparisons that determine whether evolving findings are solely characteristic to a single case or generalizable across multiple cases (Crowe et al., 2011). Therefore, the multiple case study approach was suitable for exploring strategies IT administrators use to mitigate data security threats and breaches.

Because researchers use multiple qualitative research designs to explore phenomena, I considered the phenomenological design wherein researchers examine participants' emotional and social experiences (Gelling, 2015), which was not the intent of this study. I also considered the ethnographic design, which includes examining participants' experiences with social and cultural phenomena (Ryan, 2017; Tumilowicz, Neufeld, & Pelto, 2015), which was not the intent of this study. Researchers use the narrative inquiry and grounded theory designs to examine phenomena from psychological, historical, and cultural perspectives (Bruce, Beuthin, Sheilds, Molzahn, & Schick-Makaroff, 2016; Carey & Griffiths, 2017; Goulding, 2017; Lewis, 2015), which was not the intent of this study.

The qualitative multiple case study design involves using methodological triangulation (Cronin, 2014). Triangulation is a process that includes using multiple data collection techniques to investigate a particular phenomenon with participants at multiple

research sites (Cronin, 2014; Morgan, Pullon, Macdonald, McKinlay, & Gray, 2017). Because researchers also use the multiple case study design to evaluate program or workplace strategies (Yin, 2015), which was the intent of this study, the multiple case study design was suitable for exploring strategies IT administrators use to mitigate data security threats and breaches.

Population and Sampling

The targeted population for this qualitative multiple case study consisted of IT administrators (e.g., chief information officer, chief information security officer, chief security officer, and IT director or manager) at three technology organizations in central North Carolina. The sample consisted of four IT administrators. Participants were required to (a) reside in central North Carolina, (b) have at least 3 years of IT experience implementing strategies to mitigate data threats and breaches, and (c) work at an IT organization with 1,000 to 3,000 employees. I used the purposeful sampling construct to recruit the adequate sample size. Purposeful sampling refers to selecting participants with ample insight pertinent to the focus of the study, which eliminates the need for a large sample size (Malterud, Siersma, & Guassora, 2016; Merriam, 1998).

The justification for implementing the purposeful sampling technique was that researchers use the technique to explore and gain insight, and to select a sample size that offers the most pertinent data pertaining to the phenomenon (Benoot, Hannes, & Bilsen, 2016). Qualitative researchers support purposeful sampling because the core function of the technique involves examining the intricacy of multiple viewpoints as opposed to obtaining a particular ‘correct’ response (Hannes, Booth, Harris, & Noyes, 2013;

Marshall, Cardon, Poddar, & Fontenot, 2013). To delimit a sample size that provided sufficient data to analyze and reach saturation, I specified a sequence of purposeful inclusion and exclusion criteria for the study. The inclusion criteria included attributes that participants had to comply with to participate in the study, while exclusion criteria stipulated attributes that considered participants ineligible to participate in the study.

An insufficient sample size can limit adequate depth and scope, and an overly large sample size could yield superficial or cumbersome amounts of data (Sandelowski, 1995). Stake (1995) indicated that the efficacy of multiple case study research decreases with less than four cases, and studies with more than 10 cases could provide too much data for researchers and readers to process. Yin (2015) posited that five to six cases is sufficient to obtain a high degree of contrasts and generalizations across various cases, which strengthens external validity. I recruited four participants to explore strategies IT administrators use to mitigate data security threats and breaches.

My recruitment practices spanned three IT organizations in central North Carolina to recruit four IT administrators with at least 3 years of experience successfully implementing strategies to mitigate data security failure. Numerous issues (e.g., constructing theories or exploring phenomena to contribute to existing literature) can define sample size in qualitative research (Cleary, Horsfall, & Hayter, 2014). My rationalization for selecting multiple cases was to ensure that data saturation occurred during data analysis.

Data saturation occurs when implementing new data does not enhance the descriptions of the themes or provide any new themes (Morse et al., 2014). Morse (2015)

indicated that the goal in qualitative research is not to saturate facts regarding specific actions pertaining to cases. Rather, the objective is to saturate significant themes that develop because of (a) research questions, (b) interview questions, (c) the purpose of the study, and (d) the conceptual framework that underpins the study (Morse, 2015).

Implementing method triangulation practices helps researchers increase internal validity and answer research questions, as well as achieve data saturation (Santiago-Delefosse, Gavin, Bruchez, Roux, & Stephen, 2016). I assumed that using the multiple case study design and triangulating multiple data sources (e.g., introductory interviews, member checks, field notes, and reviewing organization documents) would lead to data saturation. I also assumed that triangulating multiple data would provide an in-depth depiction of data security failure.

Identifying a sample population involves stipulating inclusion and exclusion criteria for participants (Robinson, 2014). Qualitative researchers must select a sampling approach to (a) describe the population, (b) determine the sample size, (c) select sampling strategies, and (d) obtain access to cases (Robinson, 2014). By implementing all four factors, researchers improve the validity of the research practices and the study findings (Robinson, 2014). Implementing Robinson's 4-point sampling approach was instrumental in recruiting participants for this study.

Ethical Research

Ethics in research becomes apparent because of value clashes (The National Commission, 1978). Researchers describe ethical inconsistencies in ways such as (a) individuals' human rights to confidentiality as opposed to unfair exploitation, (b)

transparency versus privacy, and (c) future wellbeing instead of imminent comfort (The National Commission, 1978). Every assessment made in research links to a possible concession of one belief for another (Watts et al., 2017). Unethical research conduct has consequences such as lack of trust in research findings, as well as lack of trust in the validity of the research (Antes, 2014; Rozmus, Carlin, Polczynski, Spike, & Buday, 2015). To minimize research misconduct, scholars proposed a mandate of ethics training for researchers (e.g., Antes, 2014; Rozmus et al., 2015).

Scholars must strive to minimize threats to participants by predicting and addressing ethical issues from the onset of the research process (Todd et al., 2017), while attempting to capitalize on the quality of collected data (Watts et al., 2017). During data collection, researchers might disclose confidential data. The possible benefits of contributing to best practices in business offset the risks of exposing confidential data (Todd et al., 2017). Heeney (2017) posited that researchers could mitigate research misconduct by collecting and analyzing data objectively, as well as refraining from making value judgements regarding participants' responses.

My approach to maintaining research ethics involved three strategies. First, I completed the National Institute of Health online training modules related to protecting the rights of human participants. Second, I observed the standards indicated in the Belmont Report, which provided guidelines for protecting the rights of vulnerable and underprivileged human research participants. Third, I submitted a research proposal to my committee Chair and Walden University's Internal Review Board (IRB) for numerous critiques and approval.

Upon receiving IRB approval, I conducted semistructured interviews to collect data. Prior to participants agreeing to contribute to this study, I sent participants a consent form Researchers use consent forms to protect recognizable confidential study data from mandatory release (Wolf et al., 2015). Lange, Rogers, and Dodds (2013) indicated that the consent form should include a brief synopsis of the study and a listing of ethical and researcher accountability standards the researcher must practice to ensure participants' confidentiality and wellbeing throughout the study.

Researchers have a responsibility to protect the confidentiality of participants' rights, as well as the data they collect during research (Wolf et al., 2015). I informed prospective participants that participation in the study was voluntary and informed them that they could withdraw from the study without explanation. To prevent perceptions of research misconduct, researchers should not offer remuneration to participants for participating in the study (Heeney, 2017). Because participation in this study was voluntary, I did not provide incentives to participants as compensation for participating in the study.

Data Collection Instruments

The researcher is the primary data collection instrument and assumes multiple roles in the data collection process (Kaczynski et al., 2013; Katz, 2015; Morse et al., 2014; Yin, 2018). Lincoln and Guba (1985) posited that humans are best suited to collect data in qualitative research for six distinct reasons:

1. Humans are receptive to situational cues and capable of interacting with individuals in environments.

2. Humans are capable of collecting multiple sources of data concurrently.
3. Humans are capable of observing situations holistically.
4. Humans are able to interpret data immediately.
5. Humans can deliver prompt feedback and verify data.
6. Humans can explore uncharacteristic or unpredictable phenomena.

Multiple case study methods require researchers to incorporate multiple techniques to collect data and identify parallel themes among the data (Cronin, 2014). Yin (2015) stipulated that case study researchers triangulate six data gathering tools: (a) documents, (b) archival reports, (c) interviews, (d) direct observation, (e) participant observation, and (f) physical artifacts. The data collection instruments I used to triangulate with the interview data were (a) semistructured interviews, (b) an Android tablet to audio record interviews, (c) field notes, (d) a comprehensive literature review, and (e) organization documents (e.g. organization newsletters and data security plans).

Prior to collecting data, the researcher is responsible for identifying a conceptual framework to underpin the study (Katz, 2015). The researcher reviews the extant literature to associate the constructs of the framework with the literature (Yin, 2018). I analyzed and synthesized the extant data security literature to indicate the rationale for conducting semistructured interviews to explore strategies IT administrators in the IT industry use to mitigate data security threats and breaches.

Semistructured interviews are conducive for conducting reciprocal interview sessions (McIntosh & Morse, 2015). I used semistructured interviews because the technique was favorable for implementing open-ended questions, which allowed me to

ask probing questions to obtain more insight regarding data security failure. I used an interview protocol (see Appendix A) to ask questions pertinent to strategies IT administrators use to mitigate data security threats and breaches.

Data Collection Technique

Among the numerous research designs available, selecting the suitable design for a study is contingent upon the research question the researcher intends to answer (Lewis, 2015). Pietkiewicz and Smith (2014) asserted that qualitative methods allow researchers to collect in-depth rich data to answer research questions, which is not attainable by using quantitative data collection techniques. I elected to use the qualitative multiple case study design to explore strategies IT administrators use to mitigate data security threats and breaches in cloud computing.

Case study research develops from using multiple sources of data to accomplish triangulation during data collection and analysis (Yazan, 2015). Yin (2017) suggested that researchers use six data sources: documents, archival records, interviews, direct observations, participant observation, and physical artifacts to collect data. I used (a) semistructured interviews, (b) a comprehensive literature review, (c) organization documents (e.g. organization newsletters and data security plans), and (d) field notes to collect data. Researchers contended that using interview protocols to pose questions regarding similar events helps mitigate bias during triangulation (Fusch & Ness, 2015; Marshall & Rossman, 2016).

An interview protocol is a means of consistently obtaining input from participants and providing in-depth accounts of participants' experiences (Castillo-Montoya, 2016;

Tenório et al., 2017). Applying knowledge acquired from reviewing the extant data security literature, I developed an interview protocol (see Appendix A). The protocol included a script I used to (a) introduce myself, (b) explain the purpose of the study, (c) explain the interview process, and (d) pose identical interview questions to participants, which enhanced the reliability and validity of study findings.

Gatekeepers grant researchers access to interact with study participants (Collings et al., 2016). Negotiating with gatekeepers to recruit study participants involves identifying and recruiting participants and gaining access to research sites (Collings et al., 2016). I identified participants for the study by searching online to identify IT technical organizations in central North Carolina. Once I received IRB approval, I contacted 17 IT managers at 11 IT technical organizations by accessing email addresses and telephone numbers found on managers' respective organization websites.

To gain access to participants, I sent managers consent forms explaining the scope of the study. I requested that managers compile lists of participants. After receiving participant lists, I sent out requests for participants. The sample of respondents who agreed to participate in the study included four IT managers from three IT technical organizations. Ethics in research requires that researchers advise participants regarding informed consent, privacy, and protection of participant rights prior to conducting interviews (Carey, 2019; Peticca-Harris et al., 2016). After participants agreed to participate in the study, I sent each participant a consent form via email. I also informed participants that because participating in the study was voluntary, I would not offer incentives for contributing to the study. Offering incentives and payment for research

participation could be perceived as coercive, and the topic remains debatable among research ethics boards, scholars, and research regulatory agencies (Largent, Emanuel, & Lynch, 2019; Millum & Garnett, 2019). Once participants agreed to the terms of the study, I scheduled interviews. Two days prior to interviews, I sent participants reminder emails.

Semistructured interviews, comprised of open-ended questions, are the standard form of data collection in qualitative research (Marshall & Rossman, 2016; McIntosh & Morse, 2015; Yin, 2018); therefore, I did not conduct a pilot study. The purpose of interviewing participants is not to merely obtain responses to interview questions rather; the intent is to understand how participants make meaning of lived experiences (Seidman, 2013). With participants' permission, I conducted four interviews: two interview sessions at two participants' work sites in private conference rooms, and the remaining two interview sessions occurred at off-site locations elected by participants.

Dempsey et al. (2016) indicated that researchers must conduct interviews that provide in-depth and meaningful data, while simultaneously making participants feel comfortable discussing confidential data with strangers. I began interview sessions by welcoming participants with informal conversation to establish rapport. I reiterated the purpose of the study and reassured participants regarding informed consent guidelines and collected participants' signed consent forms. I asked eight interview questions interjecting probing questions to obtain extended responses. Some common probing errors are (a) asking leading questions, and (b) probing too early in the interview session (Tenório et al., 2017). I actively listened as participants responded to interview questions,

and I refrained from guiding participants' responses. At the conclusion of interview sessions, I thanked participants for contributing to the study and asked them if they had any final comments. I turned off the recorder and informed each participant that I would provide a copy of the interview transcript for member checks to review for accuracy.

Member checking involves requesting participants to check researchers' interpretations of data collected during interviews to determine that researchers depicted participants' responses accurately (Iivari, 2018; Kornbluh, 2015; Madill & Sullivan, 2018). Researchers triangulate field notes compiled during and after interviews (e.g., impressions of participants' reactions to questions, interview settings, and distractions) with participants' responses to enhance data analysis (Korstjens & Moser, 2018; Maharaj, 2016; Phillippi, & Lauderdale, 2018). Combining the advantages of member checking and field notes improves the quality of data analysis (Phillippi, & Lauderdale, 2018). During interview sessions, when necessary, I repeated aspects of participants' initial responses and asked for clarification. I affirmed participants' responses to determine how the interview would proceed. Before transcribing the interview transcripts, I referred to field notes I compiled during and immediately after interviews to reflect on (a) participants' eagerness to reveal candid information regarding data security, (b) participants' preparedness for interview sessions, and (c) participants willingness to provide extended responses to enhance responses to interview questions.

After transcribing interview responses, I emailed participants to invite them to review summaries of their respective interview transcripts. I invited participants to review the interpretations I described as influencing the strategies they implemented to mitigate

data security threats and breaches. I invited participants to indicate whether I had excluded any important details, or if I had misrepresented their responses. I also invited participants to indicate if they agreed with my interpretations by replying within 3 days with corrections to my interpretations if applicable. I stipulated that not responding within 3 days would translate as consent for me to proceed with the research as presented. During member checks, participants could request researchers to revise interview interpretations, as well as provide new data (Kornbluh, 2015; Yin, 2018). I did not receive requests from participants to revise interpretations of interview data or include new data.

Organization documents supplement and validate participants' interview responses (Owen, 2014). I requested that participants provide copies of organization documents prior to scheduled interviews. Reviewing organization documents (e.g., organization newsletters and data security plans) helped me assess IT administrators' (a) data loss prevention procedures, (b) internal and external threat assessment strategies, and (c) data security compliance practices. Researchers enhance the validity and reliability of study findings by triangulating organization documents, transcripts, and audio recordings (Cronin, 2014; Morgan et al., 2017).

