


2017

Security Strategies for Hosting Sensitive Information in the Commercial Cloud

Edward Steven Forde
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

 Part of the [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), and the [Databases and Information Systems Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Edward Forde

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. Steven Case, Committee Chairperson, Information Technology Faculty

Dr. Gene Fusch, Committee Member, Information Technology Faculty

Dr. Timothy Perez, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Security Strategies for Hosting Sensitive Information in the Commercial Cloud

by

Edward S. Forde

MS, University of Phoenix, 2010

BS, University of Phoenix, 2008

Doctoral Study Submitted in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Information Technology

Walden University

June 2017

Abstract

IT experts often struggle to find strategies to secure data on the cloud. Although current security standards might provide cloud compliance, they fail to offer guarantees of security assurance. The purpose of this qualitative case study was to explore the strategies used by IT security managers to host sensitive information in the commercial cloud. The study's population consisted of information security managers from a government agency in the eastern region of the United States. The routine active theory, developed by Cohen and Felson, was used as the conceptual framework for the study. The data collection process included IT security manager interviews ($n = 7$), organizational documents and procedures ($n = 14$), and direct observation of a training meeting ($n = 35$). Data collection from organizational data and observational data were summarized. Coding from the interviews and member checking were triangulated with organizational documents and observational data/field notes to produce major and minor themes. Through methodological triangulation, 5 major themes emerged from the data analysis: avoiding social engineering vulnerabilities, avoiding weak encryption, maintaining customer trust, training to create a cloud security culture, and developing sufficient policies. The findings of this study may benefit information security managers by enhancing their information security practices to better protect their organization's information that is stored in the commercial cloud. Improved information security practices may contribute to social change by providing by proving customers a lesser amount of risk of having their identity or data stolen from internal and external thieves

Security Strategies for Hosting Sensitive Information in the Commercial Cloud

by

Edward S. Forde

MS, University of Phoenix, 2010

BS, University of Phoenix, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2017

Dedication

I dedicate this work to my wife Stephanie, my beloved parents, siblings (Yvette and Yvonne), my children (Diamond, Anaise, Steven, and Erik, and friends for their constant love, support, time, and encouragement they gave me during the period I was preparing this work.

Acknowledgments

I thank God for the gift of life, good health, and protection. Great honor goes to my mentor, Dr. Steven Case, Dr. Fusch, Dr. Perez, for their guidance and patience. To the rest of the DIT staff of Walden University who provides their students an excellent learning environment and has opened the opportunity for me to study at their university. Thanks to all my colleagues for proper coordination and group work during the study. I acknowledge my lectures for instilling me with knowledge, which I applied during the project preparation. Lastly, I am so grateful to my parents, my two daughters, my two sons, and my beautiful wife for their love, continued support, and the many inspirations they gave me during the preparation of this dissertation.

Table of Contents

List of Figures	iv
Section 1: Foundation of the Study.....	1
Background of the Problem	1
Problem Statement	2
Purpose Statement.....	2
Nature of the Study	3
Research Question	5
Interview Questions	5
Conceptual Framework.....	6
Definition of Terms.....	6
Assumptions, Limitations, and Delimitations.....	8
Assumptions.....	8
Limitations	9
Delimitations.....	9
Significance of the Study	10
A Review of the Professional and Academic Literature.....	12
The Routine Activity Theory	14
Security Strategy Conceptual Model	21
Internal and External Attacks in the Cloud Environment.....	24
Security Strategies - Informal, Formal, and Technical	27
Informal strategies.	29

Formal strategies.....	30
Technical strategies.....	37
Complexity of Strategies in Cloud Computing.....	42
Privacy and confidentiality.	42
Data integrity and segregation.	44
Data center operations.....	45
Knowledge Gap	46
Transition and Summary.....	49
Section 2: The Project.....	51
Purpose Statement.....	51
Role of the Researcher	51
Participants.....	53
Research Method and Design	54
Research Method	54
Research Design.....	58
Population and Sampling	62
Ethical Research.....	63
Data Collection	66
Data Collection Instruments	66
Data Collection Techniques	68
Data Organization Techniques.....	70
Data Analysis	71

Reliability and Validity.....	73
Reliability.....	74
Validity	75
Transition and Summary.....	77
Section 3: Application to Professional Practice and Implications for Change	78
Overview of Study	78
Presentation of the Findings.....	79
Theme 1: Avoiding Social Engineering Vulnerabilities.....	80
Theme 2: Avoiding Weak Encryption	84
Theme 3: Maintaining Customer Trust.....	89
Theme 4: Training to Create a Cloud Security Culture	92
Theme 5: Developing Sufficient Policies	95
Applications to Professional Practice	98
Implications for Social Change.....	98
Recommendations for Action	103
Recommendations for Further Study	104
Reflections	105
Summary and Study Conclusions	105
References.....	108
Appendix A: Interview Protocol.....	141
Appendix B: Observation Protocol.....	146

List of Figures

Figure 1. Security strategy conceptual model.....	22
---	----

Section 1: Foundation of the Study

Cloud service users face constant and significant risks both inside and outside their cloud communities. Cloud services carry privacy and security risks that leave sensitive data vulnerable. The purpose of this study was to identify a need for systematic strategy assessment and then to simplify the complex remedying process for IT security managers. In this study, I first detail the problems that IT security managers face in cloud security; I then present the literature behind the study's basic framework.

Background of the Problem

Cloud service providers offer and manage the cloud infrastructure, which is the most distinctive element of cloud computing. The cloud infrastructure allows a company to store sensitive information offsite; this method of storage facilitates authorized and unauthorized access to information (King & Raja, 2012). The main obstacles in cloud computing are the security and privacy risks that IT security managers face while protecting sensitive information (Zhang & Zhang, 2014). This statement means that IT security managers might want to consider the main obstacles while building a strategy framework.

The data's security depends on elements of availability, integrity, and confidentiality. These three elements establish a foundational block in the design of secure information systems (Zissis & Lukas, 2012). Although cloud computing permits shared resources and components between subscribers, it also carries an increased risk that subscribers might capitalize on unauthorized access to sensitive information by exploiting vulnerabilities found in the cloud (King & Raja, 2012). The cloud computing

environment has high system complexity, providing hackers with opportunities for unauthorized data access (Rathi & Parmar, 2015). Furthermore, because commercial cloud providers deliver their services over the Internet, malicious outsiders execute high network threats on exposed data and applications (Riungu-Kalliosaari, Taipale, Smolander, & Richardson, 2014). In this study, I explored the strategies that IT security managers, with experience against internal and external data breaches in the cloud computing context.

Problem Statement

Service users fail to recognize the extent of security vulnerabilities in the cloud. In fact, Rong, Nguyen, and Jaatun, (2013) noted that many cloud services fail to provide assurance of security or privacy. Given that malicious insiders and outsiders threaten the cloud's information security, this issue demands immediate study. Ahuja and Komathukattil (2012) indicated that insider attacks accounted for 17% of data breaches, while external attacks represented 92% of the security attacks (Rao & Selvamani, 2015). The general IT problem is that companies that store data in the cloud could expose their customers' private information to these internal and external data breaches. The specific IT problem is that some IT security managers lack the strategies necessary to host sensitive information in the commercial cloud.

Purpose Statement

The purpose of this qualitative, single case study was to explore the strategies that IT security managers use to host sensitive information in the commercial cloud. The research participants were IT security managers from a government agency in the eastern

region of the United States with experience implementing security strategies to host sensitive information in the cloud. The findings from this study may benefit information security practice by increasing their understanding of the complex nature of internal and external threats and breaches. The implication for positive social change lies in the potential to improve security of a user's private data while stored in the commercial cloud.

Nature of the Study

I considered which research method best supported this study. The research method I adopted for this study was the qualitative method. In the qualitative method, scholars emphasize the description of meaning, concepts, elements, symbols, and definitions of the phenomenon (Fallahpour & Zoughi, 2015). Researchers rely on subjectivism when using the qualitative research method. Subjectivism is an epistemological position that posits that human subjects create the meaning of a phenomenon (Hathcoat & Nicholas, 2014). Other research methods, such as quantitative or mixed methods research, were less productive to the overall objectives of this study. A quantitative researcher builds on the positivism epistemology, where researchers use theory to formulate and test hypotheses (Everett, Neu, Rahaman, & Maharaj, 2015). This study did not involve formulating and testing hypotheses. Mixed-methods researchers builds on the pragmatism philosophy. Onwuegbuzie and Corrgin (2014) pointed out that mixed-methods research involves combining both qualitative and quantitative approaches. Mixed-methods research requires the formulation and testing of hypotheses (Green et al., 2015). I did not use mixed-methods research because I was exploring open-

ended questions. A qualitative methodology best maintained my objective in the study: to understand security strategies in cloud computing from the perspectives of experienced IT managers.