When considering a suitable instrument to audio record interviews, researchers should consider factors such as (a) ease of use, (b) cost-effectiveness, and (c) portability (Tarr, Howard, & Stager, 2014; Tilton, 2015). Researchers typically use portable digital recording instruments that have no removable components, which eliminate distracting noises and provide clear interview recordings (Tarr et al., 2014). Handheld digital voice

recorders are slim line and equipped with memory capacity for longer recording time, which makes transcribing data an easier process (Tarr et al., 2014). I considered using my cell phone to record interview sessions; however, the threat of telephone call interruptions would have interfered with participants' ability to remain focused. Budget restraints required that I use a recording device comparable to the standard digital recorder to record interview sessions.

Because of advances in technology, many tablet computers are equipped with software applications capable of performing data collection processes, such as audio recording and transcribing data, which is comparable to digital voice recorders (Tilton, 2015). I used my Android tablet, equipped with a built-in software application, entitled the Voice Recorder, version 1.5.6, to record and transcribe interview data verbatim. I elected to use the tablet to record interviews because the device was accessible, user-friendly, and cost-effective. Tilton (2015) conducted a study to explore how college students were using tablets to replace digital devices to gather and publish research data. Sixty-six percent of the 26 college students indicated that tablets were comparable to digital recorders to prepare for and complete research tasks such as gathering and transcribing data (Tilton, 2015). Tilton's findings revealed that three tablets and software applications in particular were comparable to digital recorders for transcribing voice recordings to textual data: (a) Siri on Apple devices, (b) S-Video on Samsung devices, and (c) Google Voice Recognition on many Android devices. My Android tablet generated clear and understandable audio recordings, and I was able to transcribe interview data to report findings for this study.

Qualitative data collection techniques pose advantages and disadvantages. Conducting semistructured interviews is the standard technique for collecting data in qualitative studies (Oltmann, 2016; Seidman, 2019). Semistructured interviews afford participants the flexibility of providing in-depth explanations regarding phenomena (Oltmann, 2016; Seidman, 2019). Unlike telephone or email interviews, participants tend to stay focused and engaged during face-to-face interviews (Oltmann, 2016; Seidman, 2019). I conducted face-to-face semistructured interviews and the participants demonstrated (a) eagerness to reveal candid information regarding data security, (b) preparedness for interview sessions, and (c) willingness to answer probing questions. The possible disadvantages of face-to-face interviews include participants (a) having scheduling conflicts, (b) feeling uncomfortable discussing sensitive topics and under reporting experiences, (c) perceiving interview sessions as invasive and (d) recanting their decision to participate in the study (Seidman, 2019). The two disadvantages regarding conducting interview sessions for this study were scheduling conflicts and finding participants in a timely manner.

Collecting secondary data, such as organization documents, is essential for substantiation and triangulation in qualitative research (Owen, 2014; Seidman, 2019). Reviewing documents (a) provide information that participants may not reveal during interviews (b) is economical, and (c) is not invasive (Owen, 2014). Two disadvantages of using secondary data are that reviewing documents is time consuming, and participants may not provide documents in a timely manner (Owen, 2014; Seidman, 2019). Participants willing provided organization documents, and I obtained data from

organizations' public websites. The disadvantage for using organization documents in this study was reviewing the documents was time consuming.

Field notes are a recommended form of secondary data in qualitative research (Maharaj, 2016; Phillippi & Lauderdale, 2018). Moreover, field notes are a mechanism for sharing data among researchers for later analysis, and compiling notes is cost-effective (Maharaj, 2016; Phillippi & Lauderdale, 2018). Although field notes are an economical means of collecting secondary data, one disadvantage of using field notes is that data could be lost if researchers neglect to record notes in a timely manner (Maharaj, 2016; Phillippi & Lauderdale, 2018). I made notes during and immediately after interviews to record details regarding interviews (e.g., my reactions to participants' responses and details regarding participants' reactions to interview questions). One disadvantage of using field notes for this study was the process of comparing multiple organization documents with field notes was time consuming. I triangulated participants' responses, organization documents, and field notes to enhance reliability.

Data Organization Technique

Percy, Kostere, and Kostere (2015) recommended applying simple codes to units of data to conceal participants' identity. I assigned alphanumeric codes to participants (e.g., Org1P1, Org2P2, Org2P3, and Org3P4). I used the same alphanumeric coding strategy to categorize organization documents participants provided (e.g., Org1D1, Org2D2, Org2D3, and Org3D4). I compiled a journal of (a) my interpretations of participants' responses, (b) accounts from the literature review, and (c) evaluations of organization documents to categorize themes across all data sources. The purpose of the

journal was to help me acknowledge my preconceived views and judgments throughout the research process. Reflecting on my predetermined thoughts regarding data security failure allowed me to focus on describing participants' perspectives regarding the subject with minimal partiality.

Managing and storing confidential research data can range from manually cataloging and storing paper documents to creating electronic file folders with data software applications (Malagon-Maldonado, 2014). Howard et al. (2017) suggested backing up research databases to a coded external hard drive kept in an inaccessible filing cabinet. All online files were stored on a password-protected laptop and on a flash drive. The files will remain stored in this capacity for 5 years in a locked file cabinet at my home. I will shred and delete research data after 5 years.

Data Analysis

Methodological triangulation is an essential aspect of the data analysis process (Heesen, Bright, & Zucker, 2019; Löwe & Van Kerkhove, 2019; Renz, Carrington, & Badger, 2018). Options for methodological triangulation include (a) conducting interviews, (b) compiling field notes, (c) directly observing participants, and (d) reviewing documents (Renz et al., 2018). Data analysis for this study included triangulating organization newsletters, data security plans, interview transcripts, and field notes. These multiple sources of data required a method of analysis that would give meaning to the strategies IT administrators use to mitigate data security threats and breaches. I analyzed data using Yin's (2018) 5-stage process of analysis: compiling, disassembling, reassembling, interpreting, and concluding.

Compiling

Compiling data involves assembling the data in an organized manner (Castleberry & Nolen, 2018; Yin, 2018). After transcribing interview data, I collated and color coded data in a Word document to compare content. I cross-referenced interview transcripts with field notes and organization documents to substantiate participants' responses to interview questions. Before analyzing the data, I listened to the audio recordings of interviews as I read the hardcopy transcripts. I compared aspects of interview responses with organization documents and field notes, and made corrections as I discovered discrepancies in my interpretations. I completed these steps numerous times throughout data analysis to ensure accuracy. Castleberry and Nolen (2018) asserted that researchers should manage and transcribe data to become familiar with all aspects of the content. After organizing data in a structured format, I disassembled the data to identify similarities and differences.

Disassembling

Disassembling data includes sorting data into categories to identify reoccurring patterns (Mallette & Saldaña, 2019; Yin, 2018). Researchers convert raw data into meaningful groups by dividing data into headings and subheadings (Castleberry and Nolen, 2018; Yin, 2018). I divided data into headings and subheadings by grouping reoccurring words and phrases to construct sentences and paragraphs according to relevance. Color coding the data allowed me to identify similarities and differences and map data into themes expeditiously. Because I coded data throughout the study, once I finalized coding, I compared my early analysis with data that I coded later in the process.

After reviewing the coded groupings of data numerous times, I realized that I had achieved data saturation. Saturation implies that no new themes emerge as researchers analyze new data (Morse, 2015). After identifying codes and themes, I created tables in a Word document to reassemble the data.

Reassembling

Reassembling refers to coding and organizing data into themes and patterns in relation to how the data answers the research question (Braun, Clarke, & Terry, 2019; Yin, 2018). After dividing data into themes, I used a Word document to color code themes into subthemes based on (a) participants' frequency reference to themes, (b) themes' relevance to conceptual framework, and (c) frequency reference to themes in existing literature. Having a visual depiction of theme similarities and differences help researchers manage large datasets, which expedites the theme analysis process (Braun et al., 2019)? After reviewing the clusters of data in tables, I organized data according to three themes: (a) reliance on third party risk assessment services, (b) employee education, and (c) best practices. Using NVivo to graph and chart reoccurring themes helped substantiate thematic analysis and my interpretations.

Interpreting

Interpreting data involves providing analytical conclusions regarding codes and themes that emerged during data analysis (Yin, 2018). Albeit data analysis is a linear process, researchers should begin interpreting data during the compiling, disassembling, and reassembling stages (Yin, 2018). After I coded and reassembled the data, I extracted excerpts from participants' responses, organization documents, and data security

literature. I compared and contrasted the information to interpret how participants perceived data security based on their diverse experiences and data security protocols. I identified themes that related to the to the research question, Yin (2018) posited that researchers' sole focus should not be how many times a theme occurs; rather theme analysis involves verifying collected data are sufficient to answer the research question. Interpretations should be representative of analyzing multiple data sources because interpretations are the foundation for presenting credible conclusions after coding and analyzing data (Yin, 2018).

Concluding

Thematic analysis involves using raw data to identify codes and themes, which help researchers interpret data (Yin, 2018). After analyzing and interpreting data, researchers provide conclusions to answer research questions (Yin, 2018). Qualitative researchers use the anthropological approach, which emphasizes providing a comprehensive and narrative conclusion of data analysis (Castleberry & Nolen, 2018). Qualitative scholars typically follow the case study format with headings and subheadings to present findings (Braun et al., 2019; Castleberry & Nolen, 2018).

I structured the findings section depicting in-depth descriptions with headings and subheadings according to themes that emerged from triangulating multiple sources of data (e.g., interview responses and transcriptions, literature review analysis, field notes, conceptual framework concepts, and organization documents). Presenting the study findings included compiling a comprehensive analysis of emerging themes from all data sources. I incorporated quotes from participants' interview responses and similar

scholars' findings in the literature review to corroborate emerging themes. I triangulated and analyzed participants' interview responses using integrated ERM framework concepts. Because COSO (2004) developed the framework to help IT professionals manage enterprise risks associated with data security, the framework was suitable to underpin my exploration regarding strategies IT administrators use to mitigate data security threats and breaches. I composed and formatted the study following the American Psychological Association guidelines.

Data Analysis Software

Researchers can code, chart, and identify themes manually or scientifically using computer software programs (Phillips & Lu, 2018). NVivo is a qualitative data analysis software that allows researchers to achieve multiple data analysis tasks: (a) identifying themes; (b) coding data; (c) generating reports; and (d) creating visual depictions of data (e.g., word trees, charts, and graphs; Phillips & Lu, 2018). I manually color coded and analyzed emerging themes in a Word document; however, I used NVivo 11.0 to expand the thematic analysis process using graphs and charts to depict participants' frequency reference to themes and subthemes.

Reliability and Validity

Evaluating the trustworthiness of study findings requires researchers to assess the consistency of the study relative to the use and suitability of the chosen research methods and the reliability of the conclusions (Noble & Smith, 2015). Researchers seek to establish credibility, dependability, confirmability, and transferability when defining the legitimacy of qualitative research (Leung, 2015). Qualitative researchers conduct

research on the assumption that researchers collect data to make sense of phenomena by identifying emerging themes, while preserving the reliability and validity of the study findings (Houghton et al., 2013).

Reliability

The objective of reliability in qualitative research is to establish dependability of data collection and reporting practices (Leung, 2015). Considering the diverse standards in qualitative research, evaluating reliability is taxing and counter-intuitive for novice researchers (Leung, 2015). Although studies may differ regarding (a) the scope of the study, (b) the research design, and (c) the research method, a study is reliable when the research methods remain consistent, transparent, and readily available for examination (Houghton et al., 2013). I established reliability by using one interview protocol (see Appendix A) to ask participants the same open-ended questions. I confirmed interpretations of participants' responses by performing member checks during and after interview sessions. Member checking allows interviewees to assess the accuracy of the interpretations of interview responses and request revisions where applicable (Kornbluh, 2015).

Validity

Personal bias and fallible research methods can distort the validity of research findings (Houghton et al., 2013). Bracketing techniques help qualitative researchers identify and mitigate preconceptions, apprehensions, or vulnerabilities regarding phenomena (Ahern, 1999). To avoid inadvertently reflecting my personal biases in the written presentation of the study findings, I acknowledged my personal biases and

assumptions about the phenomenon prior to initiating the research. By exposing personal biases, the researcher gives readers permission to identify with the study findings because the researcher presents the data in a humanistic manner (Houghton et al., 2013). Criteria for confirming research validity includes credibility, confirmability, and transferability (Noble & Smith, 2015).

Credibility, also referred to as trustworthiness, occurs when researchers verify the accuracy of data interpretations by conducting member checks with participants (Houghton et al., 2013). Unlike quantitative researchers who use statistics to establish rigor in research findings (Noble & Smith, 2015), qualitative researchers integrate methodological approaches to confirm the trustworthiness of study findings (Watkinson et al., 2016). Strategies such as (a) identifying personal biases that could influence study findings, (b) recognizing sampling biases, (c) creating a data matrix to compare initial and emerging themes, and (d) maintaining concise and transparent records of all research processes helps the researcher focus on collected data instead of personal biases (Noble & Smith, 2015).

To mitigate bias, I acknowledged possible biases early in the research process. I used one interview protocol (see Appendix A) to collect data from all participants. I also performed member checks during and after interviews to verify that I had accurately interpreted participants' responses.

A second technique that establishes trustworthiness in qualitative research is data replication (Eisenhardt & Graebner, 2007). Data replication enhances credibility in study findings because having multiple forms of data confirms that data are not characteristic of

one specific case (Eisenhardt & Graebner, 2007). Integrating multiple cases in a study sample signifies replication (Watkinson et al., 2016). Researchers can also signify replication by collecting the same data numerous times (Watkinson et al., 2016). Data triangulation is also a notable form of data replication in qualitative research (Kornbluh, 2015). I used multiple data sources (e.g., organization newsletters, data security plans, interview responses, and field notes) to explore strategies IT administrators use to mitigate data breaches.

Confirmability involves using techniques to ensure that study findings and conclusions represent the views and experiences of participants rather than researchers' predisposed views (Houghton et al., 2013). I triangulated data (e.g., interview transcripts, organization documents, and field notes) to establish confirmability. I also used member checking during and after interviews to verify that my interpretations aligned with participants' accounts regarding data security failure

Transferability involves quantitative researchers assessing study findings to determine whether the results are generalizable across other environments or samples (Elo et al., 2014). Quantitative researchers use large random groups to improve the generalizability of statistical conclusions (Morse et al., 2014). Although generalizability is never the objective in qualitative research (Elo et al., 2014), transferability can occur when researchers achieve data saturation, which indicates that participants provided no new data (Morse et al., 2014). Contrary to Morse et al.'s assertion, Elo et al. (2014) posited that qualitative researchers should present findings in a manner that future researchers could determine if findings were transferable.

Transition and Summary

In Section 2, I discussed the processes I used to ensure that I conducted this study in an ethical manner. I also expanded on the data collection techniques and instruments, as well as the anticipated approaches I used to analyze and organize the data. I explained the criteria I used to establish reliability and validity of the study findings. The impetus for initiating this qualitative multiple case study was to explore strategies IT administrators use to mitigate data threats and breaches. The sample for the study included four IT administrators employed at three IT organizations in central North Carolina. One implication for social change derived from implementing strategies to reduce the effects of data threats and breaches on individuals, organizations, and community members. Data collection included (a) conducting semistructured interviews, (b) reviewing organization documents, and (c) compiling field notes.