The most suitable design merited equal consideration. The case study method provided the best option, due to its strengths for investigating a contemporary event without manipulating relevant behaviors. Stake (2013) suggested that researchers use a case study design to explore a subject through multiple points of view. I considered other designs. Tracy (2012) explained that phenomenology deals with the exploration and understanding of an individual's lived experiences; a researcher using phenomenology focuses on lived experiences presented in the participant's words. This focus on lived experiences was less relevant to the goals of this study. Venters and Whitley (2012) pointed out that ethnographers combine research design fieldwork with other methods. This combination occurs as researchers attempt to develop a greater understanding of a particular culture or subculture. Throughout the premise of this study, I hoped to focus less on comprehending the value of the IT manager than on focusing on the methods that IT managers can use to protect information on the cloud. Although the narrative design includes interviews, narrative scholars seek to create meaning from interview answers, culminating them into a story that furthers life's meaning (Grbich, 2015). In this study, I sought not to qualify life, but to focus on security problems and security strategies in the cloud environment.

Research Question

The main research question was the following: What security strategies do IT security managers use to host sensitive information in the commercial cloud?

Interview Questions

The open-ended interview questions follow:

1. What habits do you repeatedly see among cloud-hackers when you consider which security strategies to implement?
2. What security vulnerabilities in the cloud-computing environment have you experienced?
3. What types of insider or outsider attacks in the cloud has your organization experienced?
4. What do you consider is the impact of these insider or external attacks?
5. In what ways have insider or external data breaches affected the cloud services provided to your clients?
6. What were your challenges addressing insider or external threats in your organization's use of cloud computing?
7. What security strategies have you used that failed to secure sensitive information in the cloud?
8. What security strategies have you used that succeeded to secure sensitive information in the cloud?
9. What additional information would you like to provide that I have not already asked?

Conceptual Framework

The conceptual framework for this study was the routine activity theory. Cohen and Felson (1979) developed the routine activity theory in 1979. According to the routine activities theory, activities that occur on a daily basis present unpredictable opportunities for crime and predation (Barclay, 2014). Hollis and Wilson (2014) suggested that the theory has three aspects necessary for predatory breaches to occur: missing guardians, a valuable target, and a willing offender. These aspects are required for crime commission because their temporal and spatial converging provides necessary opportunities. Thus, when a target meets all three aspects, a crime occurs (Denham, 2015). Considering this information, I adopted the routine activity approach to study the internal and external threats in the cloud computing environment; I used this theory to identify effective security strategies to protect sensitive information in the commercial cloud.

Definition of Terms

Cloud computing: The cloud computing model enables access to shared computing resources that are readily available, convenient, and universal, allowing for quick deployment and restricted interaction with the service provider (Samani, Honan, & Reavis, 2015).

Community cloud: The community cloud system provisions itself for use by consumers with shared, similar concerns (Ab Rahman & Choo, 2015).

Hybrid cloud: The hybrid cloud system comprises of two or more distinct cloud systems; these systems are distinct entities mutually joined with proprietary or

homogeneous technology for enabling application and data portability (Samani et al., 2015).

Infrastructure as a service (IaaS): The IaaS service model allows the client to compute resources such as networks, storage, and processing, and to run and deploy software (Zikkis & Lekkas, 2012).

Malicious insider threat: A malicious insider threat arises from a former or current contractor, employee, or other business partner with legal access to an organization's data, network, or system. These individuals deliberately abuse or surpass their access in order to affect the privacy, accessibility, or integrity of data or information systems negatively (Yusop & Abawajy, 2014).

Multitenancy: Resource sharing occurs among various clients within the cloud environment (Ab Rahman & Choo, 2015).

Platform as a service (PaaS): The PaaS model offers clients the ability to deploy the cloud system and applications the customer has created or acquired. The cloud service provider offers program languages and tools to produce the cloud system and its applications. (Zikkis & Lekkas, 2012).

Private cloud: A private cloud system restricts use to only one organization, which may include various clients (Samani et al., 2015).

Public cloud: A public cloud infrastructure open to the general public (Samani et al., 2015)

Software as a service (SaaS): The SaaS model provides the client with the ability to use applications on the cloud system that the cloud service provider offers (Zikkis & Lekkas, 2012).

Assumptions, Limitations, and Delimitations

The work in this study adheres to some assumptions, limitations, and delimitations. Barnham (2015) suggested that all individuals see the world in their own perspective; therefore, researchers should recognize and admit their underlying assumptions in the pursuit of objectivity. In the following section, I outline the assumptions, limitations, and delimitations of this qualitative study.

Assumptions

I should recognize my assumptions. Farquhar (2012) argued that an assumption appears when a researcher initiates a qualitative study and his or her primary theoretical expectations direct his or her supportive conclusion. Mortari (2015) suggested that researchers support the primary interpretive/theoretical frameworks while conveying the personal insights that frame the path of the investigation. Individual interpretations can shape the path of research. A particular set of assumptions arose in this study as well. Ardagna, Asal, Damiani, and Vu (2015) suggested that I should consider the participants in qualitative research as experts in the areas relevant to the study. In addition, the participants should provide truthful responses in the semistructured interviews. I anticipated both statements would be true and, as a result, the data collected reflected the complexity of combating data breaches in the cloud computing environment. I also

assumed that the use of a qualitative research methodology would be effective in providing the data needed to answer the research question.

Limitations

Researchers cannot generalize the restriction of a single case study. Ercikan and Roth (2014) claimed that limitations center on issues in reliability, validity, and generalizability. I anticipated some potential weaknesses in this investigation. First, using a qualitative design could have introduced researcher or participant bias. The participants or I could provide distorted, subjective opinions (Hammond, 2013). The limitation of using case study design meant the results hinged primarily on the experiences that the participants shared in the semistructured interview. If the participants did not have a particular experience, the results reflected that absence. The second limitation was that data collection occurred through participants from one government agency; though this limitation could have inhibited the generalization of findings to the private industry, many of the strategies the agency uses could apply to IT practice elsewhere. The third limitation was that the strategies that the security managers used are for private clouds, making generalizations to public or hybrid clouds difficult.

Delimitations

I should consider delimitations just as I should consider the limitations and assumptions. Rosenberg and Koehler (2015) claimed that delimitations are those factors within my control that limit scope and create the study boundaries. The scope of the study was to research internal and external data breaches in cloud computing. The first delimitation was the study's focus: the informal, formal, and technical strategies that IT

security managers implement in pursuit of cloud data protection. Another delimiter was my focus on government organizations and not on private industry. The research included all IT security managers (approximately 10) from a U.S. government sector. The third delimiter was that the study participants and I worked for the same agency but in entirely different departments and locations. The final delimiter was that these IT security managers were involved in the use of cloud-based products and providing security in the cloud infrastructure, so that their lived experiences would provide relevant information on the complexity involved in the cloud's internal and external data breaches, as identified by Ardagna et al. (2015).

Significance of the Study

Cloud service users fail to recognize to what extent their sensitive information is vulnerable in the cloud. This study is valuable to IT security managers because I propose security strategies for protecting cloud information. Its findings might provide IT security managers with a robust framework for assessing cloud data security. The study's findings may contribute to IT practice by enriching the literature on internal and external threats and the security strategies used to combat them, thereby expanding an understanding of the complex nature of these topics. The goal of this study was to create a security strategy model for IT security managers grounded on the routine activity theory, a model that may benefit IT security managers when using a combination of what Chang and Ramachandran (2015) called formal, informal, and technical strategies. With this framework in place, IT security managers could implement the correct combination measures against certain internal and external data breaches.

This research could contribute to positive social change by creating awareness for IT managers on the complexity of internal and external attacks in the cloud environment. Greater society might benefit from this research's potential to strengthen knowledge around informal, formal, and technical strategies. IT security managers might be able to choose, more efficiently, which strategies work best to combat particular internal or external data breaches.

Security strategies for fraud protection rest in the hands of both the individual and national agencies. Fraud in online circles is one of the most trending forms and aspects of behavioral deviance in modern society (Williams, 2015). This deviance takes various shapes and forms, as the distinction and veracity of online fraud and subsequent thefts differ from one country to the next. Mergel and Bretschneider (2013) stated that security measures should consider all components in a multifaceted matrix to explain the different tenets that may expose differing groups of people. For instance, the national security measures regarding cyber welfare and protection strategies determine whether a country could be more prone to compromise. Furthermore, Williams (2015) claimed that individuals must ensure that their data are safe from prospects of easy infringement and theft. In addition, Williams argued that an attempt should be made to associate online identity theft to the physical and personal choice of security measures. The responsibility for cyber security rests on the cloud computing environment, as well as the persons involved in online businesses.

There are difficulties surrounding online fraud and security break down. Reysn and Henson (2015) highlighted how the thief may get away, but the victim often suffers

from the consequences associated with a stolen identity; thieves can also use the victim's identity to commit other crimes. There are few explanations of the causes correlating occurrences of identity theft to the subsequent victimization. Criminals might establish some patterns or routine procedures to recreate an occurrence for crime. For instance, the hackers and the cyber criminals may develop an algorithm through binary regression models to try to determine the future behavioral pattern of an online user (Ahmad, Maynard, & Park, 2014). Thus, it would be easier to navigate through some of the most common platforms and sites that the online user frequents and to create a duplicate, resulting in identity theft. Making note of these behavioral patterns is crucial to security measures.

A Review of the Professional and Academic Literature

Many researchers have undertaken security strategies for hosting sensitive information in the commercial cloud. Waleed, Chunlin, and Naji (2014) found that, despite researchers' efforts to determine cloud security issues, the intervention measures have not been effective because cloud security issues have continued to be a threat to organizations that use the cloud. As a result, IT security managers seeking security strategies for hosting sensitive information in the commercial cloud look to previous studies for guidance. Therefore, I reviewed the previous research regarding the most effective intervention methods. These intervention methods can help IT managers overcome challenges they face while managing their organizations' cloud security. Ali, Khan, and Vasilakos (2015) reviewed literature relevant security in cloud computing. I have done the same. I also added aspects of the routine activity that were relevant to this

study, including influences on the conceptual model, security strategies, internal and external attacks, and an observation of the complexity of security strategies.

During this phase, I organized the contents of the literature review with security strategies in mind. I outline the conceptual model by first explaining the routine activity theory (RAT). After providing a general background of the theory and its use in multiple IT studies, the I present the main components of the security strategy conceptual model. I contextualize the security strategy conceptual model, separating the internal and external attacks, and moving into the informal, formal, and technical strategies. The most efficient security strategies include a combination of formal, informal, and technical controls because many of the strategies necessitate complexity to deal with complex issues and include concerns regarding privacy and confidentiality, data integrity and segregation, and data center operations.

To amass the information necessary for this literature review, I searched through scholarly databases to compile 200 sources; these databases included University Library, Google Scholar, ProQuest, SAGE, Academic Search Complete/Premier, and EBSCO host. The search terms included *data breaches*, *internal and external data breaches*, and *IT strategies for data breaches*. My focus narrowed to literature about current themes in internal or external attacks and the strategies used to prevent them. There were a total of 95 sources in the literature review. Of those sources, 85, or 89%, were peer-reviewed and verified through Ulrich. These sources were recent, with 94 out of 95, or 99%, of the literature review sources having a publication date within 5 years or less of expected chief academic officer (CAO) approval. Data breaches remain a common occurrence, as

demonstrated with recent attacks on Sony and Apple. Scholarly references to those attacks are minimal, however, and research remained far spread. In instances where the sources appeared earlier than 5 years, I either countered or added to them with work that was more recent.

The routine activity approach, used as the basis for the conceptual framework of this study, originally appeared in 1979—well beyond the 5 years of the CAO approval. Studies that were more recent have implemented and expounded on this theory. Some of these studies, such as work undertaken by Drawve, Thomas, and Walker (2014), have attempted to move beyond the deciding factors of criminalization and have tried to create methods of prediction in various crimes like assault or Internet fraud. I attempted something similar in this study, believing that a firm that understands criminal motivation can predict potential crimes to prevent potential crimes. In this way, the RAT was in concordance with the development of cybercrime. Weisburd, Groff, and Yang (2014) used RAT to predict crimes at the national level. In this review, I explained the lack of a national standard for cloud security protection.

The Routine Activity Theory

The RAT was a component of this study's literature review. Cohen and Felson developed the RAT with the aim of explaining the occurrence of crimes in the world (Branic, 2015). Though the theory is not in alignment with most criminology theories, it can be used to explain some crimes. In fact, the theory's focus was on computer crimes rather than physical crimes. According to RAT, offenders are motivated to conduct a crime whenever a suitable target emerges (Leukfeldt & Yar, 2016). Crime remains

unaffected by social causes such as unemployment, inequality, and poverty. In computer victimization, the offender will be motivated to commit crime and will do so once a target appears. Vakhitova, Reynald, and Townsley (2015) claimed that most of the people involved in these sorts of criminal activities are youths. Vakhitova et al. covered computer victimization's evolution, how different models have shaped the routine activity theory, as well as the theory's critical analysis.

Evolution of the theory. The RAT has changed since its conception. Cohen and Felson first postulated the theory in the year 1979 (Leukfeldt & Yar, 2016). Cohen and Felson introduced the theory in response to the rise of computer victimization, which demanded the discovery of both an explanation of the crime and its solutions. Cohen and Felson (as cited in Leukfeldt & Yar, 2016) established their own RAT. The theory is built on three principles; these principles include a motivated offender who is willing to commit crime, a suitable target at the receiving end, and the absence of someone who can defuse the situation (Cohen & Felson, 1979). Schafer and Mazerolle (2015) stated that when all three elements are present, crime will likely happen. The absence of one of the elements may be enough to discourage crime from happening. When computer security is absent, crime could happen. Similarly, Reys and Henson (2015) claimed that the number of people victimized by computer criminals has been on the rise. Hackers or cyber criminals invade other people's computers without their permission.

Supportive theories. Researchers created the RAT during a time when victimization entered the foreground of many people's attention. The focus shifted not only in to the criminal offender but also to the victim. Some of the theories in support of

RAT are what Vakhitova, Reynald, and Townsley (2015) pointed out as the human ecology theory and lifestyle exposure theory. These theories are about similar issues of crime but consider different elements the cause behind crime's occurrence. According to the human ecology theory and lifestyle exposure theory, individual daily activities contribute to victimization, either on the computer or in real life. Hawley (1950) created the human ecology theory in 1950 and suggested that the interaction of an individual with his or her environment will fuel him or her to crime. In the lifestyle exposure theory, individuals will act depending on the way they interact with their surroundings (Schaefer & Mazerolle, 2015). Although RAT centers more on computer victimization, it suggested that an individual's daily activities would drag him or her toward criminal behavior. Ultimately, the human ecology theory and lifestyle exposure theory offered similar conclusions as the RAT.

Contrasting theories. Lifestyle exposure theory and human ecology theory include similar issues, though they do have some variation. Human ecology theory focuses entirely on the physical acts that humans commit against each other. Human ecology theorists cover only those crimes that offenders physically commit against their victims. The lifestyle exposure theory appeared later in response to technological advancement. The theory's main aim was to address computer victimization (Bunch, Clay-Warner, & Lei, 2015). According to the lifestyle exposure theory, certain lifestyles lead to the occurrence of computer victimization. For instance, lifestyle exposure theorists have linked leisure time and its influence on computer victimization.

Criticism of the theory. Though the RAT has been used to explain the occurrence of criminal acts in the world, it has failed in some aspects. Major critiques arose on the issue of provision of testable propositions on the offenders. Bunch, Clay-Warner, and Lei (2015) pointed out that the RAT cannot be used to establish extensive research on computer victimization. Felson and Cohen (1979) did not explain what motivated offenders into doing their acts. Felson and Cohen believed that motivation was constant. Felson and Cohen neglected to provide an explanation of how an individual's social status influences his or her actions. Social aspects, like poverty, could affect someone's actions. The theory does not cover all types of crime but a given section only.

RAT and IT practice. The RAT can be combined with IT, other theories, and subjects. Karanasios (2014) examined theory and knowledge of shortcomings of ICT for Development (ICT4D) with RAT. The RAT also was used in information systems security. Wang, Gupta, Rao, and Raghav (2015) quantified the risk of information systems applications to insider threats. Bossler and Holt (2013); Wang et al. (2015); and Reyns, Henson, and Fisher (2015) pointed out the significant influence of guardianship in combating malware infections, an element crucial to the development of this study's conceptual framework. These findings suggest guardians like IT security managers are integral to cloud data protection. Other theories were considered to further the import of this finding.

Previous scholars' application of the RAT made it a choice for the conceptual framework for this study. Franklin, Franklin, Nobles, and Kercher (2012) noted that the RAT includes copyright infringement crimes related to peer-to-peer file sharing,

corporate espionage, and employee theft. Anandarajan, D'Ovidio, and Jenkins (2013) pointed out that the way that routine activities occur daily could create opportunities for predation. I built on RAT because its account of the motivations to commit crimes created a better understanding of the types of strategies available.

Victims can incur property loss or loss of means of livelihood. Turanovic and Pratt (2014) claimed that the criminal victimization may have adverse ramifications to the individual and society. In addition, victimization may include mental harm, such that the affected persons would undergo episodes of psychological torture during and after the ordeal. Turanovic and Pratt also expressed that repeat victimization is likely to occur. A particular section of the society that might have suffered from victimization in the past may experience similar occurrences. There is no one reason that can determine the prospect or likelihood of a victim's chances of victimization in future. A person's lifestyle may place him or her at a disadvantage to be more likely to be exposed to such victimizations, depending on the nature and pattern of their routine (Holtfreter, 2015). Such occurrences may occur in future as they might have occurred previously.