Section 3 begins with a restatement of the purpose of the study. The remaining segments of Section 3 include data interpretations, data analysis, and a depiction of themes in relation to the conceptual framework constructs. Section 3 also includes (a) applications to professional practice, (b) implications for social change, (c) recommendations for future action, and (d) study conclusions. The conclusion of Section 3 contains recommendations for future research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore strategies IT administrators use to mitigate data security threats and breaches in cloud computing. The target population consisted of four IT administrators at three IT organizations who (a) employed 1,000 to 3,000 employees, (b) were employed in organizations in central North Carolina, and (c) had successfully implemented strategies to mitigate data security threats and breaches in cloud computing. The conceptual framework for this study was the integrated ERM framework. I triangulated organization documents (e.g., organization newsletters and data security plans), participant interview responses, and field notes to answer the research question. The three themes that emerged were (a) reliance on third-party risk management services, (b) employee education, and (c) best practices. My analysis of the data revealed strategies IT administrators use to successfully mitigate data security threats and breaches in cloud computing.

Presentation of the Findings

The central research question for this study was the following: What strategies do IT administrators use to mitigate data security threats and breaches in cloud computing? I reviewed organization documents, compiled field notes, and conducted semistructured face-to-face interviews to collect data. I achieved data saturation once the interview responses and organization documents I examined generated repetitive information, thereby providing no new data.

After collecting and analyzing data, I gained a better understanding of the

significance of implementing strategies to mitigate data security threats and breaches in cloud computing. Participants provided relevant strategies for assessing data security risks and vulnerabilities. Although this study is not a definitive guide to minimizing losses caused by data security susceptibilities (e.g., identity theft, humiliation, economic and emotional damages), IT administrators and business leaders can form alliances to use the emergent theme and subtheme strategies to improve data security best practices to create a competitive advantage in business operations and IT functions.

The emergent themes and subthemes in this study aligned with the integrated ERM framework. COSO (2004), which consists of a group of administrators from five private institutions, developed the integrated ERM framework to identify regulations and frameworks pertaining to ERM, internal controls, and IT fraud prevention. The constructs included in the integrated ERM framework are a combination of elements focused on (a) risk identification, (b) risk assessment, (c) risk management, (d) risk awareness, (e) information sharing, (f) employee training, and (g) communication across divisions, which function to guide IT administrators' and organization leaders' decision-making regarding managing data security risks (COSO, 2004). Analysis of the data in the current study revealed that key words such as *training*, *risk assessment*, *third-party vendors*, and *best practices* emerged in all three themes and subthemes. Table 1 depicts the ERM framework and themes.

Table 1

Integrated Framework

Framework concepts	Theme 1 Reliance on third-party vendors	Theme 2 Employee education	Theme 3 Best practices
Internal environment			
Objective setting			Best practices
Event identification	Task force		
Risk assessment	Risk assessment		
Risk response	Third-party expertise	Information sharing	
Control activities		Information sharing	Employee training
Information and Communication		Communication	Limited user access
Monitoring	Monitoring		Two-factor authentication

Theme 1: Reliance on Third-Party Vendors for Risk Management Services

The first emergent theme was reliance on third-party vendors for risk management services. The emergent subthemes for Theme 1 were (a) data security expertise, (b) risk assessment, and (c) monitoring. I analyzed data security plans, organization newsletters, and participant interview responses to describe strategies IT administrators use to mitigate data security threats and breaches. Figure 2 illustrates Theme 1 and the emergent subthemes.

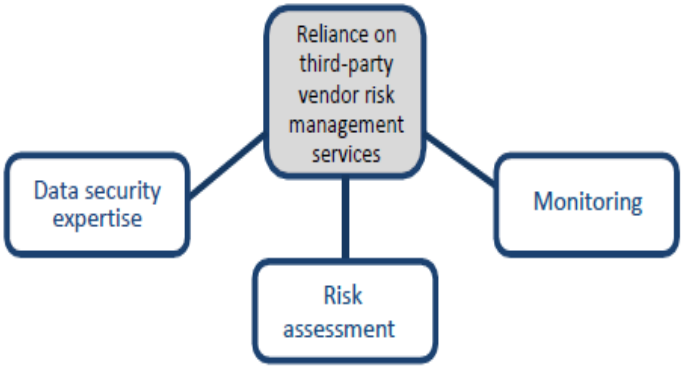

Figure 2. Theme 1 and emergent subthemes.

Data security expertise. Review of Org1P1, Org2P2, Org2P3, and Org3P4's security plans and interview responses revealed that all participants rely on the expertise of third-party vendors to provide risk management services to enhance data security practices. Org1P1 stated,

> We partner with third-party vendors and we have contracts with three major vendors, so we keep up-to-date with all the latest software updates. We have also hired third-party hackers to keep abreast with the latest data security issues out there. Software hackers are proactive and companies are usually reactive. We hire hackers to try to be proactive by keeping up with the latest data security issues, which makes us proactive just like potential hackers. By doing this, we learn hackers strategies so we work to stop events before they happen.

Org2P2 remarked,

> Because we are handling security from a third-party approach, we rely heavily on third-party training and expertise. We collaborate with our third-party vendors to alert us of updates and possible threats and concerns. Our service providers are

more up-to-date and we rely on them for constant notifications and assessments. Org2P3 commented,

> We rely on third-party vendor expertise to help us identify and assess our systems and make sure we are up-to-date on data security concerns. We don't have the resources to do large scale security things, but we rely on our partnerships with third-party partners.

Review of Org3P4's security plan revealed that Org3 also relies on the expertise of third-party vendors for multi-cloud management services to provide management of cloud servers, operating systems, applications, and the entire cloud ecosystem. Org3P4 stated, "We use cloud computing services such as SaaS to secure data integrity." Review of Org3P4's security plan also revealed that IT administrators rely on the SaaS computer service because of the scalability of the software, which means the software is safe for use during increases in users, work capacity, or data transactions without added cost to the organization because the vendor owns the cloud environment. Org3 rents the software, which minimizes the organization's responsibility for managing the upkeep of the service.

Risk assessment. Analysis of Org1P1, Org2P2, Org2P3, and Org3P4's security plans and interview responses indicated that all administrators rely on third-party vendors to assist with establishing ongoing risk assessment practices to protect their IT infrastructures. Org2P3 commented, "The most convenient way to prevent threats and breaches is to have frequent backups, monitor systems, and perform frequent system assessments." Review of Org2 P2 and Org2P3's security plan revealed that Org2 relies

on a third-party vendor to run vulnerability scans and reviews and provide vulnerability assessment reports.

Review of Org3P4's security plan indicated that Org3 collaborates with a security solutions group that performs network system tests, evaluations, and vulnerability assessments. Org3's plan also revealed that the security group helped Org3's IT administrators develop a systems test and evaluation plan. Org1P1's security plan and interview responses indicated that Org1 has stringent internal and third-party risk assessment strategies in place to assess users' access and system vulnerabilities. Org1P1 commented,

> Not to brag about our company, but we don't have careless incidents because our security constraints are so tight and so strict, that before an individual can access a program, it goes through certain protocols where I, as the engineer manager, or the engineer director can see what that individual is trying to access. We can decide if they need that kind of permission or if they don't.

One of the eight constructs of the integrated ERM framework is risk assessment. Risk assessment includes evaluating, predicting, and categorizing risks based on significance (COSO, 2004). Reducing risks involves implementing assessment strategies to minimize the likelihood of risks occurring (Kholidy et al., 2016). Table 2 depicts elements of all organizations' security plans.

Table 2

Elements of Organizations' Security Plans

	Org1	Org2	Org3
Communication	X	X	X
Employee training	X	X	X
Internal task force			X
Monitoring	X	X	X
Risk assessment	X	X	X
Third-party vendor	X	X	X
Threat research lab			X

Monitoring. Review of Org3P4's security plan revealed that IT administrators established a threat research lab, which consists of a task force to monitor internal and external users' access to networks. The task force monitors network communication and Internet traffic to help IT administrators identify suspicious activity. The task force's daily duties include (a) monitoring system events; (b) monitoring command and control servers; (c) monitoring and responding to suspicious activity; and (d) monitoring NetFlow (origination, destination, and volume of network traffic flow).

Org1P1 stated,

> In our IT area, there's cameras everywhere and we monitor everything. We have what's called footprint software where we can track your keystrokes so

> we know what the individual is looking at and we have a program that picks up on key words that are typed. In the IT field, certain keywords will bring up a red flag so we use that to keep our security pretty tight. It's a learning curve and a learning experience so we are always growing.

Although Org2P2 and Org2P3 work at the same organization, they supervise two separate divisions within the organization. Org2P2 and OrgP3 had varying viewpoints regarding how monitoring systems helps mitigate threats and breaches. Org2P2 stated, "The most convenient way to prevent threats and breaches is to have frequent backups, monitor systems, and perform frequent system assessments." Org2P3 commented, "A lot of what we do is we identify what a user's workflow is, methods they're using to access their data, and if they're following company protocol." Org2P3 focuses on monitoring users' access patterns on systems, whereas Org2P2 emphasizes monitoring systems to identify risk vulnerabilities to mitigate threats and breaches.

The findings in Theme 1 depicted three of the eight elements of the ERM integrated framework: event identification, risk assessment, and monitoring (see Table 1). The results substantiate Dreyfuss and Giat's (2018) and Kalaimannan and Gupta's (2017) conclusions that risk assessment and monitoring are effective strategies to evaluate security risks and provide an added level of systems reinforcement, which allows system owners to address emerging internal vulnerabilities as they occur rather than after external attacks occur. Org2P2 stated, "The most convenient way to prevent threats and breaches is to have frequent backups, monitor systems, and perform frequent system

assessments." This finding contradicts Meszaros and Buchalcevova's (2017) assumption that monitoring is time consuming and ineffective as a strategy to assess and manage risks. All participants' responses support COSO's (2004) deduction that risk assessment and monitoring help IT administrators evaluate, predict, and categorize risks based on significance.

All participants erred on the side of caution and obtained third-party risk assessment services to enhance data security practices. Org2P2 remarked,

> Because we are handling security from a third-party approach, we rely heavily on third-party training and expertise. We collaborate with our third-party vendors to alert us of updates and possible threats and concerns. Our service providers are more up-to-date and we rely on them for constant notifications and assessments.

Org2P3 commented,

> We rely on third-party vendor expertise to help us identify and assess our systems and make sure we are up-to-date on data security concerns. We don't have the resources to do large-scale security things, but we rely on our partnerships with third-party partners.

These results support Schulz et al.'s (2016) assertion that some IT administrators lack the expertise to perform risk assessments. These findings also substantiate Al-Musawi et al.'s (2015) deduction that obtaining the expertise of third-party risks assessment services helps IT and business administrators identify disruptive events.

Administrators in one organization formed an internal task force to identify risks. This finding supports the integrated ERM framework's event identification element,

which indicates that establishing an internal task force to identify internal and external events that might interrupt business performance helps reinforce data security processes (COSO, 2004). The event identification element also elaborates on Almgren's (2014) conclusion that event identification and risk assessment help IT administrators and organization leaders perceive risk events as opportunities to increase their risk management awareness. Because communication among stakeholders during crises may be complex, establishing risk assessment standards early may help stakeholders understand their roles in mitigating risks prior to data security crises. Figure 3 depicts data analysis results for participants' frequency reference to Theme 1.

Figure 3. Participants' frequency reference to Theme 1.

Theme 2: Employee Education

Org1P1, Org2P2, Org2P3, and Org3P4's interview responses indicated that all participants advocate implementing effective communication and information sharing programs to educate employees and organization leaders' regarding mitigating data

security threats and breaches. Org2P2 commented, “Awareness is first in mitigating data security issues. Sizing up the user’s level of awareness and their ability to leverage security tools is important. Next, I think coaching and training is key.”

Org2P3 remarked,

> One physical data security protocol we use is making sure that users log off systems daily and appropriately and that the user complies with company protocol regarding locking down and accessing systems. I think the biggest thing in any kind of data environment where you have multiple people accessing the data you want to keep is providing user education. That’s gotta be the biggest thing in security in general. You can lock systems down all day, but if you have users that can access systems but don’t know how to lock down systems and keep systems secure on their end, it doesn’t matter how good IT administrators are, you will still have problems because users don’t know how to keep systems secure on their end.

Org2P3 also commented on education from the perspective of educating organization leaders. Org2P3 further commented,

> Trying to educate the business side of the house about the importance of spending the appropriate amount of dollars to ensure that we have the necessary infrastructure to have the necessary data security protocols in place is a large part of what I do in the client relationship side of the house. So often, the business side is looking at dollars and cents; whereas the IT side is looking at having what we need to make sure, our data are secure. The IT department educates the business

> side to help them see that aligning what they want to keep safe with the bottom line is the only way that the organization is going to function properly. Without this kind of alignment, things won't work. We try to make them see the benefit of having the right security plan in place and what it will cost the organization if there is a breach; therefore, we try to make them see the benefit of IT and business working together.

Org1P1 commented on education from the perspective of collaborating with coworkers. Org1P1 stated,

> We have a status meeting every morning at 10:00 and during that meeting, it's like a round table. We go around the table and every engineer has to give us an update on any project or any particular concern they might have. We don't digress to the next person until we have thoroughly digested that person's problem, so it keeps everybody on the same page.

Review of Org3P4's organization newsletter indicated that Org3 has a strong presence in the community for providing ongoing data security education and awareness initiatives to make remote users knowledgeable about accessing the organization's systems. A quote from Org3P4's organization newsletter revealed,

> Aside from these flagship programs, our employees work hard every day to make a difference in their local communities, from offering tours of our network and security operations facilities to students to hosting cryptography clinics, cybersecurity super hero programs, and hackathons. To learn more about what

you can do to help educate future generations for a career in cybersecurity, follow the conversation online.

Figure 4 illustrates Theme 2 and the emergent subthemes.

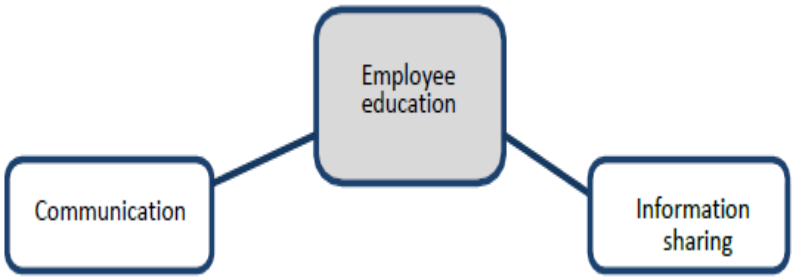

Figure 4. Theme 2 and the emergent subthemes.

Communication. Review of interview responses indicated that all administrators emphasized using effective communication strategies to make individuals accountable for identifying and responding to data security practices. Org2P2 remarked,

> For the most part, in-house conversations are the most genuine way to communicate regarding data security. For instance, if there was a breaking security issue, we're gonna broadcast the event every way possible. We're not gonna wait for our monthly newsletter to go out every two weeks, we're gonna hit our social media accounts and make it public and give users the nuts and bolts to educate them immediately." We rely heavily on communication to keep users informed regarding best practices. Our communication is timely and with authority.

All administrators agreed that ongoing communication is essential to make sure all divisions in organizations stay informed regarding data security practices. Org2P3 responded,

> We do user education quite a bit. When we see a potential risk, we use the opportunity to teach our people as a whole instead of one single person. We have education on how to recognize suspect emails and areas that might permit remote users to access our systems inappropriately. We let inside users know what to look for, how to read what they see, and how to handle what they identify.