Regular online patterns or routines could lead to higher chances of identity theft and subsequent victimization (Reyns, 2013). For instance, people who uses the Internet and other online platforms regularly are at a higher disposition to becoming victims. Specifically, the customers who use online banking services, instant messaging, and e-mail services are most likely to form an online pattern that could expose them to online offenders (Reyns, 2015). People who download and use online shopping platforms are at a 30% increased risk (Reyns, 2015). These statistics might be an extension of traditional

or conventional direct-contact offenses. The online web surfing patterns may cover other aspects of online surfing characteristics (Reyns, 2015).

Other researchers have focused on remedying computer systems to mitigate criminal activity. Crossler et al. (2013) explored factors in mitigating and protecting against technological threats. For instance, Crossler et al. reasoned that IT personnel could institute software or hardware security measures within computer systems. However, it may be difficult to fully cover technological assets within a larger context. Willardson (2013) and Braswell, McCarthy, and McCarthy (2015) agreed that the challenges of security compatibility rest in the technical issues. Crossler et al. and Braswell et al. outlined potential actions to cover technological assets in larger contexts. They drew their focus on Behavioral InfoSec (Information Security) research modes, outlining its technical and mechanical challenges. These modes pursue future measures for crime mitigation. There is a difference between deviance and misbehavior on the part of the insider and outsider, however.

Gang activity is taking a new form. Pyrooz, Decker, and Moule (2015) specified that deviance and crime form some of the components of the human life and society. The advancements, modifications, and changes in the Internet or IT has introduced a landscape of technological complexity. Accordingly, the approaches to criminal behavior and victimization have also changed in proportion to the alterations in the technological world. Pyrooz et al. elaborated on how gangs have shifted to focusing on online settings. Pyrooz et al. gathered data from 585 research respondents from various cities all over the world, and 418 research participants were current and former gang members.

Where crime occurs is just as important as why it occurs. Henson, Reynolds, and Fisher (2013) and later Newton and Felson (2015) investigated places where crime occurs. Security chiefs and IT security managers should note that criminals have changed their traditional places of attack and crime, such as street corners or isolated street segments, and have brought crime into neighborhoods. Neighborhood theorists have, in the past, attempted to explain the mental processes of the offenders (Newton & Felson, 2015). These researchers posited that three main conditions predicted crime: the crime pattern theory, RAT, and the rational choice theory. Not all these concepts are mutually exclusive; some degree of dependability exists between the crime pattern theory and RAT.

Determining a theory to use to build the conceptual framework depended, first, on a consideration of the research problem. The overall complexity of addressing security issues in the cloud needed a solution that would not only be able to break that complexity into manageable parts but also assist in application against insider and outsider attacks. The goal of this study was to develop a robust framework that IT specialist can use to determine which strategies will best protect sensitive information stored in the cloud. Williams (2015) pointed out that, in terms of predictability, the RAT was the best option. Miller (2013) stated that when Cohen and Felson's theory emerged in the 1970s, they hoped to understand the situations and opportunities that create crime; over time, this theory became one of the founding principles of criminology. Both Miller and Policastro and Payne (2015) demonstrated how the RAT theory branched in a combination of factors, but two dependent variables—concerned with either crime or criminality. That

branching meant that RAT could apply to any number of investigative works, including investigations into street codes and gang work, cyber bullying, and telemarketing fraud (Arntfield, 2015; Hughes & Short, 2013; McNeeley & Wilcox, 2015).

Security Strategy Conceptual Model

The goal of this research was to determine a strategy that could help boost an organization's cloud security. I hoped to accomplish this by adding more layers to a security strategy conceptual model. Akeel, Wills, and Gravel (2014) stated that adding more layers implies that the model will become more complex, making it increasingly difficult for hackers to perform their hacking operation. Furthermore, adding an assurance layer to the security strategy conceptual model could aid in monitoring the function of the entire system. In case of any intrusion into the system, the assurance layer should be capable of immediately notifying the system administrator about a detected problem. To best address cloud security's complexity, my conceptual framework needed a theoretical foundation.

The conceptual framework centers around the routine activity theory. Tang and Liu (2015) investigated the complex strategies that consumers need to pick a cloud service provider for SaaS; I wanted to model their work but have my conceptual framework build off the RAT in order to understand internal or external threats in the cloud environment better. I hoped this understanding would help IT security managers determine effective security strategies against those data breaches. Figure 1 below demonstrates how the security strategy conceptual model maps relate to the RAT.

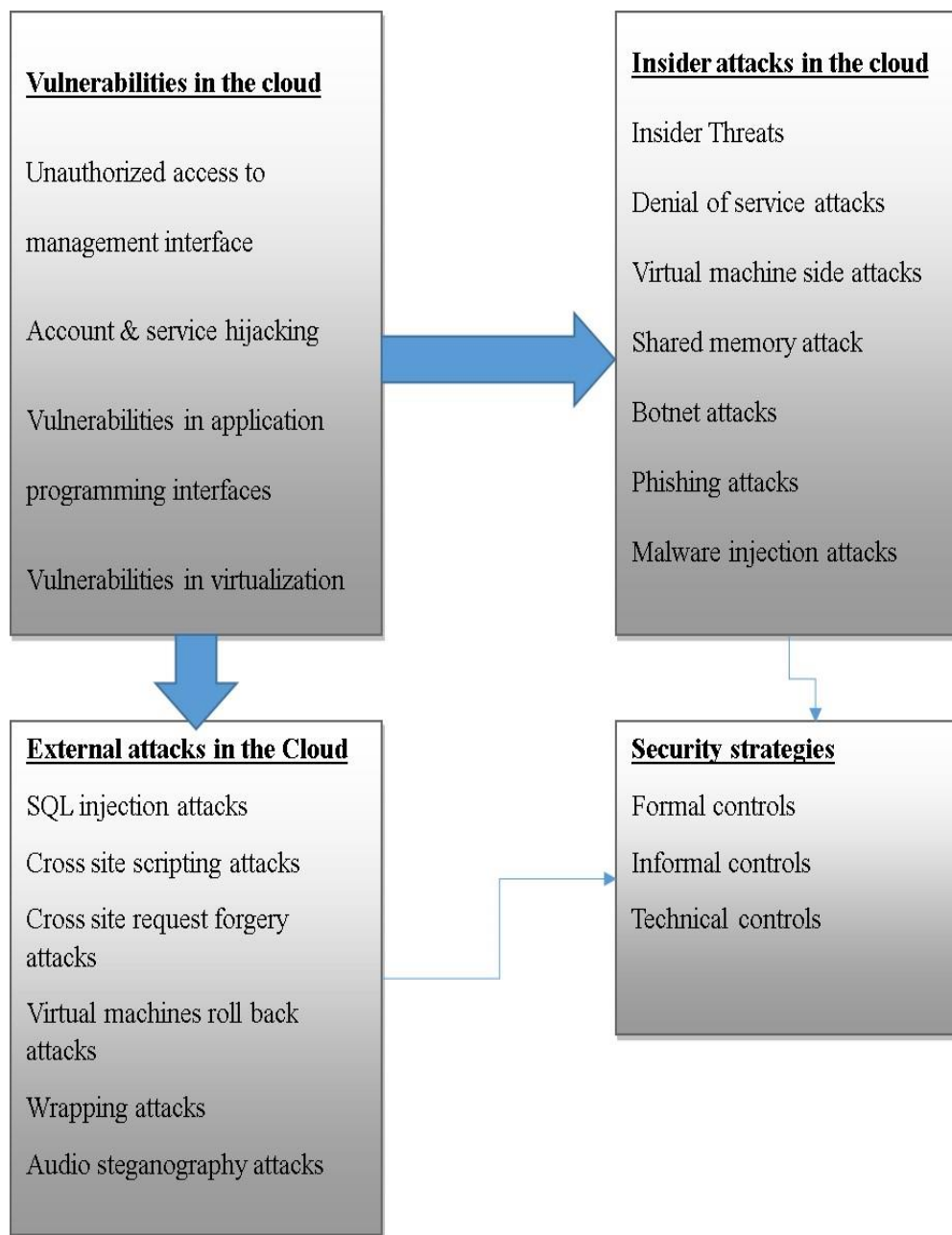


Figure 1. Security strategy conceptual model.

In Figure 1, vulnerabilities in the cloud, in combination with four properties of the RAT (visibility, inertia, value, and accessibility), present hackers with opportunities to execute various attacks. Tang and Liu (2015) pointed out that hackers have previous knowledge about the vulnerabilities in the cloud infrastructure; they also have the necessary capabilities to exploit those vulnerabilities through an execution of different attacks. By executing these attacks, hackers can access highly sensitive customer information, which they later sell for a profit. Therefore, researchers anticipated benefits for initiating attacks in the cloud. In short, this model coincided with conclusions made by Bartolacci, LeBlanc, and Podhradsky (2014). Bartolacci et al. (2014) concluded that some environments are suitable targets because they demonstrate four properties from the routine activity approach: high visibility, low inertia, easy accessibility, and high value. I stopped reviewing here due to time constraints. Please go through the rest of your section and look for the patterns I pointed out to you. I will now look at Section 2.

Leukfeldt (2014) dealt with many of these same properties in a Netherlands-based investigation of the motivations behind phishing victimization, one of many attacks relevant to cloud security as well. Leukfeldt (2014) found that homes with higher income (greater value), items of less weight (low inertia), items of conspicuousness (high visibility), and with easy access (accessibility) were desirous prospects, necessitating the need for proper security measures. Whether in phishing or cloud security, all of these properties rely on the insider's privileged access to the cloud infrastructure and the outsider's capabilities to exploit vulnerabilities in the cloud system. Therefore, continuing in line with the routine activities theory and the conclusions made by Bartolacci,

LeBlanc, and Podhradsky (2014), security strategies should deal with hackers through a combination of informal, formal, and technical controls.

Although applications of RAT to IT work were familiar, I was the first to apply this particular conceptual framework. Mergel and Bretschneider (2013) claimed that I should construct the conceptual frameworks in research as opposed to copying or finding them. The framework built on my understanding of RAT, in which to predict, prevent, or remedy data breaches, one must first understand the vulnerabilities, recognize the potential sources of attack, and then apply one or more of the informal, formal, or technical strategies. Ultimately, this study relied on the conceptual model, shown above, to outline the complexity surrounding insider and outsider attacks. Rezaeibagha et al. (2015) established the importance of technical features using an extensive literature review and Prisma flow diagram. I hoped to model the success of their study, aiming for a conceptual framework that could help establish whether IT security managers have implemented appropriate security strategies.

Internal and External Attacks in the Cloud Environment

Insiders and outsiders exploit the vulnerabilities found in the cloud environment, resulting in the execution of attacks against the cloud system. An insider threat, in the context of cloud computing, is a former or current contractor, employee, or other business partner with legal access to an organization's network, system, or data. Yusop and Abawajy (2014) defined an insider as an individual who abused their access to affect the confidentiality, availability, or integrity of the data or information systems negatively. Other researchers, such as Nurse et al. (2014), described an insider as one who violated

the policy on security by utilizing legal access; insiders gain illegal access to violate the policy on control.

In the cloud-computing context, insiders could embody rogue system administrators. Claycomb and Nicholl (2012) defined a rogue system administrator as an internal organization exploiting cloud weaknesses for illegal access, or those individuals who use cloud systems to execute attacks on an organization's local resources. A rogue administrator attacks the cloud infrastructure with an objective of stealing sensitive information; this particular attack leads to the loss of integrity and confidentiality of the data. In addition, a rogue administrator could hope to obtain the information and technology infrastructure of the cloud system.

There are various categories of rogue administrators in cloud computing, including application, system, virtual image, and hosting firm administrators. These rogue administrators can execute different attacks to the cloud system. For instance, application administrators can target vulnerabilities found in the virtual machine drivers. They can acquire control of the platform that hosts the cloud services, or they can execute malicious configurations to the cloud's applications. Mallaiah and Ramachandram (2014) pointed out that system administrators can execute conventional operating attacks, such as Trojan horses and root compromises. Meanwhile, virtual image administrators can copy virtual disks or machines, creating alternating images that fail to conform to the established baseline despite reports stating otherwise; they might also modify individual cases of a virtual machine within the cloud, leading to some aspects of the cloud behaving incorrectly (Claycomb & Nicholl, 2012). Finally, administrators from the

hosting firm can implement network taps on hosted systems; they can utilize social engineering techniques to monitor the hosting software.

The second category of insider threat includes those individuals who exploit the vulnerabilities in the cloud system to acquire illegal access to an organization's data or system. Claycomb and Nicholl (2012) found that this threat might be unintentional or malicious; variations in the access control or security policies between the client's and cloud systems enable this type of insider threat. In short, an individual gaining access to sensitive data for fraudulent purposes characterizes this category of insider threat.

One more class of insider threat exists. The final class, as defined by Freitas and Watson (2014), has attackers utilizing the cloud to conduct nefarious activities. In this context, the insider uses the cloud as a tool to conduct attacks on data or systems not automatically related. In this case, an insider uses cloud services, such as file sharing and email, to steal information. To clarify, the insiders utilize their lawful access to violate the security policy. Then insiders expand their rights, allowing them to sidestep policies related to access control and security. Yusop and Abawajy (2014) noted that excessive privileges could cause insiders to act without accountability and restriction. Trusted individuals execute insider attacks with different degrees of access to an organization's cloud system; insiders have adequate knowledge of the underlying infrastructure, making it easy for them to execute attacks in the cloud.

There are more advantages for insiders than outside hackers attacking the cloud system. Mallaiah and Ramachandram (2014) pointed out the various challenges that exist in relation to the insider threat. For instance, insiders have greater success executing

attacks because they are familiar with the internal security controls. In addition, the majority of the designed security tools typically deal with external rather than internal threats. Rafeeq and Kumar (2015) explained that insider attacks include the deletion of critical information, the tampering of sensitive information, data duplication, and the unauthorized extraction of such data. Sabotage, bribery, extortion, embezzlement, and espionage represent some of the many motivations behind insider attacks (Nurse et al., 2014). Overall, the issue of the insider threat in the cloud computing environment warranted further empirical investigations to determine the perceptions of IT security managers about this issue. Their response may help to recognize effective security mechanisms to overcome this challenge.

External hackers are somewhat limited in their attacks in the cloud environment. They rely on internal mistakes or lack of security practice allowing their exploits to work on cloud vulnerabilities. Mukwasi and Seymour (2012) considered external attacks in the cloud similar to those occurring in systems not based on the cloud infrastructure because both share underlying technologies.

Security Strategies - Informal, Formal, and Technical

As previously stated, this study's purpose was to explore strategies used to store information in the cloud. Three separate categories defined these strategies: informal, formal, and technical. Ahmed and Hossain (2014) used these categories as derivatives from the routine activity theory; these categories formed the foundation for this study's conceptual framework. The conceptual framework identified vulnerabilities that hackers could exploit to execute various attacks in the cloud computing setting. It might also aid

security managers in implementing effective security strategies to deal with internal and external threats in the cloud environment.

Three types of strategies largely defined the security mechanisms possible to address cloud security complexity. First, Lowry and Moody (2014) claimed that informal controls provide education on information security and create a security culture in the organization. Formal controls necessitate compliance with regulations and policies related to information security (Silbey, 2013). Finally, technical controls address issues with access management. These strategies remain useless without a guardian to implement them.

Guardians are critical to the cloud security process. Researchers like Weisburd, Groff, and Yang (2014) defined guardians as individuals with the ability to prevent a crime. Ahmed and Hossain echoed this statement, claiming that guardians are critical to the prevention of crime because they maintain vigilance and implement the necessary interventions to deter potential offenders. Guardians define an organization's internal and external strategies as either informal, formal, or technical in nature. Pyrooz, Decker, and Moule Jr. (2015) noted that a lack of able guardians, as well as an appropriate target and a possible offender, were three aspects of predatory breaches in the routine activity theory. These aspects are required for crime commission because their temporal and spatial converging provide the necessary opportunities to commit a crime. Therefore, the implication of the routine activity theory is that a crime can only take place when all of those three aspects are present (Pyrooz, Decker, & Moule Jr, 2015).

Just like a guardian is important to deflecting cloud attacks, other factors play in as well. Reyns (2015) presupposed there would always be a motivated offender willing to commit a crime if the right opportunity appears. This presupposition is how another element, the rational choice theory, worked into this study's conceptual framework. Routine activity theory influenced work by Haines, Horowitz, Guo, Andrijcic, and Bogdanor (2015); they presumed that potential offenders calculate their expected risks, costs, and benefits before perpetrating a crime. Implementation of formal strategies requires at least a basic awareness of opportunities that could be considered tempting. Therefore, to understand strategies better, one must also recognize the four properties that determine a suitable attack target, namely: value, inertia, visibility, and accessibility. Moon, Morash, Jeong, and Yoon (2015) argued a target with high visibility, limited inertia, easy accessibility, and significant value attracts a criminal. In a demonstration of their close relationship, the four properties successfully describe two aspects of the routine activity theory, namely opportunities and a lack of able guardians (Weisburd, Groff, & Yang, 2014).