Review of Org3P4's security plan revealed that Org3 implemented a comprehensive set of communication initiatives called *Unified Communications and Collaboration Services* by collaborating with third-party vendors to promote secure communications and teamwork activities across divisions. Org3's security plan also revealed that the reason for adopting third-party communication services was to:

> (a) enhance employee engagement and accelerate problem solving, (b) jump-start productivity, (c) protect against cyberattacks and reduce the risk of disruption, (d) deliver a common collaborative experience that people love, (e) rely on vendor's technology expertise and relationships to improve IT agility, and (f) spend more time on the bottom line.

Org1P1 was adamant about IT administrators and business executives communicating to develop strategies to align data security practices with organizational objectives. Org1P1 reiterated, "When we have our status meeting every day at 10:00, it includes business and IT. When both parties are at the table, we can address situations and be better informed."

Information sharing. Review of Org2P2 and Org2P3's security plan and interview responses revealed that Org2 relied on third-party vendors' expertise to help educate staff and share security information across divisions regarding strategies to mitigate data security threats and breaches. Review of Org2's organization newsletter revealed that administrators actively engaged community partners to educate remote users regarding data security.

Org2P3 commented,

> Once we identify a potential for a weakness, we share that concern with users and parties involved in the vulnerability and we go into damage control mode. We find a way to stop the potential risks, inform the necessary party or division of the potential risk, and let them know there is a threat. We partner with third-party vendors to help us educate others regarding potential risks.

Review of one of Org2P2's organization newsletters indicated that Org2 collaborated with three third-party vendors to initiate social change by sharing information to surrounding communities through interactive training sessions, webinars, and monthly newsletters highlighting recent IT and data security topics. Regional magazines have supported Org2's information sharing practices through a range of awareness initiatives (e.g., IT think tank seminars and IT leadership podcasts) to provide continuing publicity regarding the significance of implementing strategies to mitigate data security vulnerabilities. Org2P2 stated, "Our role as IT service providers is to create awareness. Education is key."

Review of Org3P4's security plan revealed that Org3 relied on a third-party

vendor to provide a service called *Webex Meetings*, which allows IT administrators and users to get together to collaborate onsite or remotely. Vendors manage the technology, which makes it possible for IT administrators to concentrate on what matters most – implementing and sharing strategies across divisions in the organization to respond promptly to internal and external data security vulnerabilities without interruptions in business operations. Org3P4's security plan also revealed that administrators viewed virtual communication as an effective way to keep all parties involved in communication regarding data security practices. Org3P4 commented, "Notify the proper people and take action to prevent breaches in the future." Org1P1 commented, "We address situations at our everyday status meeting and everyone is better informed."

The results in Theme 2 included two of the ERM integrated framework's eight elements (information and communication, and risk response; see Table 1). The findings revealed strategies IT administrators use to communicate across divisions to manage data security risks. Review of Org3P4's security plan revealed that IT administrators established a threat research lab to monitor system events and internal and external users' access to networks and respond to suspicious activity. This finding refutes Schulz et al.'s (2016) assertion that event assessments are ineffective because criteria for classifying disruptive events are vague, and IT administrators often lack the expertise to perform risk assessments. By contrast, this result substantiates Al-Musawi et al.'s (2015) implication that creating workspaces to track system event patterns that cause potential risks help IT

and business administrators identify and respond to events that disrupt business performance.

Theme 2 findings included a combination of strategies that elaborated on the integrated framework elements information sharing and communication as strategies IT administrators use to mitigate data security threats and breaches. Review of interview responses indicated that all administrators emphasized using effective communication strategies to educate users and disseminate information across divisions to make individuals accountable for identifying and responding to data security practices. Org2P2 remarked,

> For the most part, in-house conversations are the most genuine way to communicate regarding data security. For instance, if there was a breaking security issue, we're gonna broadcast the event every way possible. We rely heavily on communication to keep users informed regarding best practices. Our communication is timely and with authority.

This strategy aligns with COSO's (2004) conclusion that distributing information across divisions helps IT administrators to educate members regarding data security practices so they can perform their respective responsibilities. Review of one of Org2P2's organization newsletters indicated that Org2 collaborated with three third-party vendors to initiate social change by sharing information to surrounding communities through interactive training sessions, webinars, and think tank seminars and IT leadership podcasts to provide publicity regarding data security. Org2P2 stated, "Our role as IT service providers is to create awareness. Education is key." These strategies elaborated on

Kitchin and Dodge's (2019) assumption that obtaining community input regarding security strategies allows IT administrators to implement security strategies that provide the best economic utility, which minimizes risks to organizational performance and sustainability and enhances community relations. These findings also support Rae et al.'s (2017) implication that open communication and obtaining regular external feedback are effective risk assessment strategies. Information sharing, communication, and education strategies help IT administrators evaluate the sources of internal and external information to confirm that data is an accurate account of business objectives and IT operations (COSO, 2004; Pham et al., 2017). Figure 5 indicates data analysis results for participants' frequency reference to Theme 2.

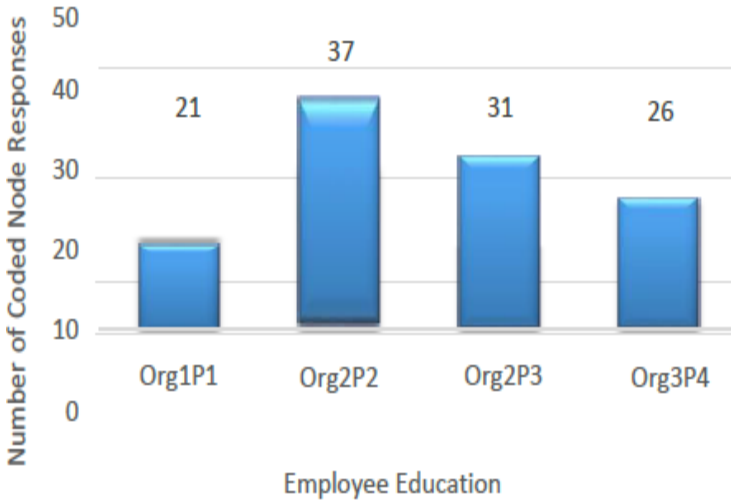

Figure 5. Participants' frequency reference to Theme 2.

Theme 3: Best Practices

Org2P2 remarked,

> Businesses declare best practices but users don't; however, it is helpful for users to understand what best practices are and how to maintain a balance between

security and appropriately using software to make sure systems remain safe. Everything goes back to best practices. Being able to identify what is a big red flag and knowing what to look for is key to security. Scalability of security practices is the key to setting up best practices that protect systems. Knowing what data security approaches work best for your organization is the best way to set up best practices that work best. Figure 6 illustrates Theme 3 and the emergent subthemes.

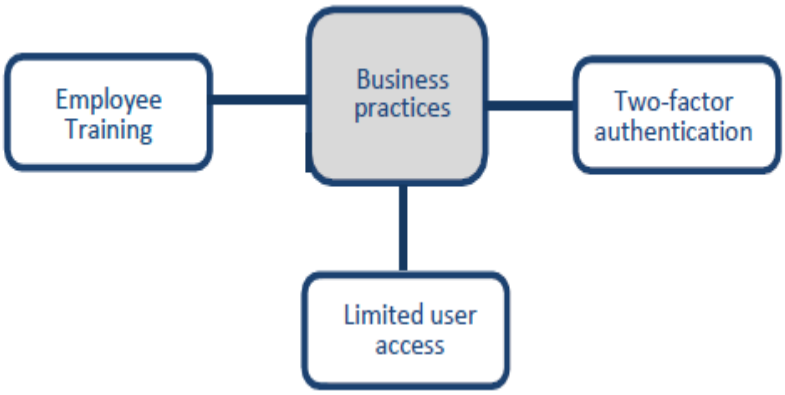

Figure 6. Theme 3 and the emergent subthemes.

Employee training. Review of Org2P2 and Org2P3's security policy revealed that Org3 provides a *personal direct approach* to training for remote users. The policy revealed that Org3 implemented a one-on-one training alternative to help remote users learn how to properly access Org3's network servers and mitigate data security concerns in their respective organizations. Org3 frequently recommends that users attend one-on-one training sessions after attending public workshop training sessions. Org2P2 commented,

When you're talking about effective data security, education is the key thing.

> You can have all the strategies and plans in place to help with data security, but if you have people that don't know how to use the strategies, you're still at risk for breaches in your security measures. That's why education and training is so important. Users need to know what they're clicking on, who they're communicating with online, and how they're allowing outside users to access our systems. At the end of the day, education is the only way to ensure that data security is effective. You're only as safe as your least educated user when it comes to data security.

Org2P3 remarked,

> One of the main things that help us create a strategy about security is that we have to weigh the balance between security and convenience. There are a couple of strategies that I have adopted but even those come with their own burden if the end user doesn't know how to use the software. We use two third-party password managers; however, the software can offer the moon, but if the end user doesn't know how to navigate the software, there is still the risk of having enabled security that the user doesn't understand. We aim to offer consultation periods that are tailored to consulting users and making them feel comfortable using software securely. Once they find that we offer training that makes them feel comfortable, we can present solutions that help keep systems secure. The key to successful training is knowing how the conversation should go when you talk to different users. We assess users' knowledge level, which helps us know how to train users regarding data

security.

To improve individuals' awareness of the organization's business objectives and IT functions, Org1 approached training from the perspective of cross training. Org1P1 remarked,

> We have cross training. If we don't have cross training and someone wants to take off, who's gonna fill that spot. We have cross training and we cross train very thoroughly. We have what is known as periodic on the job training classes. We setup a small enterprise network in a user acceptance testing (UAT) offline environment and conduct various network penetration tactics. We also invite our vendors to send their engineers onsite here to further enhance our training knowledge base. The training accomplishes several goals:
>
> - identifies network vulnerabilities,
> - identifies the weak areas of each engineer,
> - identifies the strong areas of each engineer,
> - tests the new fixes/software patches,
> - expands the engineer(s) knowledge base, and
> - creates proprietary software.

UAT testing refers to the final steps of the software-testing phase (Scherr, Elberzhager, & Holl, 2018). During UAT testing, vendors employ actual software users to test software applications to make certain customers can use the software to achieve necessary tasks in their respective organizations (Scherr et al., 2018).

Org1P1's security plan revealed that Org1 relied on third-party vendors to customize software applications to meet their security software specifications and training needs.

Org3P4 commented, "Training is done by the organization, in-house. We have training classes on data security and the training is online videos about data security." Review of Org3P4's security policy regarding training processes indicated that Org3 has a rigorous training program. The program entails offering security consultations that provide users direct access to the resources, administrators' expertise, and best practices they need to reinforce data security and compliance. Org3's policy revealed that the lists of training consultation services include:

- best-in-class methodologies and practices for addressing security risks;
- a team of experienced security experts and thought leaders with an average of 18 years of experience;
- a complete family of services that span the full security lifecycle—from assessments to full implementation;
- flexible, vendor-agnostic solutions that make the most of organizations' current security and compliance investments; and
- deep industry understanding and ongoing expertise through memberships in ISO, ISACA, ISSA, IEEE and CSI.

Review of Org3's organization newsletter also revealed that Org3 received recognition as a finalist for the Leading Lights Award, an award given to commend IT organizations and their executives for exceptional accomplishments in "next-

generation communications technology, applications, services, strategies, and innovation." Org3's training practices could increase IT administrators' capacity to (a) proactively recognize and mitigate data threats and breaches, and (b) align IT functions with organizational objectives to sustain competitive advantage.

Limited user access. Review of study participants' interview responses indicated that all participants advocated limiting users' access to sensitive data as an effective best practice to mitigate data security threats and breaches. Org2P2 stated,

> We limit access to certain systems based on users' profile and security rights. Not everybody has access to all areas of systems. Once we realize users have inappropriately used their access rights, their rights are removed immediately. We assess our systems and users' access rights so we will know where to draw the line between open access and security.

Org3P4 remarked, "Limit users' access and have a good fire wall protection from outside threats. Make sure to change passwords and make them very difficult to crack to limit users' access to data." Review of Org2P3's security plan revealed that IT administrators deny remote users access to Org2's networks when remote users' WiFi router addresses are not on specified media access control (MAC) lists and fail to authenticate with Org2's preferred Wi-Fi network protocols.

Org1P1 commented,

> Internally, the best strategy is limit the user access, limit the access of certain parties, be it engineers, be it the IT professional, be it the, you know, software engineers so that they can only access certain areas. We strengthen

> our protocol as far as how many people can access certain things. We set a limit as far as your duration on the server, plus the allotted space that you can use on the server. In doing that, that keeps a person limited if they're trying to download a file. They can't download it because they only have a certain amount of space. Depending on the individual, we'll know what files he'll be using, so we make sure his access space or rights on the server is less than the file he'll need so therefore, the file can never be accessed unless they get added security rights.

Two-factor authentication. Review of Org2P2, Org2P3, and Org3P4's security plan revealed that remote users must complete a two-factor authentication process to access systems; yet, Org1P1's security plan revealed that users must complete a 3-step authentication process before and after gaining access to systems. Review of OrgP2 and Org2P3's security plan revealed that IT administrators encouraged internal and external users to use two-factor authentication. Additionally, the plan indicated that Org2 administrators emphasized to users that two-factor authentication can help keep accounts and data safe from hackers. Org2's security plan indicated that administrators promoted using a personal identification number that administrators sent to users via an email, SMS, or app. Two-factor authentication can protect against stolen passwords and prevent an external person from accessing systems and accounts. Ussatova, Nyssanbayeva, and Wojcik (2019) asserted that multifactored-authentication improves security and validating users' rights to access confidential data.

Review of Org1P1's security plan revealed that IT administrators authenticated remote users' identity by using a third-party 3-step access protocol during the time users initially access servers and periodically after users have signed off systems. Org1 administrators authenticated users' access based on a shared protocol, such as users' passwords. Org1P1 noted,

> The main strategy is we use our servers and we have what's called host servers and protocol servers. So, when you access our network you don't access one server. You go through what's called our security server, which leads you to our data server that transfers you to whatever server you need. We have what's called parallel hosts, and we have those in place so by the time you get to the third server, which is all the data, you have been authenticated with a process called CHAP, challenge handshake authentication protocol.

Review of Org1P1's security plan indicated that IT administrators authenticated remote users' identity by using CHAP, a three-factor authentication process that includes the (a) administrator sending a challenge message to the respective user, (b) user responding using a predetermined encrypted code, and (c) administrator verifying the response against the encrypted code. If there is a discrepancy during the authentication process, the administrator denies the user access to Org1's systems. Org1's administrator then sends the user a new challenge code at random recesses and repeats the 3-step process, which provides the user another opportunity to complete the three-factor authentication process. Org3P4 remarked, "Enable two-factor authentication by encrypting data and having a

24/7 security monitoring service and advanced firewall technology.” Figure 7 depicts participants’ frequency reference to Theme 3.