Informal strategies. Informal strategies focus on providing information. Wei-Wen et al. (2013) argued these strategies dealt with providing an education on information security to create a security culture in the organization. In this regard, employers should provide employees with training to increase their awareness of the internal or external threat. Greitzer, Kangas, Noonan, Brown, and Ferryman (2013) suggested that awareness among organizational employees enables them to identify suspicious behavior among their co-workers, thus helping to thwart insider events.

Furthermore, training employees on this issue create a vigilant community in the organization, which can play a significant role in exerting deterrence against insider or outsider activities. Ruefle, Dorofee, Mundie, Householder, Murray, and Perl (2014) suggested the training programs establish a culture of security that is suitable for an organization.

Formal strategies. Formal strategies are associated with regulation compliance and policies about information security. Peppard, Galliers, and Thorogood (2014) claimed formal strategies involve the following rules. Ambre and Shekokar (2015) suggested that organizations consistently enforce and communicate information security policies so that employees understand how to prevent insider or outsider attacks. There should be clarity in the policies, in terms of acceptable use of organizational resources, information, and systems, the use of privileged accounts, and the processes for dealing with employee grievances. In addition, the policies should outline the consequences for violating the expected standards.

Furthermore, comprehensive service level agreements between customer and cloud service provider should be in place to provide direction on how to cover information security risks posed by insiders or outsiders (Ambre & Shekokar, 2015). The agreements should delineate monitoring capabilities, supervise the activities of employees, and determine the level of restrictions for accessing the client's sensitive information in the cloud. Soomro, Shah, and Ahmed (2016) pointed out that agreements are necessary to guarantee that the cloud service providers exceed or meet the required security standards; the agreements must also confirm that the providers will adopt

mitigating controls to minimize the risk of internal and external data breaches. Another formal strategy is to put in place procedures and policies for incident reporting; this strategy enables employees to report any malicious activity by their co-workers. Ruefle et al. (2014) claimed the incident-reporting program should address the incidents committed by insiders or outsiders and should have a chain of escalation; they should outline the necessary authorities who make decisions about a certain problem. This outline provides individuals in an organization with a mechanism for reporting insider or outsider attacks, providing IT managers with opportunities for initiating the necessary remedies.

Governance and enterprise risk management. Governance is associated with controlling and supervising the procedural and operational activities of cloud services. Specifically, Samani, Honan, and Reavis (2015) pointed to issues such as service testing and monitoring, legal issues, development standards for applications, procedures, and policies as relevant to the governance of the cloud system. Conversely, cloud computing requires an examination of legal issues and policies, due in part to the dependencies found in this context. Therefore, one should identify and address threats associated with protection of sensitive data, transparency of the cloud service provider, and breaches of service level agreements. Organizations must have the capability of governing, measuring, and managing enterprise risks associated with data in the cloud.

The significant problems of governance and enterprise risk management concern suitable identification and execution of the organization's processes, structures, and controls to maintain effectual risk management, security governance, and compliance. Liu, Sheng, and Marston (2015) suggested companies should also guarantee sensible

information security across an information supply chain, which should consist of providers and clients of the cloud computing services, as well as the supporting, third party sellers in any cloud operation model. Liu, Sheng, and Marston (2015) went on to say that properly developed information security governance procedures result in IS management programs that are scalable with the organization, measurable, repeatable across the organization, defensible, continually improving, sustainable, and lucrative on an ongoing basis.

Compliance management and data regulation. Compliance with legal issues related to information in the cloud context is a considerable challenge. Because of the nature of cloud computing in terms of its ubiquity and different service models, cloud service providers have to evaluate compliance requirements arising in the deployment of their services. Elifoglu, Guzey, and Tasseven (2014) pointed out that the regulatory and legal issues that cloud providers have to follow vary based on the location of the cloud services. Thus, users affect various operational functions, including privacy and security responsibility, electronic discovery, and management of the data lifecycle, potentially violating the client's privacy and security. Sookhak et al. (2015) suggested that cloud service providers be made to comply with industry regulations and laws related to protection of the client's sensitive data. In addition, cloud providers have to conduct both external and internal audits to assure that risk management actions, related to information security, build on best practices.

In the United States, cloud computing faces some legal restrictions. Currently, the U.S. lacks inclusive federal legislation for protecting personal data and consumer's

privacy; King and Raja (2012) pointed out the country also lacks regulation applicable in limiting exportation of sensitive data to other countries from the United States.

Furthermore, a federal regulation that categorizes which consumer data is sensitive, or one that delineates the type of enhanced information security and privacy protections required for sensitive data, is non-existent. Conversely, various federal regulations adequately identify the classification of sensitive customer data. For instance, the Children's Online Privacy Act defines sensitive data as information gathered by websites on children aged below 13 years, while the Gramm-Leach-Bliley Act considers data acquired by financial organizations on their customers as sensitive data (Sookhak et al., 2015). Similarly, the Health Insurance Portability and Accountability Act considers data acquired by healthcare providers about their patients as sensitive, while the Fair Credit Reporting Act categorizes consumer data as sensitive if credit reporting organizations gathered it. Businesses operating in these industries are subject to federal regulation in terms of gathering, processing, and disclosing sensitive data, including obligations for protecting the security and privacy of their consumer data. In general, regulations extend to the cloud environment for the industries under federal regulation.

King and Raja (2012) suggested that federal regulations require businesses operating in regulated industries to attain minimum-security standards and offer incentives for organizations that adopt specific security protocols. For instance, federal law requires healthcare providers to offer security for personally identifying health information about customers; Leonard (2014) pointed out they are not obligated to use encryption mechanisms for such information. Still, Thompson, Ravindran, and Nicosia

(2015) explained that if the healthcare provider uses adequate encryption standards and a data breach occurs leading to illegal access, healthcare providers are not required to report such breaches to a government agency or the consumers due to the assumption that adequate encryption would ensure the breach does not lead to harm. Therefore, businesses can decide to encrypt sensitive data to avoid the possible loss of its customers and the expenses associated with reporting security breaches.

If a specific industry lacks legislation requiring security and data protection, businesses utilizing cloud computing are under no legal obligation to ensure the security and privacy of personal data. This lack of legal obligation includes personal data used for business purposes not defined as sensitive and not protected by legislation in the United States, such as race or sex, income level, email addresses, residential addresses, and the names of the consumer (King & Raja, 2012). Despite the lack of a single legislation dealing with consumer data protection, the security of consumer's personal data is still achieved by consumer protection laws, privacy tort laws, and data breach notification regulations at the state level.

In the United States, the majority of states have established statutes for data breach notification; these statutes obligate organizations to notify customers when security breaches occur, even though no federal regulation requires data breach notification. State law describes the consumer data categories that meet requirements for breach notification; Smith (2016) suggested these state laws facilitate the identification of sensitive data in order to prevent identity theft. These regulations aid in protecting consumers from harm associated with data breaches because businesses are encouraged

to use security mechanisms, even though the regulations normally do not offer directives for particular security protocols. Erdos (2014) explained that firms that fail to comply with laws on breach notification face legal risks, including criminal penalties and civil proceedings.

Tort laws at the state level offer further protections for information security; they enable remedies for consumers when organizations misuse their sensitive data. There is still uncertainty about applying tort law to address an organizational failure to secure consumer's sensitive data. Consumers still use civil proceedings to deal with organizations who fail to provide adequate security for personal data (King & Raja, 2012). Many consider tort law an ineffective mechanism for protecting the security of sensitive data because of the difficulty to establish proof of economic harm.

Businesses utilizing cloud computing also have to determine if customers have remedies based on laws for consumer protection. For instance, Wheatley (2014) detailed that an organization can contravene section V of the Federal Trade Commission Act by failing to offer sufficient security for sensitive information in the cloud, enabling access to unauthorized individuals. This failure equates to a violation of consumer protection, even when the business has failed to adopt an information security policy required for providing protection of sensitive data. In addition, Wheatley (2014) went on to explain that an organization is in violation of the Federal Trade Act by promising to offer security and privacy of sensitive data and failing to fulfill such promises. In this context, a consumer can bring complaints before the Federal Trade Commission, asking this agency to pursue enforcement action against a business violating the relevant regulation.

Evidently, there is a lack of comprehensive legislation for protecting the security of sensitive data in the cloud environment, which means that cloud service providers are free to design their privacy and security protections. The non-existence of an inclusive regulatory framework in the cloud environment might lead cloud providers to establish low boundaries for data security; cloud providers can also outline service level agreements that reduce their legal burden when they fail to provide sufficient security (Bacon, Eyers, Pasquier, Singh, Papagiannis, & Pietzuch, 2014). For instance, such agreements may fail to address the mechanisms put in place for dealing with insiders and focus only on external hackers. Therefore, cloud service clients have to ensure that service level agreements established with the cloud service provider are comprehensive enough to protect sensitive data and define the legal responsibilities of the cloud service provider.

Furthermore, regulations in the United States do not place restrictions on the exportation of personal data to other countries; Fernandes et al. (2014) pointed out this failure to place restrictions allows cloud service providers the freedom to transfer data to computer servers found in various countries and further creates legal compliance issues, as legislation does not mandate cloud service providers (King & Raja, 2013; Whitley, Willcocks, & Venters, 2013). Moreover, this failure in regulation exposes sensitive data to insiders or outsiders found in different countries. Thus, the service level agreements between the client and cloud service provider should have provisions for transferring sensitive data to other locations.

Incident response. In a management system for information security, incident response is required, underscoring its relevance in the cloud system. In this context, there are needs for an incident response process that considers the tools, processes, and programs in the cloud system. When a security event appears, guardians should undertake suitable actions to discover the circumstances that led to the incident. Due to the architecture of the cloud systems, such as multi-tenancy and high scalability, it poses challenges to conducting digital forensics and determine the vectors of the attack (Ghilic-Micu, Stoica, and Uscatu, 2014). Kalloniatis et al. (2014) asserted a robust forensic framework must have the ability to perform verification of a security incident, to analyze the attack, and to restore secure service. In the cloud-computing context, it is important to put in place an incident response framework that covers detection and response to security incidents.

Technical strategies. Technical strategies address issues with access management. Preventative measures for technical control include application security; encryption and key management; identity, entitlement, and access management; and virtualization. Lian, Yen, and Wang (2014) considered technical strategy a critical role for security dimensions in cloud computing, including areas of privacy and confidentiality, data segregation and integrity, and availability. Further methods to implement technical strategies include encryption and key management; information management and data security; and identity, entitlement, and access management. If all

those methods fail, disaster recovery is a necessity. All of these strategies continue in detail below.

Encryption and key management. The encryption and key management dimension consider the importance of encrypting data to minimize possible data leakage, specifically relevant in the context of cloud computing. Lian, Yen, and Wang (2014) explained that encryption describes a process of information encoding meant to ensure only legal users have access to certain data. There are concerns about the process of encrypting data in the cloud. Chen and Zhao (2012) suggested that the multi-tenancy characteristic of the cloud environment means that when a cloud application processes and stores data from various users, the presence of unencrypted data poses a serious security threat.

Therefore, researchers have proposed solutions to ensure data security in the encryption process. For instance, Crete-Nishihata, Deibert, and Senft (2013) explained *private information retrieval*, a proposed technical mechanism that hides queries performed on encrypted information in the cloud. Conversely, the authors considered this approach as being very expensive in relation to computation costs. Chen, Violetta, and Yang (2013) confirmed that the majority of the available encryption mechanisms fail to support data processing within the encrypted medium. Chen et al. (2013) further claimed that role-based access control (RBAC) would facilitate a superior technical strategy in securing data. Consequently, researchers Wheeler and Winburn (2015) suggested homomorphism encryption: a solution that allows secure processing of encrypted data in the cloud environment.

A privacy manager is an integral part of encryption and key management. Li et al. (2014) pointed out a privacy manager also operates as a security mechanism for processing encrypted data. In this context, the privacy manager uses obfuscation methods to reduce the personal data found in the cloud, minimizing the risk of data leakage. The idea behind this approach is to store the client's sensitive information in an encrypted format while still allowing processing on this data. The restriction is that the cloud service provider must be willing to execute this mechanism to guarantee the security of sensitive information. The privacy manager shares their security strategies with informal and formal mechanisms.

Encryption approaches are another important strategy. Wei, Zhu, Cao, Dong, Jia, Chen, and Vasilakos (2014) suggested that encryption approaches, such as asymmetric or symmetric encryption algorithms, prevent illegal access to personal information in the cloud. A healthcare organization successfully implemented this technique when they moved their sensitive data to a commercial cloud provider. In addition, Wheeler and Winburn (2015) felt that the encryption standards established by the NIST protect the confidentiality and privacy of sensitive information in the cloud environment. Kazim and Ying (2015) felt that encryption techniques that preserve the format of data, as well as those that are aware of the format or type of data and context of data usage, are critical in the cloud. Management of the key is a challenging process in a cloud environment, especially of those utilizing the multi-tenancy framework. In this domain, an organization has to address various issues, including safeguarding and storing keys, practices in key management, and reliable cryptographic services (Kalloniatis et al., 2014).

Information management and data security. In cloud computing, data is critical, and its protection in the context of multi-tenancy is vital. Kalloniatis et al. (2014) pointed out that protecting such data occurs through protection of the physical and virtual networks, data cryptography, data backup, and data segregation and integrity. Crete-Nishihata et al. (2013) and Kalloniatis et al. (2014) felt that IT security managers should consider robust cryptography, sanitization, suitable maintenance of hardware, and effective computation methods when managing the life cycle of cloud data. This approach is necessary for addressing various security threats, including data leakage, insiders, and insecure interfaces. This domain highlights the relevance of information management in the cloud, involving policies and processes for creating, storing, using, sharing, archiving, and destroying information. Roy, Sarkar, Ganesan, and Goel (2015) pointed out the identification and control of access to data stored in the cloud is necessary for both external and internal users to achieve successful information management.

Identity, entitlement and access management. Identity, entitlement, and access management appear to best suited for IS managers to include in their technical strategies. In cloud computing, a transformation of identity management includes entitlement in the process of managing access (Kalloniatis et al., 2014). Particularly, Kazim and Ying (2015) suggested cloud applications and services use different sources in identifying users; management of entitlement offers a decision process to authorize access to the cloud's data, processes, and system. This domain focuses on all identity types significant for cloud computing, including agents, organization, code, device, and users. Brandas, Megan, and Didraga (2015) considered the two important elements to ascertain these identity types are, first, the strengths of the attributes and, secondly, the identity expected to offer higher flexibility within the cloud. In the cloud, access covers data to process, application, system, and network dimensions. The process of entitlement has to ensure that linkages exist between the users' security needs and business needs by using rules to govern access to various cloud entities.

Traditional security, business continuity, and disaster recovery. The innate security concerns attributed to cloud computing require the identification, assessment, and control of business continuity. The continuity requires suitable safety measures vital for managing security risks and assuring information availability, integrity, and confidentiality. Kazim and Ying (2015) argued the cloud services have to be continuously available to the cloud users and, in the case of interruptions, the cloud service provider should have a robust recovery system to ensure continuity of normal business operations. Service availability is critical; Kshetri (2013) pointed out that the breakdown of continuity in cloud services might lead to the closure of cloud users' normal businesses. Such breakdown attributes to either failure in the cloud hardware or attacks. In the cloud, disaster recovery and data backup are required for supporting reliability in data transition and protection. Thus, full virtualization of the data storage structure and scalability of recovery applications and file systems are required for disaster recovery and continuity of business operations in the cloud.

Complexity of Strategies in Cloud Computing

In the cloud-computing environment, security is a complex concept. In order to address these issues, solutions often require a combination of informal, formal, and technical strategies. These combined strategies reflect the characteristics of the cloud-computing environment and feature in the subsections that follow.

Privacy and confidentiality. Confidentiality is data access by authorized systems or parties only. The possibility of a data breach is high due to an increase in the quantity of applications, devices, and involved parties; this possibility results in more

opportunities for unauthorized access. Zissis and Lekkas (2012) claimed the multitenancy, application security, and data eminence making up the cloud environment increases confidentiality and privacy risks. Multitenancy, as defined by Elhaida and Frueh (2015), is a characteristic that shares resources among different clients. In the context of cloud computing, users share data, networks, programs, and memory.

Cloud computing resource shares at the application, host, and network levels. Virtually, the users are separate but still share the cloud system hardware. Because of multitenancy, security and privacy risks, where users access client's data stored in the cloud without authorization, are high. (Mouratidis, Islam, Kalloniatis & Gritzalis, 2013). Meanwhile, data confidentiality can occur because of data eminence. Zissis and Lekkas (2012) described data eminence as the lingering illustration of data ostensibly erased. In the cloud-computing environment, the logical drives are virtually separate, but the hardware remains unseparated between multiple users on a single cloud infrastructure. Therefore, data eminence might result in unintentionally disclosing sensitive information (Zissis & Lekkas, 2012; Roy et al., 2015).

In the cloud, data confidentiality requires user authentication. To this end, electronic authentication determines the authenticity of user identities electronically presented within an information system. Dawson (2015) noted that privacy breaches occur when a robust electronic authentication is lacking, resulting in unauthorized access to a client's account. Further, cloud system security entails software confidentiality, which relates to the belief that particular processes and applications should maintain and handle a client's sensitive data. Within a cloud-computing environment, clients delegate

confidence to the applications offered by the firm that owns the cloud system. Therefore, the applications that interact with the client's information should achieve certification to avoid further privacy and confidentiality risks (King & Raja, 2012; Elhaida & Frueh, 2015). This unauthorized access occurs when users exploit vulnerabilities in the software or applications.