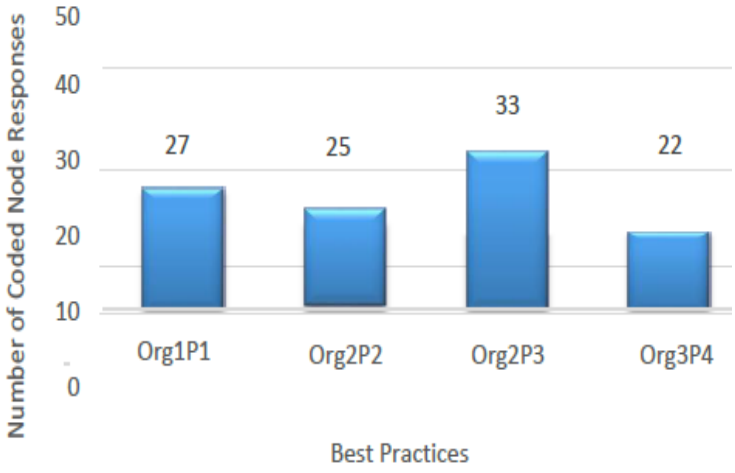

Figure 7. Participants’ frequency reference to Theme 3.

The findings in Theme 3 were characteristic of two of the eight elements of the ERM integrated framework (objective setting and control activities; see Table 1). The interview responses indicated that business leaders developed set objectives to create best practices to identify potential risks and disruptions to business performance. Org2P2 remarked,

> Businesses declare best practices but users don’t; however, it is helpful for users to understand what best practices are and how to maintain a balance between security and appropriately using software to make sure systems remain safe. Everything goes back to best practices. Being able to identify what is a big red flag and knowing what to look for is key to security. Scalability of security practices is the key to setting up best practices that protect systems. Knowing what data security approaches work best for your organization is the best way to

set up best practices that work best.

This finding supports Chen et al.'s (2014) conclusion that best practices must be user-friendly enough that users can integrate and interpret the guidelines to identify potential security threats in the workplace. Org2P2 commented, "We rely heavily on communication to keep users informed regarding best practices. Our communication is timely and with authority." This strategy substantiates NIST's (2018) conclusion that risk management involves implementing best practices that provide a controlled basis for exploring and communicating security controls across divisions to alleviate threats and risks in data security. Review of Org3P4's security policy revealed that Org3 established best practices to reinforce data security compliance by obtaining memberships in ISO, ISACA, ISSA, IEEE and CSI, international administrations that collaborate with organizations to help them develop product and technology standards. This result elaborates on Lee et al.'s (2015) implication that organization leaders are reliant on multiple security standards to remain compliant with federal, state, and local regulations to avoid compliance penalties. Developing these types of best practices support practitioners and researchers call for organization leaders to establish mandatory polices to align business objectives with IT practices to create business value (Coltman et al., 2015 & Reynolds & Yetton, 2015). These findings are relevant to improving data security best practices because the identified strategies may increase IT administrators' and organization leaders' capacity to set objectives that align IT functions with organizational objectives to sustain competitive advantage.

Review of interview responses in Theme 3 also provided indications that all

participants use control activities, which are guidelines and processes that indicate how IT administrators and organization leaders use preventive controls to secure confidential data. The emerging control activities in Theme 3 were employee training, limited user access, and encrypted passwords (See Table 1). Review of Org2P2 and Org2P3's security policy revealed that Org3 provided one-on-one training to help remote users learn how to properly access Org3's network servers and mitigate data security concerns. Org3 recommended that users attend one-on-one training sessions after attending public workshop training sessions. Org2P2 commented,

> When you're talking about effective data security, education is the key thing. You can have all the strategies and plans in place to help with data security, but if you have people that don't know how to use the strategies, you're still at risk for breaches in your security measures. That's why education and training is so important.

To improve individuals' awareness of the organization's business objectives and IT functions, Org1 approached training from the perspective of cross training. These findings substantiate Parson's (2014) deduction that participants respond favorably to data security training that outlines the expectations and rationale of data security guidelines. These findings also elaborate on Al-Musawi et al.'s (2015) implication that improving staff awareness by providing data security training is an effective strategy to prevent data security failure in cloud environments.

All administrators enforced limited user access and two-factor authentication as preventive controls to restrict users' access to confidential data. Org2P2 stated, "We limit

access to certain systems based on users' profile and security rights. Not everybody has access to all areas of systems. Once we realize users have inappropriately used their access rights, their rights are removed immediately." Org3P4 remarked, "Limit users' access and have a good fire wall protection from outside threats. Make sure to change passwords and make them very difficult to crack to limit users' access to data." These findings support Mendelson and Mendelson's (2017) implication that (a) keeping accurate records of users' data use and (b) limiting access to live data provides control activities to improve data security. These findings also elaborate on COSO's (2004) perspective that organization leaders who combine risk-centered prevention planning and control processes to mitigate risk, as opposed to focusing on decreasing risk costs, achieve higher business value (COSO, 2004).

Review of Org1P1's security plan indicated that IT administrators authenticated remote users' identity by using a three-factor authentication (also known as multifactored authentication) process that includes the (a) administrator sending a challenge message to the respective user, (b) user responding using a predetermined encrypted code, and (c) administrator verifying the response against the encrypted code. Review of Org2P2, Org2P3, and Org3P4's security plan also revealed that remote users must complete a two-factor authentication process to access systems. These findings support Ussatova et al.'s (2019) assumption that multifactored-authentication strategies improves security and validating users' rights to access confidential data. Finally, these findings support COSO's (2004) deduction that two-factor authentication is a control activity that IT administrators use to provide users data security approvals. Two-factor authentication

could help IT administrators level the weaknesses of typical password protection.

Applications to Professional Practice

Extensive review of scholarly literature, as well as exploring the constructs of the conceptual framework, provided a comprehensive discussion regarding how IT administrators can effectively apply the findings of this study to implement strategies to mitigate data security threats and breaches in cloud computing. The findings in this study are relevant to improving data security best practices because the identified strategies may increase IT administrators' and organization leaders' capacity to align IT functions with organizational objectives to sustain competitive advantage. Strategic IT alignment (SITA) improves organization performance (Sabherwal, Sabherwal, Havakhor, & Steelman, 2019). SITA was ranked among the top three IT management concerns from 2003 to 2014 (Kappelman, McLean, Johnson, & Gerhart, 2014).

After analyzing data security plans, organization newsletters, and participants' interview responses, three themes emerged, the first theme that emerged was reliance on third-party risk management services. The emergent subthemes within Theme 1 were (a) data security expertise, (b) risk assessment, and (c) monitoring. The range of discussion regarding Theme 1 and the corresponding subthemes substantiated the integrated ERM framework constructs, which leaders use to implement effective ERM practices to identify, assess, and monitor events that disrupt business continuity.

The next emergent theme, employee education, emerged based on two subthemes, communication and information sharing. The elements within Theme 2 may help IT administrators establish the basis for collaboration, engaged leadership,

and accountability across divisions in organizations. Establishing a system of awareness consistent with IT and business requirements may help administrators develop a system of accountability to identify individuals responsible for securing, distributing, and using data in organizations (Ahmed & Litchford, 2018; Al-Ruithe et al., 2018).

The practices regarding handling and collecting information in organizations have implications for privacy, accessibility, and reliability of data (Cobb et al., 2018). Establishing best practices to secure data should be a shared process between IT administrators and organization leaders (Cobb et al., 2018). Theme 3 strategies and the corresponding subthemes may help IT administrators enhance data security best practices and improve security responsiveness for individuals with diverse levels of security awareness in organizations. Collaborating to identify security options that will improve individuals' perceptions regarding data security helps to improve risk management in organizations (Cobb et al., 2018).

Implications for Social Change

Approximately 81% of all data compromises occur because of identity theft (Chou, 2016). One implication for social change involves implementing strategies to reduce the effects of data threats and breaches among individuals, organizations, and community members, which could improve the views of data security before and after crises occur. Subsequent implications for social change include (a) fewer compromises of individuals' personal information, (b) reduced financial risks for organizations, and (c) reduced financial loss for individuals and communities.

A final implication of positive social change involves IT administrators using the three emergent strategies in this study to adopt what Kitchin and Dodge (2019) refer to as "security-by-design" (SBD) security standards. Practitioners use the SBD approach to engage community members to provide input regarding establishing proactive rather than reactive security strategies (Kitchin & Dodge, 2019). Identifying SBD best practices allow IT administrators to implement security strategies that provide the best economic utility (e.g., the ability of a product or service to meet the needs of consumers), which minimizes risks to organizational performance and sustainability and enhances community relations

Recommendations for Action

The objective of this qualitative multiple case study involved exploring strategies IT administrators use to successfully mitigate issues related to data security failure. Cloud computing has changed the IT infrastructure of U.S. organizations, generating new threats and breaches in data security (Kumar et al., 2018; Nazim & Ashgher, 2015). Economists estimated the total costs from data security breaches at approximately $8.5 billion yearly (Romanosky, 2016). IT administrators should perform risk assessments in traditional and cloud computing environments to evaluate and mitigate security risks. Organization leaders should allocate funding for data security, and establish best practices that help curtail the billions of dollars in lost revenue the public incurs annually from data threats and breaches (Atoum et al., 2014).

The basis for this research study included synthesizing scholarly literature,

transcribing and interpreting IT administrators' interview responses, and reviewing administrators' security plans and organization newsletters. The data I obtained provided sufficient information to answer the research question. After triangulation all sources of data, I was able to achieve saturation during data analysis.

The three themes that emerged were (a) reliance on third-party risk management services, (b) employee education, and (c) best practices. My analysis of the findings identified successful strategies IT administrators use to mitigate data security threats and breaches in cloud computing. The findings may motivate IT and business administrators to collaborate to mitigate data security failure.

Based on the findings in this study, I recommend that IT administrators and organization leaders collaborate to facilitate the following actions to implement strategies for sustained data security best practices:

1. Provide the necessary data security training to help all stakeholders in organizations identify, assess, and respond to data vulnerabilities to maintain business operations before, during, and after data security attacks.
2. Communicate and share relevant risk management information to divisions across organizations to make individuals accountable for identifying, responding to, and monitoring risks.
3. Evaluate the skills of IT administrators to determine it is necessary to leverage the expertise of third-party vendors.
4. Limit authorized users' access to sensitive data, based on users' security clearance.

5. Mandate multifactor authentication for access to network systems.

I plan to disseminate the findings and recommendations for action from this study by offering to provide the IT administrators in this study with fact-finding summary sheets. I will also facilitate workshops and seminars to share my study findings. I will volunteer to discuss the findings of this study at IT conferences, academic institutions, and organizations in surrounding communities. Finally, I plan to disseminate my research findings by publishing articles in industry and academic journals.

Recommendations for Further Research

The findings in this study may serve as a resource to help IT administrators develop best practices to mitigate data security threats and breaches in cloud computing environments. Because this study was limited to a sample size of four IT administrators, I recommend that future researchers increase the sample size to determine if the study findings are transferable to a larger population. I delimited my research scope to administrators in IT organizations in central North Carolina with 1,000 to 3,000 employees. I recommend that future researchers collect responses from IT professionals in larger and different types of organizations in other geographical settings to determine whether the findings will be similar or vary. This study was also limited by using the qualitative multiple case study design. I recommend that future researchers use the quantitative or mixed-methods study designs to (a) determine IT administrators' data security success and error rates, and (b) determine whether the findings will vary or remain constant.

One limitation I observed throughout this study occurred while trying to identify participants who were willing to contribute to the study. Some participants agreed to participant and later recanted their consent, which made the recruiting process an arduous task, as well as prolonged the time I spent recruiting study participants. Once I obtained an eligible sample size, I was able to collect sufficient data to analyze and complete this study. I recommend that future researchers consider allocating ample time to identify eligible study participants.

Reflections

Completing the doctoral program was undoubtedly one of the most challenging and rewarding feats, I have ever attempted. I have expanded my knowledge regarding identifying strategies to mitigate data security threats and breaches. I feel that I can confidently apply my knowledge to make recommendations to organization leaders regarding strategies to successfully assess, identify, and mitigate data security vulnerabilities. The findings in this study may contribute to existing IT data security literature, as well as provide future recommendations regarding best practices IT administrators use to mitigate data security threats and breaches in cloud computing.

The impetus for selecting my study topic stemmed from my preconceived notion that some IT administrators lacked strategies to address data security threats and breaches in cloud computing. However, all participants in this study discredited my biased perspective by providing security plans, organization newsletters, and interview responses to substantiate their expertise in implementing data security best practices to mitigate data security threats and breaches. I assumed participants would provide open

and pertinent responses to the interview questions; and I was careful not to ask leading questions, react to responses, or ask probing questions too early. I feel confident the study participants provided honest answers.

Conclusion

The purpose of this qualitative multiple case study was to explore strategies IT administrators use to mitigate data security threats and breaches in cloud computing. The knowledge gained from the study findings can potentially transform the way IT administrators and organization leaders establish and adopt best practices to mitigate data security vulnerabilities. Three core themes emerged from the research findings, which correlated with the literature review, the existing IT security literature, and the integrated ERM framework. Review of security plans, organization newsletters, and interview responses revealed that IT administrators (a) rely on third-party risk management services, (b) share information and communicate with individuals across divisions in organizations to educate users regarding data security practices, and (c) implement best practices to provide training to enhance individuals' data security expertise.

IT administrators and organization leaders must collaborate to implement strategies to reduce the effects of data security failure on individuals and communities, which can improve perceptions of data security before and after crises occur. The increased and ongoing phenomenon of data security threats and breaches in organizations requires IT administrators and organization leaders to develop and implement best practices suitable for (a) ensuring fewer compromises of

individuals' personal information, (b) reducing financial risks for organizations, and (c) reducing financial loss for individuals and community members.

References

Ahern, K. (1999). Ten tips for reflexive bracketing. *Qualitative Health Research, 9*(3), 407-411. doi:10.1177/104973239900900309

Ahmad, A., Maynard, S., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370. doi:10.1007/s10845-012-0683-0

Ahmed, M., & Litchford, A. T. (2018). Taxonomy for identification of security issues in cloud computing environments. *Journal of Computer Information Systems, 58*(1), 79-88. doi:10.1080/08874417.2016.11925

Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L., & Côté, I. (2015). A pattern-based 100 and tool-supported risk analysis method compliant to ISO 27001 for cloud systems. *International Journal of Secure Software Engineering, 6*(1), 24-46. doi:10.4018/ijsse.2015010102

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

Almgren, K. (2014). Implementing C)S) ERM framework to mitigate cloud computing business challenges. *International Journal of Business and Social Science, 5*(9), 71-76. Retrieved from http://ijbssnet.com/

Al-Musawi, F., Al-Badi, A. H., & Ali, S. (2015, September). A road map to risk management framework for successful implementation of cloud computing in Oman. In Intelligent Networking and Collaborative Systems (INCOS), 2015

International Conference on Intelligent Networking and Collaborative Systems (pp. 417-422). IEEE. doi:10.1109/INCoS.2015.80

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). Data governance taxonomy: Cloud versus non-cloud. *Sustainability, 10*(1), 1-26. doi:10.3390/su100100951

Antes, A. L. (2014). A systematic approach to instruction in research ethics. *Accountability in Research, 21*(1), 50-67. doi:10.1080/08989621.2013.822269

Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security, 22*(2014), 251-264. doi:10.1108/IMCS-02-2013-0014

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1-13. doi:10.1016/j.ejor.2015.12.023

Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, *12*(2014), 529-534. doi:10.1016/j.protcy.2013.12.525

Bajaj, S., & Sion, R. (2014). TrustedDB: A trusted hardware-based database with privacy and data confidentiality. *IEEE Transactions on Knowledge and Data Engineering, 26*(3), 752-765. doi:10.1109/TKDE.2013.38

Balasubramanian, V., & Mala, T. (2015). A review on various data security issues in cloud computing environment and its solutions. *ARPN Journal of Engineering and Applied Sciences, 10*(2), 883-889. Retrieved from http://www.arpnjournals.com/

Belk, R. W. (2017). Qualitative research in advertising. *Journal of Advertising, 46*(1), 36-47. doi:10.1080/00913367.2016.1201025

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*(C), 51-61. doi:10.1016/j.chb.2015.01.039

Benedek, P. (2016). Compliance issues in higher education. *Practice and Theory in Systems of Education, 10*(1), 55-61. doi:10.1515/ptse-2016-0008

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology, 16*(1), 21-33. doi:10.1186/s12874-016-0114-6

Bernstein, P. L. (1996). *Against the gods: The remarkable story of risk*. New York, NY: John Wiley & Sons.

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019). *Thematic analysis. Handbook of research methods in health social sciences*. Singapore: Springer.

Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management, 33*(5), 726-733. doi:10.1016/j.ijinfomgt.2013.05.004.

Bruce, A., Beuthin, R., Sheilds, L., Molzahn, A., & Schick-Makaroff, K. (2016). Narrative research evolving: Evolving through narrative research. *International Journal of Qualitative Methods, 15*(1), 1-6. doi:10.1177/1609406916659292

Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., & Toosi, A. N. (2019). A manifesto for future generation cloud computing: Research directions for the next decade. *ACM Computing Surveys (CSUR), 51*(5), 105-156. doi:10.1145/3241737

Caniëls, M. C., Lenaerts, H. K., & Gelderman, C. J. (2015). Explaining the internet usage of SMEs: The impact of market orientation, behavioral norms, motivation and technology acceptance. *Internet Research, 25*(3), 358-377. doi:10.1108/IntR-12013-0266

Carcary, M., Doherty, E., & Conway, G. (2014). The adoption of cloud computing by Irish SMEs: An exploratory study. *Electronic Journal of Information Systems Evaluation, 17*(1), 3-14. Retrieved from www.ejise.com

Carey, E., & Griffiths, C. (2017). Recruitment and consent of adults with intellectual disabilities in a classic grounded theory research study: ethical and methodological considerations. *Disability & Society, 32*(2), 193-212. doi:10.1080/09687599.2017.1281793

Carey, M. (2019). The tyranny of ethics? Political challenges and tensions when applying ethical governance to qualitative social work research. *Ethics and Social Welfare, 13*(2), 150-162. doi:10.1080/17496535.2018.1548630

Castka, P., & Corbett, C. J. (2015). Management systems standards: Diffusion, impact and governance of ISO 9000, ISO 14000, and other management standards. Foundations and Trends (R) in Technology, *Information, and Operations Management, 7*(3-4), 161-379. doi:10.1561/0200000042

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning, 10*(6), 807-815. doi:10.1016/j.cptl.2018.03.019

Chan, Z. C., Fung, Y., & Chien, W. (2013). Bracketing in phenomenology: Only undertaken in the data collection and analysis process. *The Qualitative Report, 18*(30), 1-9. Retrieved from http://nsuworks.nova.edu/tqr/

Chen, Y., Dong, F., & Chen, H. (2016). Business process and information security: A cross-listing perspective. *Journal of Industrial Integration and Management, 1*(2), 1-16. doi:10.1142/S2424862216500093

Chen, Y. H., Lin, T. P., & Yen, D. C. (2014). How to facilitate inter-organizational knowledge sharing: The impact of trust. *Information & Management, 51*(5), 568-578. doi:10.1016/j.im.2014.03.007

Chen, Y. S., Lin, C. K., & Chuang, H. M. (2016). Closing the skill gap of cloud CRM application services in cloud computing for evaluating big data solutions. ISPRS *International Journal of Geo-Information, 5*(12), 227- 247. doi:10.3390/ijgi5120227

Choi, J. Y., Choi, E. J., & Kim, M. J. (2014). A comparison study between cloud service assessment programs and ISO/IEC 27001:2013. *Journal of Digital Convergence, 12*(1), 405-414. doi:10.14400/JDPM.2014.12.1.405

Chou, J. C. (2016). "Cybersecurity, identity theft, and standing law: A framework for data breaches using substantial risk in a post-clapper world." *American University*

National Security Law Brief, 7(1), 120-181. Retrieved from http://digitalcommons.wcl.american.edu/nslb/

Chu, C. K., Chow, S. S., Tzeng, W. G., Zhou, J., & Deng, R. H. (2014). Key-aggregate cryptosystem for scalable data sharing in cloud storage. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 468-477. doi:10.1109/TPDS.2013.112

Cioca, L., & Ivascu, L. (2014). IT technology implications analysis on the occupational risk: Cloud computing architecture. *Procedia Technology, 16(*2014), 1548-1559. doi:10.1016/j.protcy.2014.10.177

Claydon, L. S. (2015). Rigor in quantitative research. *Nursing Standard, 29*(47), 43-48. doi:10.7748/ns.29.31.44.e8681

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing*, *70*(3), 473-475. doi:10.1111/jan.12163

Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., & Kohno, T. (2018). Computer security for data collection technologies. *Development Engineering, 3*(2018), 1-11. doi:10.1016/j.deveng.2017.12.002

Colesca, S. E. (2015). Understanding trust in e-government. *Engineering Economics, 63*(4), 1392-2785. Retrieved from http://www.inzeko.ktu.lt/index.php/EE

Collings, S., Grace, R., & Llewellyn, G. (2016). Negotiating with gatekeepers in research with disadvantaged children: A case study of children of mothers with intellectual disability. *Children & Society*, *30*(6), 499-509. doi:10.1111/chso.12163

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. *Journal of Information Technology, 30*(2), 91-100. doi:10.1057/jit.2014.35

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *COSO enterprise risk management for cloud computing.* Retrieved from http://www.coso.org/

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *COSO enterprise risk management for cloud computing.* Retrieved from http://www.coso.org/

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Thousand Oaks, CA: Sage.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology, 11*(1), 100-109. doi:10.1186/1471-2288-11-100

Darawsheh, W. (2014). Reflexivity in research: Promoting rigor, reliability and validity in qualitative research. *International Journal of Therapy & Rehabilitation, 21*(12), 560-568. doi:10.12968/ijtr.2014.21.12.560

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy, 5*(1), 5-29. doi:10.1016/j.jfbs.2014.01.007

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive interviewing in qualitative research. *Research in Nurse & Health, 39*(6), 480-490. doi:10.1002/nur.21743

Department of Networked Systems and Services (DNSS). (2016). Introduction to IT security. Retrieved from http://www.crysys.hu/education

DeSouza, E., & Valverde, R. (2016). Reducing security incidents in a Canadian PHIPA regulated environment with an employee-based risk management strategy. *Journal of Theoretical and Applied Information Technology, 90*(2), 197-208. Retrieved from www.jatit.org

Dillon, S., & Vossen, G. (2015). SaaS cloud computing in small and medium enterprises: A comparison between Germany and New Zealand. *International Journal of Information Technology, Communications, and Convergence, 3*(2), 87-104. doi:10.1504/IJITCC.2015.070998

Dreyfuss, M., & Giat, Y. (2018). A risk management model for an academic institution's information system. *Information Resources Management Journal (IRMJ) 31*(1), 83-96. doi:10.4018/IRMJ.2018010104

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cyber Security, 2*(1), 3-14, doi:10.1093/cybsec/tyw003

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25-32. doi:10.5465/AMJ.2007.24160888

Elgammal, A., Turetken, O., Van den Heuvel, W. J., & Papazoglou, M. (2016). Formalizing and applying compliance patterns for business process compliance. *Software & Systems Modeling, 15*(1), 119-146. doi:10.1007/s10270-014-0395-3

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *The Journal of Systems and Software, 118*(1), 64-84. doi:10.1016/j.jss.2016.04.061

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

Ernst & Young. (2013). Under cyber-attack: EY's global information security survey 2013. Retrieved from http://www.ey.com/Publication/

Fetterman, D. M. (1994). Empowerment evaluation. *Evaluation Practice, 15*(1), 1-15. doi:10.1016/0886-1633(94)90055-8

Frazer, L. (2016). Internal control: Is it a benefit or fad to small companies? A literature dependency perspective. *Journal of Accounting and Finance, 16*(4), 149-161. Retrieved from http://www.na-businesspress.com/jafopen.html

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling and Development, 91*(2), 184–194. doi:10.1002/j.1556-6676.2013.00085.x

Fung, P. H. (2016). A tool to map applications to information technology deployment models. *Journal of Management of Roraima, 6*(1), 114-127. doi:10.18227/2237-8057rarr.v6i1.3233

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/tqr/

Gardner, P. & Johnson, S. (2015). Teaching the pursuit of assumptions. *Journal of Philosophy of Education, 49*(4), 557-570. Retrieved from www.philosophy-of-education.org/publications/jope.html

Garneau, A. B., & Pepin, J. (2015). Cultural competence: A constructivist definition. *Journal of Transcultural Nursing*, *26*(1), 9-15. doi:10.1177/1043659614541294

Geertz, C. (1975). *The interpretation of cultures*. Chicago, IL: Chicago University.

Gehman, J., Glaser, V. L., Eisenhardt, K. M., Gioia, D., Langley, A., & Corley, K. G. (2018). Finding theory–method fit: A comparison of three qualitative approaches to theory building. *Journal of Management Inquiry*, *27*(3), 284-300. doi:10.1177/1056492617706029

Gelling, L. (2015). Qualitative research. *Nursing Standard, 29*(30), 43-47. doi:10.7748/ns.29.30.43.e9749

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

Gordon, A. (2016). The hybrid cloud security professional. *IEEE Cloud Computing, 3*(1), 82-86. doi:10.1109/MCC.2016.21

Goulding, C. (2017). "Navigating the complexities of grounded theory research in advertising." *Journal of Advertising, 46*(1), 61-70.

doi:10.1080/00913367.2017.1281775

Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher, 2*(6), 34-38. doi:10.7748/nr.21.6.34.e1252

Greene, M. J. (2015). On the inside looking in: Methodological insights and challenges in conducting qualitative insider research. *The Qualitative Report, 19*(29), 1-13. Retrieved from http://nsuworks.nova.edu/tqr/

Hadden, J. M., & Mahdy, A. M. (2016). The royal split paradigm: Real-time data fragmentation and distributed networks for data loss prevention. *International Journal of Computer Science and Security (IJCSS), 10*(3), 107-119. Retrieved from http://www.cscjournals.org/journals/IJCSS/

Hannes, K., Booth, A., Harris, J., & Noyes, J. (2013). Celebrating methodological challenges and changes: Reflecting on the emergence and importance of the role of qualitative evidence in Cochrane reviews. *Systematic Reviews, 2*(1), 1-10. doi:10.1186/2046-4053-2-84

Hansson, S. O., & Aven, T. (2014). Is risk analysis scientific? *Risk Analysis, 34* (7), 1173-1183. doi:10.1111/risa.12230

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16. doi:10.1080/10580530.2015.1117842

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

Hassan, M. M., Lin, K., Yue, X., & Wan, J. (2017). A multimedia healthcare data sharing approach through cloud-based body area network. *Future Generation Computer Systems, 66*(2017), 48-58. doi:10.1016/j.future.2015.12.016

Hatefi, M., & Fasanghari, M. (2015). A DEA-based approach for information technology risk assessment through risk information technology framework. *The International Arab Journal of Information Technology, 13*(1), 51-58. Retrieved from http://ccis2k.org/iajit/

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

Heeney, C. (2017). An "ethical moment" in data sharing. *Science, Technology, & Human Values, 42*(1), 3-28. doi:10.1177/0162243916648220

Heesen, R., Bright, L. K., & Zucker, A. (2019). Vindicating methodological triangulation. *Synthese, 196*(8), 3067-3081. doi:10.1007/s11229-016-1294-7

Holtfreter, R. E., & Harrington, A. (2014). Towards a model for data breaches: A universal problem for the public. *International Journal of Public Information Systems, 10(1), 40-58. Retrieved from http://www.ijpis.net/*

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. doi:10.1016/j.bushor.2016.07.004

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

Howard, A. A., Hirsch-Moverman, Y., Saito, S., Gadisa, T., Daftary, A., & Melaku, Z. (2017). The ENRICH study to evaluate the effectiveness of a combination intervention package to improve isoniazid preventive therapy initiation, adherence and completion among people living with HIV in Ethiopia: Rationale and design of a mixed methods cluster randomized trial. *Contemporary Clinical Trials Communications, 6*(2017), 46-54. doi:10.1016/j.conctc.2017.03.001

Hussein, N. H., & Khalid, A. (2016). A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security, 14*(1), 52-56. Retrieved from https://sites.google.com/site/ijcsis/

Ibrahimovic, S., & Franke, U. (2017). A probabilistic approach to IT risk management in the Basel regulatory framework: A case study. *Journal of Financial Regulation and Compliance, 25*(2), 176-195. doi:10.1108/JFRC-06-2016-0050

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Journal of Information and Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People, 31*(1), 111-133. doi:10.1108/ITP-07-2016-0168:

Ika, L., & Saint-Macary, J. (2014). Special issues: Why do projects fail in Africa? *Journal of African Business, 15*(3), 151-155. doi:10.1080/15228916.2014.956635

Information Systems Audit and Control Association (ISACA). (2012). Risk IT framework. Retrieved from http://www.isaca.org

International Organization for Standardization. (ISO). (2014). *ISO/IEC 27000:2009.* Retrieved from www.iso.org

International Trade Administration. (2016). A cloud computing top markets report (Report No. 2016 IT). Washington, D.C. ITA.

Islam, M., & Rahaman, M. (2016). A review on multiple survey report of cloud adoption and its major barriers in the perspective of Bangladesh. *International Journal of Computer Network and Information Security, 8*(5), 42-47. doi:10.5815/ijcnis.2016.05.06

Islam, S., Fenz, S., Weippl, E., & Kalloniatis, C. (2016). Migration goals and risk management in cloud computing: A review of state of the art and survey results on practitioners. *International Journal of Secure Software Engineering (IJSSE), 7*(3), 44-73. doi:10.4018/IJSSE.2016070103

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behavior & Information Technology, 35*(5), 368-379. doi:10.1080/0144929X.2016.1160287

Joos, P., Piotroski, J. D., & Srinivasan, S. (2016). Can analysts assess fundamental risk and valuation uncertainty? An empirical analysis of scenario-based value estimates. *Journal of Financial Economics, 121*(3), 645-663. doi:10.1016/j.jfineco.2016.05.003

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*(2014), 489-496. doi:10.1016/j.procs.2014.05.452

Kabbedijk, J., Bezemer, C. P., Jansen, S., & Zaidman, A. (2015). Defining multi-tenancy: A systematic mapping study on the academic and the industrial perspective. *Journal of Systems and Software, 100*(1), 139-148. doi:10.1016/j.jss.2014.10.034

Kaczynski, D., Salmona, M., & Smith, T. (2013). Qualitative research in finance. *Australian Journal of Management, 39*(1), 127-135. doi:10.1177/0312896212469611

Kalaimannan, E., & Gupta, J. N. (2017). The security development lifecycle in the context of accreditation policies and standards. *IEEE Security & Privacy*, *15*(1), 52-57. doi:10.1109/MSP.2017.14

Kappelman, L., McLean, E., Johnson, V., & Gerhart, N. (2014). "The 2014 SIM IT key issues and trends study." *MIS Quarterly Executive, 13*(4), 237-263. Retrieved from https://cdn.ymaws.com/www.simnet.org/resource/collection/7A70D436-28BA-4E88-B958-C86941C704C3/2014_MISQE_Article_with_Appendix.pdf

Kappelman, L., McLean, E., Luftman, J., & Johnson, V. (2013). Key issues of IT organizations and their leadership: The 2013 SIM IT trends study. *MIS Quarterly Executive 12*(4), 227-240. Retrieved from http://www.misqe.org

Katz, J. (2015). A theory of qualitative methodology: The social system of analytic fieldwork. *Méthod (e) s: African Review of Social Sciences Methodology, 1*(1-2), 131-146. doi:10.1080/23754745.2015.1017282

Katz, J., Saadon-Grosmana, N., & Arzya, S. (2017). The life review experience: Qualitative and quantitative characteristics. *Consciousness and Cognition, 48*(2017), 76-86. doi:10.1016/j.concog.2016.10.011

Kholidy, H. A., Erradi, A., Abdelwahed, S., & Baiardi, F. (2016). A risk mitigation approach for autonomous cloud intrusion response system. *Computing, 98*(11), 1111-1135. doi:10.1007/s00607-016-0495-8

Kim, K. K., Browe, D. K., Logan, H. C., Holm, R., Hack, L., & Ohno-Machado, L. (2014). Data governance requirements for distributed clinical research networks: Triangulating perspectives of diverse stakeholders. *Journal of the American Medical Informatics Association, 21*(4), 714-719. doi:10.1136/amiajnl-2013-002308

Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology, 26*(2), 47-65. doi:10.1080/10630732.2019.1594698

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology, 12*(4), 397-414. doi:10.1080/14780887.2015.1021941

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124. doi:10.1080/13814788.2017.1375092

Kude, T., Hoehle, H., & Sykes, A. (2017). "Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation." *International Journal of Operations & Production Management, 37*(1), 56-74. doi:10.1108/IJOPM-03-2015-0156

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science, 125*(2018), 691-697. doi:10.1016/j.procs.2017.12.089

Kumarga, N. P., & Sireesha, D. (2014). Ensuring data integrity in cloud computing. *International Journal of Computer Science and Network Security (IJCSNS), 14*(9), 34-38. Retrieved from http://ijcsns.org /

Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud computing: From scarcity to abundance. *Journal of Industry, Competition, and Trade, 15*(1), 5-19. doi:10.1007/s10842-014-0188-y

Lal, P., & Bharadwaj, S. S. (2016). "Preliminary insight into cloud computing adoption in a developing country." *Journal of Enterprise Information Management, 29*(4), *505*-524. doi:10.1108/JEIM-09-2014-0094

Lange, M. M., Rogers, W., & Dodds, S. (2013). Vulnerability in research ethics: A way forward. *Bioethics, 27*(6), 333–340. doi:10.1111/bioe.12032

Largent, E. A., Emanuel, E. J., & Lynch, H. F. (2019). Filthy lucre or fitting offer? Understanding worries about payments to research participants. *The American Journal of Bioethics, 19*(9), 1-4. doi:10.1080/15265161.2019.1631076

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational

information security. *Information Systems Research, 27*(1), 70-86. doi:10.1287/isre.2015.0607

Lee, K., Park, C., & Yang, H. D. (2015). Development of a cloud computing interoperability-based service certification. *International Journal of Security and ITS Applications, 9*(20), 11-20. doi:10.14257/ijsia.2015.9.12.02

Lee, Y. C. (2019). Adoption intention of cloud computing at the firm level. *Journal of Computer Information Systems*, *59*(1), 61-72. doi:10.1080/08874417.2017.1295792

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research, planning and design* (11th ed.). Boston, MA: Pearson.

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

Levitt, H. M., Motulsky, S. L., Wertz, F. J., Morrow, S. L., & Ponterotto, J. G. (2017). Recommendations for designing and reviewing qualitative research in psychology: Promoting methodological integrity. *Qualitative Psychology, 4*(1), 2-22. doi:10.1037/qup0000082

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

Li, A., Li, X., Pan, Y., & Zhang, W. (2015). Strategies for network security. *Science China Information Sciences, 58*(1), 1-14. doi:10.1007/s11432-014-5182-9

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* (Vol. 75). Newbury Park, CA: Sage.

Liu, S., & Wang, L. (2014). Understanding the impact of risks on performance in internal and outsourced information technology projects: The role of strategic importance. *International Journal of Project Management, 32*(8), 1494-1510. doi:10.1016/j.ijproman.2014.01.012

Lohrke, F. T., Frownfelter-Lohrke, C., & Ketchen, D. J. (2016). Organizational performance: The role of information technology systems in the performance of mergers and acquisitions. *Business Horizons, 59*(1), 7-12. doi:10.1016/j.bushor.2015.09.006

Löwe, B., & Van Kerkhove, B. (2019). *Methodological triangulation in empirical philosophy of mathematics: Advances in experimental philosophy of logic and mathematics.* London, United Kingdom: Bloomsbury.

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology, 5*(3), 321-339. doi:10.1037/qup0000089

Maharaj, N. (2016). Using field notes to facilitate critical reflection. *Reflective Practice, 17*(2), 114-124. doi:10.1080/14623943.2015.1134472

Malagon-Maldonado, G. (2014). Qualitative research in health design. *HERD: Health Environments Research & Design Journal, 7*(4), 120-134. doi:10.1177/193758671400700411

Mallette, L. A., & Saldaña, J. (2019). Teaching qualitative data analysis through gaming. *Qualitative Inquiry, 25*(9-10), 1085-1090. doi:10.1177/1077800418789458

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research*, *26*(13) 1753-1760. doi:10.1177/1049732315617444

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

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

Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 1*(1), 1-21. doi:10.1007/s11747-016-0495-4

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems, 39*(1), 1-8. doi:10.1007/s10916-014-0181-3

Mathur, N., & Purohit, R. (2017). Issues and challenges in convergence of big data, cloud and data science. *International Journal of Computer Applications, 160*(9), 7-12. Retrieved from http://www.ijcaonline.org/

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

doi:10.1177/2333393615597674

Meidell, A., & Kaarboe, K. (2017). How the enterprise risk management function influences decision-making in the organization–A field study of a large, global oil and gas company. *The British Accounting Review*, *49*(1), 39-55. doi:10.1016/j.bar.2016.10.005

Mendelson, D., & Mendelson, D. (2017). "Legal protections for personal health information in the age of big data: A proposal for regulatory framework." *Ethics, Medicine and Public Health, 3(1),* 37-55. doi:10.1016/j.jemep.2017.02.005

Merriam, B. S. (1998). *Qualitative research and case study applications in education: Revised and expanded from" case study research in education.* San Francisco, CA: Jossey-Bass.

Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security, 65*,(2017), 300-313. doi:10.1016/j.cose.2016.12.008

Michaud, V., & Michaud, V. (2017). Words fly away, writings remain–paradoxes in and around documents: A methodological proposition. *Qualitative Research in Organizations and Management: An International Journal*, *12*(1), 35-52. doi:10.1108/QROM-07-2015-1298

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* Thousand Oaks, CA: Sage.

Millum, J., & Garnett, M. (2019). How payment for research participation can be coercive. *The American Journal of Bioethics, 19*(9), 21-31.

doi:10.1080/15265161.2019.1630497

Mithas, S., & Rust, R. T. (2016). How information technology strategy and investments influence firm performance: Conjectures and empirical evidence. *MIS Quarterly, 40*(1), 223-245. Retrieved from www.misq.org/

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management, 35*(2015), 21-39. doi:10.1016/j.jom.2014.10.003

Mok, D., & Ang, E. (2016). ISO 15189: 2012 implementation: An update of related international standards and guidance documents for medical laboratory quality management. *New Zealand Journal of Medical Laboratory Science, 70*(2), 42-66. Retrieved from http://www.nzimls.org

Morgan, S. J., Pullon, S. R., Macdonald, L. M., McKinlay, E. M., & Gray, B. V. (2017). Case study observational research: A framework for conducting case study research where observation data are the focus. *Qualitative Health Research, 27*(7), 1060-1068. doi:10.1177/1049732316649160

Morse, J. M. (2015). Data were saturated. *Qualitative Health Research, 25*(5), 587-588. doi:10.1177/1049732315576699

Morse, W. C., Lowery, D. R., & Steury, T. (2014). Exploring saturation of themes and spatial locations in qualitative public participation geographic information systems research. *Society and Natural Resources, 27*(5), 557–571. doi:10.1080/08941920.2014.888791

National Institute of Standards and Technology (NIST). (2010). Guide for applying the risk management framework to federal information systems. (NIST Special Publication 800-37). Retrieved from http://csrc.nist.gov

National Institute of Standards and Technology (NIST). (2018). NIST updates risk management framework to incorporate privacy considerations. (NIST Special Publication 800-37 Revision 2). Retrieved from http://csrc.nist.gov

Nazim, M., & Ashgher, R. (2015). The cloud computing and its security issues. *International Journal of Emerging Technology and Advanced Engineering, 5*(7), 423-430. Retrieved from http://www.ijetae.com/

Nicholls, D. (2017). Qualitative research. Part 3: Methods. *International Journal of Therapy and Rehabilitation, 24*(3), 114-121. doi:10.12968/ijtr.2017.24.3.114

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

Oltmann, S. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts.[37 paragraphs]. *Forum: Qualitative Social Research, 17*(2). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/2551

Osbeck, L. M. (2014). Scientific reasoning as sense making: Implications for qualitative inquiry. *Qualitative Psychology, 1*(1), 34-46. doi:10.1037/qup0000004

Owen, G. T. (2014). Qualitative methods in higher education policy analysis: Using interviews and document analysis. *The Qualitative Report, 19*(26), 1-19. Retrieved from http://nsuworks.nova.edu/tqr/

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

Park, J. Y., Shin, S., & Song, K. Y. (2016). A proposal of risk management framework for design as a secure power control system. *Journal of the Korea Institute of Information Security and Cryptology, 26*(2), 425-433. doi:10.13089/JKIISC.2016.26.2.425

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*(2014), 165-176. doi:10.1016/j.cose.2013.12.003

Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage.

Patton, M. Q. (2008). *Utilization-focused evaluation* (4th ed.). Thousand Oaks, CA: Sage.

Payment card industry data security standard (PCIDSS). (2006). Retrieved from https://www.pcisecuritystandards.org/

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

Peticca-Harris, A., DeGama, N., & Elias, S. R. (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

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems, 21*(2017), 1-16. doi:10.3127/ajis.v21i0.1321

Phillippi, J., & Lauderdale, J. (2018). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research, 28*(3), 381-388. doi:10.1177/1049732317697102

Phillips, B. (2013). Information technology management practice: Impacts up on effectiveness. *Journal of Organizational & End User Computing, 25*(4), 50-74. doi:10.4018/joeuc.2013100103

Phillips, M., & Lu, J. (2018). A quick look at NVivo. *Journal of Electronic Resources Librarianship, 30*(2), 104-106. doi:10.1080/1941126X.2018.1465535:

Pietkiewicz, I., & Smith, J. (2014). A practical guide to using interpretative phenomenological analysis in qualitative research psychology. *Czasopismo Psychologiczne Psychological Journal*, *20*(1), 7-14. doi:10.14691/CPPJ.20.1.7

Pitsis, T. S., Sankaran, S., Gudergan, S., & Clegg, S. R. (2014). Governing projects under complexity: Theory and practice in project management. *International Journal of Project Management, 32*(8), 1285-1290. doi:10.1016/j.ijproman.2014.09.001

Ponemon Institute. (2015). *Cost of data breach study.* Ponemon Institute LLC, Michigan.

Ponemon Institute. (2018). Cost of data breach study. Ponemon Institute LLC, Michigan.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide:

A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551-567. doi:10.1016/j.im.2014.03.009

Prasad, A., & Green, P. (2015). Governing cloud computing services: Reconsideration of IT governance structures. *International Journal of Accounting Information Systems, 19*(1), 45-58. doi:10.1016/j.accinf.2015.11.004

Prasetyo, H. N., & Surendro, K. (2015). Designing a data governance model based on soft system methodology (SSM) in organization. *Journal of Theoretical and Applied Information Technology, 78*(1), 46-52. Retrieved from http://www.jatit.org/

Privacy Rights Clearing House. (2016). Data breaches. Retrieved from https://www.privacyrights.org/

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance. *Australasian Accounting Business & Finance Journal; Wollongong, 11*(1). 28-54. doi:10.14453/aabfj.v11i1.4

Rao, C., & Ramana, A. V. (2016). Data security in cloud computing. *International Journal of Current Trends in Engineering & Research (IJCTER), 2*(4), 84-92. Retrieved from http://www.ijcter.com

Rapport, F., Clement, C., Doel, M. A., & Hutchings, H. A. (2015). Qualitative research and its methods in epilepsy: Contributing to an understanding of patients' lived experiences of the disease. *Epilepsy & Behavior, 45*(2015), 94-100.

doi:10.1016/j.yebeh.2015.01.040

Ratten, V. (2014). "A US-China comparative study of cloud computing adoption behavior: The role of consumer innovativeness, performance expectations and social influence." *Journal of Entrepreneurship in Emerging Economies, 6*(1), 53-71. doi:10.1108/JEEE-07-2013-0019

Reece, R. P., & Stahl, B. C. (2014). The professionalization of information security: Perspectives of UK practitioners. *Computers & Security, 48*(1), 182-195. doi:10.1016/j.cose.2014.10.0070167-4048/

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research, 28*(5), 824-831. doi:10.1177/1049732317753586

Reynolds, P., & Yetton, P. (2015). Aligning business and IT strategies in multi-business organizations. *Journal of Information Technology, 30*(2), 101-118. doi:10.1057/jit.2015.1

Rid, T., & Buchanan, B. (2015). Attributing cyberattacks. *Journal of Strategic Studies, 38*(1-2), 4-37. doi:10.1080/01402390.2014.977382

Risk Based Security. (2015). Data breach notification laws. Retrieved from https://www.riskbasedsecurity.com/

Riungu-Kalliosaari, L., Taipale, O., Smolander, K., & Richardson, I. (2016). Adoption and use of cloud-based testing in practice. *Software Quality Journal, 24*(2), 337-364. doi:10.1007/s11219-014-9256-0

Robinson, O. C. (2014). "Sampling in interview-based qualitative research: A theoretical

and practical guide." *Qualitative Research in Psychology*, *11*(1), 25-41. doi:10.1080/14780887.2013.801543

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. New York, NY: Guilford Press.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135. doi:10.1093/cybsec/tyw001

Rozmus, C. L., Carlin, N., Polczynski, A., Spike, J., & Buday, R. (2015). The Brewsters: A new resource for interprofessional ethics education. *Nursing Ethics*, *22*(7), 815-826. doi:10.1177/0969733014547974

Ryan, S. (2017). An introduction to the origins, history and principles of ethnography. *Nurse Researcher, 24*(4), 15-21. doi:10.7748/nr.2017.e1470.

Sabherwal, R., Sabherwal, S., Havakhor, T., & Steelman, Z. (2019). How does strategic alignment affect firm performance? The roles of information technology investment and environmental uncertainty. *MIS Quarterly*, *43*(2), 453-474. doi:10.25300/MISQ/2019/13626

Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, *53*(1), 65-78. doi:10.1016/j.cose.2015.05.012

Saidani, M., Shibani, A., & Alawadi, K. (2013). Managing data security in the United

Arab. *Sky Journal of Business Administration and Management, 1*(1), 1-9. Retrieved from http://skyjournals.org/

Samimi, A., Ledary, R., & Samimi, M. (2015). ICT and economic growth: A comparison between developed and developing countries. *International Journal of Life Science and Engineering, 1*(1), 26-32. Retrieved from http://www.ijlsci.in/

Sandelowski, M. (1995). Sample size in qualitative research. *Research in Nursing & Health, 18*(2), 179-183. doi:10.1002/nur.4770180211

Santiago-Delefosse, M., Gavin, A., Bruchez, C., Roux, P., & Stephen, S. L. (2016). Quality of qualitative research in the health sciences: Analysis of the common criteria present in 58 assessment guidelines by expert users. *Social Science & Medicine, 148*(C), 142-151. doi:10.1016/j.socscimed.2015.11.007

Savola, M. J. (2014).Towards measurement of security effectiveness enabling factors in software intensive systems. *Lecture Notes on Software Engineering, 2*(1), 104-109. doi:10.7763/LNSE.2014.V2.104

Scherr, S. A., Elberzhager, F., & Holl, K. (2018, May). Acceptance testing of mobile applications-automated emotion tracking for large user groups. Paper presented at the Fifth International Conference on Mobile Software Engineering and Systems. Gothenburg, Sweden.

Schlechtendahl, J., Kretschmer, F., Sang, Z., Lechler, A., & Xu, X. (2017). Extended study of network capability for cloud based control systems. *Robotics and Computer-Integrated Manufacturing, 43*(1), 89-95. doi:10.1016/j.rcim.2015.10.012

Schulz, C. M., Krautheim, V., Hackemann, A., Kreuzer, M., Kochs, E. F., & Wagner, K. J. (2016). Situation awareness errors in anesthesia and critical care in 200 cases of a critical incident reporting system. *BMC Anesthesiology, 16*(4), 1-10. doi:10.1186/s12871-016-0172-7

Seidman, I. (2019). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (5th ed.). New York, NY: Teachers College Press.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341. doi:10.1080/07421222.2015.1063315

Senarathna, I., Yeoh, W., Warren, M., & Salzman, C. (2016). Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs. *Australasian Journal of Information Systems, 20*(1), 1-20. doi:10.3127/ajis.v20i0.1193

Senyo, P. K., Effah, J., & Addae, E. (2016). "Preliminary insight into cloud computing adoption in a developing country." *Journal of Enterprise Information Management, 29*(4), 505-524. doi:10.1108/JEIM-09-2014-0094

Sharma, G. P., Singh, S., Singh, A., & Kaur, R. (2016). Virtualization in cloud computing. *International Journal of Scientific Research in Science, Engineering and Technology, 2*(4), 181-186. Retrieved from http://ijsrset.com/

Singh, A., & Teng, J. T. C. (2015). Enhancing supply chain outcomes through information technology and trust. *Computers in Human Behavior, 54*(2016), 290-

300. doi:10.1016/j.chb.2015.07.051

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employee's adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi:10.1016/j.im.2013.08.006.

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

Sridhar, S. (2016). Cloud computing made easy. *International Journal of Innovative Technology and Research, 4*(2), 2875-2906. Retrieved from http://www.ijitr.com.

Stake, R. E. (1995). *The art of case study research*. London: Sage.

Starr, M. A. (2014). Qualitative and mixed-methods research in economics: Surprising growth, promising future. *Journal of Economic Surveys, 28*(2), 238-264. doi:10.1111/joes.12004

Sultan, N. (2013). Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations. *International Journal of Information Management, 33*(1), 160-165. doi:10.1016/j.ijinfomgt.2012.08.006

Talluri, S. (2016). Big data using cloud technologies. *Global Journal of Computer Science and Technology, 16*(2), 16-19. Retrieved from http://globaljournals.us/

Tang, C., & Liu, J. (2015). 'Selecting a trusted cloud service provider for your SaaS program.' *Computers & Security, 50*(1), 60-73. doi:10.1016/j.cose.2015.02.001

Tapsuwan, S., Mankad, A., Greenhill, M., & Tucker, D. (2017). The influence of coping appraisals on the adoption of decentralized water systems in Australia. *Urban*

Water Journal, *14*(1), 45-52. doi:10.1080/1573062X.2015.1057179

Tarr, E., Howard, J., & Stager, B. (2014). Listener preferences for analog and digital summing based on music genre. Paper presented at the 137th Audio Engineering Society Convention, Los Angeles, CA. Abstract retrieved from https://theproaudiofiles.com/wp-content/uploads/2015/01/Analog_Summing_Tarr_2014.pdf

Tenório, N., Pinto, D., Vidotti, A. F., De Oliveira, M. S., Urbano, G. C., & Bortolozzi, F. (2017). Tool based on knowledge management process: An interview protocol to gather functional requirements from software industry experts. *Matter: International Journal of Science and Technology*, *3*(1), 45-54. doi:10.20319/Mijst.2017.31.4554

The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research* DHEW Publication No. OS-78-0014). Washington, DC: US Department of Health, Education, and Welfare.

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly*, *32*(3), 316-322. doi:10.1016/j.giq.2015.05.001

Tilton, S. (2015, June). Archiver, documentarian, & proxy tool: A multimethod analysis of the tablet as the social scientist researcher's kit. Paper presented at the meeting of the Communication Association 2015 Annual Conference, Ohio.

Tisdale, S. M. (2015). Cybersecurity: Challenges from a system, complexity, knowledge management and business intelligence perspective. *Issues in Information Systems, 16(3), 191-198. Retrieved from http://www.iacis.org/*

Todd, E. M., Torrence, B. S., Watts, L. L., Mulhearn, T. J., Connelly, S., & Mumford, M. D. (2017). Effective practices in the delivery of research ethics education: A qualitative review of instructional methods. *Accountability in Research, 24*(5), 297-321. doi:10.1080/08989621.2017.1301210

Toye, T., Williamson, E., Williams, M. A., Fairbank, J., & Lamb, S. E. (2016). What value can qualitative research add to quantitative research design? An example from an adolescent idiopathic scoliosis trial feasibility study. *Qualitative Health Research, 26*(13), 1838-1850. doi:10.1177/1049732316662446

Tsai, J. M., & Hung, S. W. (2014). A novel model of technology diffusion: System dynamics perspective for cloud computing. *Journal of Engineering Technology Management, 33*(2014), 47-62. doi:10.1016/j.jengtecman.2014.02.003

Tumilowicz, A., Neufeld, L. M., & Pelto, G. H. (2015). Using ethnography in implementation research to improve nutrition interventions in populations. *Maternal Child Nutrition, 11*(3), 55-72. doi:10.1111/mcn.12246

Ussatova, O. A., Nyssanbayeva, S. E., & Wojcik, W. (2019). Software implementation of 2 FA Software implementation of two-factor authentication to ensure security when accessing an information system. *Journal of Mathematics, Mechanics and Computer Science, 101*(1), 87-95. doi:10.26577/JMMCS-2019-1-620

Verma, S., & Bhattacharyya, S. S. (2017) "Perceived strategic value based adoption of big data analytics in emerging economy: A qualitative approach for Indian firms." *Journal of Enterprise Information Management, 30*(3), 354-382. doi:10.1108/JEIM-10-2015-0099

Vithayathil, J. (2018). Will cloud computing make the information technology (IT) department obsolete? *Information Systems Journal, 28*(4), 634-649. doi:10.1111/isj.12151

Walsh, I., Holton, J. A., Bailyn, L., Fernandez, W., Levina, N., & Glaser, B. (2015). What grounded theory is: A critically reflective conversation among scholars. *Organizational Research Methods, 18*(4), 581-599. doi:10.1177/1094428114565028

Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study. *International Journal of Production Economics, 165*(1), 234-246. doi:10.1016/j.ijpe.2014.12.031

Wang, C. C., & Geale, S. K. (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, C., Wood, L. C., Abdul-Rahman, H., & Lee, Y. T. (2015). When traditional information technology project managers encounter the cloud: Opportunities and dilemmas in the transition to cloud services. *International Journal of Project Management, 34*(3), 371-388. doi:10.1016/j.ijproman.2015.11.006

Watkinson, A., Nicholas, D., Thornley, C., Herman, E., Jamali, H. R., Volentine, R., & Tenopir, C. (2016). Changes in the digital scholarly environment and issues of trust: An exploratory, qualitative analysis. *Information Processing & Management, 52*(3), 446-458. doi:10.1016/j.ipm.2015.10.002

Watts, L. L., Todd, E. M., Mulhearn, T. J., Medeiros, K. E., Mumford, M. D., & Connelly, S. (2017). Qualitative evaluation methods in ethics education: A systematic review and analysis of best practices. *Accountability in Research, 24*(4), 225-242. doi:10.1080/08989621.2016.1274975

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

Wolf, L. E., Patel, M. J., Tarver, B. A. W., Austin, J. L., Dame, L. A., & Beskow, L. M. (2015). Certificates of confidentiality: Protecting human subject research data in law and practice. *The Journal of Law, Medicine & Ethics*, *43*(3), 594-609. doi:10.1111/jlme.12302.

Xia, Z., Wang, X., Sun, X., & Wang, Q. (2016). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems, 27*(2), 340-352. doi:10.1109/TPDS.2015.2401003

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134-152. Retrieved from http://nsuworks.nova.edu/tqr/

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud

computing. *Journal of Internet Services and Applications, 7*(5), 2-12. doi:10.1186/s13174-016-0046-8

Yin, R. K. (2018). *Case study research: Design and method*. (6th ed.). Thousand Oaks, CA: Sage

Yin, R. K. (2015). *Qualitative research from start to finish* (2nd ed.). New York, NY: Guilford Press.

Yousif, M., Edsall, T., Krebbers, J., Pappe, S., & Khalidi, Y. A. (2014). Cloud computing roundtable. *IEEE Cloud Computing, 1*(1), 40-49. doi:10.1109/MCC.2014.5

Zafar, F., Khan, A., Malik, S. U. R., Ahmed, M., Anjum, A., Khan, M. I., Javed, N., Alam, M., & Jamil, F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy, and future trends. *Computers & Security, 65*(2017), 29-49. doi:10.1016/j.cose.2016.10.006

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. *Risk Management and Healthcare Policy, 9*(1), 75-85. doi:10.2147/RMHP.S99908

Zlatev, J. (2016). Turning back to experience in cognitive linguistics via phenomenology. *Cognitive Linguistics, 27*(4), 559-572. doi:10.1515/cog-2016-0057

Appendix A: Interview Protocol

Upon reading the entire informed consent form, I asked participants to sign, date, and submit the form to me. The subsequent information outlines the organization and interview protocols for collecting interview data:

1. I contacted participants via email, phone, and personal visit.
2. I sent a reminder email two days prior to scheduled interview.
3. I greeted participants informally to establish rapport, reiterated the study purpose, and reassured participants regarding informed consent guidelines.
4. I requested permission to record interview sessions.
5. I began sessions with an official welcome introductory statement: *"Hello, my name is Wanda Cotton. I am pursuing the Doctor of Business Administration degree at Walden University. Thank you for agreeing to participate in my research study. The purpose of this study is to explore strategies IT administrators use to mitigate data security breaches. Data compromise issues are problematic for organizations in all business industries worldwide. Despite the ongoing prevalence of data security failure, IT administrators lack the skills to improve this phenomenon."*

   "This research is significant because it contributes to the existing literature regarding data security breaches. Because of the continued frequency of data security failure in organizations, the findings in this study may help educate organization leaders regarding the significance of aligning ERM and IT risk management practices to mitigate data security risks. This study is relevant to the field of organization and management in that the findings may educate leaders about how breaches in data security can adversely influence performance and sustainability. This morning/afternoon, an IT administrator from an IT organization in the southern region of the United States joins me to

discuss the data security dilemma that plagues organizations. To protect participants' identities, I will reference them as Participant [1, 2, 3, 4, 5, or 6] from Organization [A, B, C, D, E, or F]. Thank you for being here, Participant 1, 2, 3, 4, 5, or 6], shall we begin the interview?"

6. I began the interview using a semistructured interview design.

7. I posed the following eight interview questions:

a. What strategies have you used to identify data security risks in cloud computing?

b. What strategies have you used to assess IT systems for data security vulnerabilities in cloud computing?

c. What strategies have you used to respond to potential and realized data security threats and breaches in cloud computing?

d. What strategies have you found work best to mitigate data security risks in cloud computing?

e. What communication strategies have you used to mitigate data security threats and breaches in cloud computing?

f. What strategies have you used to recover from careless data security threats and breaches in cloud computing?

g. What strategies have you used to align business objectives and IT security functions in the cloud?

h. What else would you like to share regarding strategies that you have used to mitigate cloud computing data threats and breaches?

8. I used an Android tablet to audio recorded interview session complied field notes.

9. I asked probing questions when applicable:

   a. Describe how you collaborate with other agencies or organizations to mitigate data threats and breaches.

   b. What training procedures have you used to mitigate data threats and breaches?

10. I concluded interviews; thanked participants for their input; and stopped recording.

11. I performed verbatim transcription of interview data.
12. I reviewed interviewer's analysis of the interview sessions.
13. I provided participants with my interview summation after member checks.
14. I made revisions or integrated new data from participant per member checks, if applicable.
15. I then analyzed data.

Appendix B: Letter of Cooperation

Community Research Partner Name

Contact Information

Date

Dear Wanda Cotton,

Based on my review of your research proposal, I give permission for you to conduct the study entitled Strategies Administrators Use to Mitigate Cloud Computing Data Threats and Breaches within the Insert Name of Community Partner. As part of this study, I authorize you to conduct semistructured interviews with information technology (IT) administrators that meet the study requirements (e.g., 18 years of age or older in a leadership position with at least 3 years' experience implementing strategies to mitigate data threats and breaches in cloud computing). Individuals' participation will be voluntary and at their own discretion.

We understand that our organization's responsibilities include:

- Permitting IT administrators, 18 years of age or older in a leadership position, with at least 3 years' experience implementing strategies to mitigate data security threats and breaches in cloud computing to participate in semistructured interviews.
- Providing a private area to conduct 30 minute to half hour interviews, of which during the last 10-15 minutes of the interview you can review the researcher's interpretation of your responses to interview questions for accuracy.
- Providing nonspecific organization documents (e.g., enterprise risk management and data security procedures) for the researcher to review.

We reserve the right to withdraw from the study at any time if our circumstances change.

I understand that the student will not disclose the identity of our organization in the doctoral project report after publishing the final research project in Proquest.

I confirm that I am authorized to approve research in this setting and that this plan complies with the organization's policies.

I understand that the data collected will (a) remain entirely confidential and may not be provided to anyone outside of the student's supervising faculty/staff without permission from the Walden University IRB, (b) be kept for at least 5 years on an encrypted laptop

only accessible by the researcher, and (c) be destroyed after the specified 5 year time period.

Sincerely,

Authorization Official
Contact Information

Walden University policy on electronic signatures: An electronic signature is just as valid as a written signature as long as both parties have agreed to conduct the transaction electronically. Electronic signatures are regulated by the Uniform Electronic Transactions Act. Electronic signatures are only valid when the signer is either (a) the sender of the email, or (b) copied on the email containing the signed document. Legally an "electronic signature" can be the person's typed name, their email address, or any other identifying marker. Walden University staff verifies any electronic signatures that do not originate from a password-protected source (i.e., an email address officially on file with Walden).