Data integrity and segregation. Users can easily realize data integrity in single systems, but cloud computing necessitates the use of several databases to store data for multiple users; as a result, it is challenging to assure data integrity. Zissis and Lekkas (2012) referred to data integrity and segregation concept as the fortification of sensitive information against unauthorized fabrication, modification, or deletion. Thus, authorization is important to guaranteeing data integrity; it ensures that only authorized clients can access sensitive information.

The cloud environment possesses some degree of virtualization; normal methods to maintain data integrity, such as hypertext transfer protocol, are unlikely. Thus, achieving data integrity occurs by implementing it at the Application Programming Interface phase (Hemalatha, Jenis, Donald, & Arockiam, 2014). On the other hand, Mouratidis et al. (2013) realized this approach could further complicate security measures by creating potential vulnerabilities in the API technology, or the API stack itself. These vulnerabilities provide attackers with opportunities to intercept sensitive data and modify it, resulting in further data corruption or theft (Hemalatha, Jenis, Donald, & Arockiam, 2014).

Multi-tenancy is the lead charge for cloud computing providers. Cloud computing is characterized by multi-tenancy; Hart (2013) pointed out multiple users store their sensitive data in the applications of service delivery models. In this context, several users' data exists in one location, making data intrusion by one of the users a possibility. Data intrusion transpires by injecting a client code into the cloud system, or hacking vulnerabilities found in the application. Thus, cloud services should assure boundaries for client data at the application and physical level.

The security strategy for cloud service must be able to segregate data from multiple clients. Malicious users can use application vulnerabilities to develop parameters that can bypass security checks and provide access to user information (Hemalatha, Jenis, Donald, & Arockiam, 2014). Riungu-Kalliosaari, Taipale, and Smolander (2012) suggested that security managers could test and validate data segregation in the cloud environment using assessments such as insecure storage, data validation, and SQL injection flaws. Vulnerabilities identified with these tests might gain attackers unauthorized access to a client's sensitive data. For instance, Chang et al. (2016) detailed how a security defect found in Google Docs exposed credentials to other users. The occurrence of this security problem was due to flaws in session allocation, and it demonstrated the importance of data segregation to prevent data leakages.

Data center operations. The successful functioning of a data center requires the deliberation of various strategies. Those strategies include assessments of cloud service provider's operational procedures, the architecture of the data center, and its dissemination of security strategies (Islam et al., 2013; Kalloniatis et al., 2014). The data

center is a fundamental element in the operations of the cloud environment because it hosts the cloud's applications. Cloud service users need lasting stability and continuous services associated with the features of the data center. Tankard (2015) suggested other related issues under the data center domain include service management requirements, regulatory requirements, security standards, and the data center's location.

Knowledge Gap

Some literary works addressed informal, formal, and technical strategies, but none of them addressed a combination of all three. In short, of the six papers relevant to this study, none sufficiently offered strategies IT security managers should use to protect information in the cloud. The evidence of this statement details in the following table.

Figure 2: Table of Relevant Studies and Findings

Author(s)/Year	Informal	Formal	Technical	Significant Findings
Gonzalez et al. (2012)	X			Surveyed regulatory & legal issues to determine whether the responsibility of information security fell with the cloud service provider or the customer.
Soomro, Shah, & Ahmed, (2016)	X			Characterized cloud security issues into three categories: data control by a third party, availability issues, and conventional security challenges.
Hong & Rong (2014)		X		Recommended the cloud be consistent with usage policy.
Lin et al. (2014)		X	X	Examined security issues around privacy, data control, data integrity, data confidentiality, and data availability.
Rizvi & Mitchell (2015)	X		X	Surveyed privacy and security issues in cloud computing, offered guidelines for firms that planned to use cloud services.
Shah et al. (2013)	X		X	Presented a survey of security concerns in various cloud service levels, namely IaaS, PaaS, and SaaS.

Empirical studies have examined the issue of security in the cloud-computing context. For instance, Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Naslund, and Pourzandi (2012) surveyed the regulatory and legal issues in cloud computing to determine whether the responsibility for information security is with the cloud service provider or the customer. Other researchers, Shah, Anandane, and Shrikanth (2013), addressed the security concerns in the cloud environment by categorizing them into security issues associated with data control by a third party, availability issues, and conventional security challenges in cloud computing. The researchers outlined potential directions to alleviate issues in data control and establish the different categories of auditing in the cloud-computing environment. First, the researchers identified a need for a trusted monitor within the cloud server; this monitor would facilitate auditing of the servers' actions and provide demonstrable proof of security-auditing compliance to the client. Second, data organizations store in the cloud should be self-protecting with the capacity to establish a secure environment. Hong and Rong (2014) recommended this necessary environment be consistent with a usage policy.

In another study, researchers Lin, Lin, Chou, and Lee (2014) examined the security issues of privacy, data control, data integrity, data confidentiality, and data availability in the cloud environment. The authors also looked at how cloud service providers are dealing with security issues, such as data control, data integrity, confidentiality, and availability. The researchers proposed a strategy: security auditing should occur at the software level of the virtual cloud system, with the system providing minimum monitoring of logs and events. Researchers Rizvi and Mitchell (2015) surveyed

privacy and security issues associated with cloud computing, offering guidelines for firms that planned to use cloud services. In a different study, Shah, Anandane, and Shrikanth (2013) presented a survey of security concerns in various cloud service levels, namely infrastructure as a service, platform as a service, and software as a service. The researchers identified the different security concerns in these service models.

Evidently, researchers have conducted significant research to investigate issues around information security strategies in the cloud computing environment. These studies have not included security strategies from IT security managers, however. Therefore, I acknowledge a significant gap in knowledge, necessitating the need for further empirical studies. This study sought to fill this gap by examining the issue of information security in cloud computing from the strategies of IT security managers. As a result, I used a case study research design for this study.

Transition and Summary

The routine activity theory by Marcus and Cohen has tried to explain the occurrence of different crimes in the world. Though not necessarily applicable to all crimes, the theory has revealed the process of occurrence behind many criminal attempts. Generally, most of the studies carried out today show support to the theory (Reyns & Henson, 2015; Leukfeldt & Yar, 2016). The theory's focus was on computer victimization, which is on the rise and involves people of all ages. The theory considered and unpacked the factors fueling criminal occurrence; the theory concluded that a combination of factors leads to criminal occurrences. This conclusion has helped future research in dealing with security issues.

This section discussed literature on information security theory and strategies in the context of cloud computing. Particularly, the routine activity theory offered the framework that developed a conceptual model for this investigation. Moreover, the study so far discussed the routine activity theory, conceptual model, security strategies, internal and external attacks, and the complexity of security strategies. The next section presents the methodology employed to gather and analyze data used in response of the research question.

Section 2: The Project

Purpose Statement

The purpose of this qualitative, single case study was to explore the strategies that IT security managers use to host sensitive information in the commercial cloud. The research participants were IT security managers from a government agency in the eastern region of the United States with experience in implementing security strategies to host sensitive information in the cloud. The findings from this study may be beneficial for information security practice by increasing understanding of the complex nature of internal and external threats and breaches. The implication for positive social change lies in the potential to improve security of a user's private data while stored in the commercial cloud.

Role of the Researcher

In regards to my personal relationship with the subject, I work for the same agency under the Department of Defense (DoD) as the participants in this study but in an entirely different department. I have over 19 years of experience in both private and public sectors. I have been safeguarding compliance with valid DoD requirements and the use of current industry standards. For the last 6 years, I have performed as an Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) within the DoD spaces and infrastructures. During this time, I have been using National Security Agency (NSA) Configuration Management and hardening guidelines that include agency policies, IT/IS regulations, and current industry and NSA best practices. As an ISSM, I manage the ISSOs and ISSEs who analyze existing platform

accreditation needs by providing guidance to systems owners on the necessary DCID 6/3 requirements and NIST SP 800-53 controls. Also as an ISSM, I develop and write policies and procedures for the computer security department. Despite my experience with the topic, I still upheld myself to a set of standards to ensure the mitigated success of this study.

I prioritized adherence to the Belmont report. In addition to creating the interview protocol, I needed to create a comfortable environment and good rapport with my interviewees, as well as provide sophisticated questions, as suggested by Grenier and Dudzinska-Przesmitzki (2015). This environment ensured my compliance with the respect for persons' principle of the Belmont report (U.S. Department of Health and Human Services, 1979). I treated the participants as autonomous agents by using only volunteers, respecting their decision to leave at any point of the process. I developed the interview questions and disseminated those results. In the semistructured interview, I used objective questions, developed over time with expert help, to generate what Barnes (2015) calls the participants' subjective responses. These subjective responses remained confidential and secured under protective and encrypted formats to maintain my participants' well-being, ensuring my compliance with the beneficence principle of the Belmont Report. Finally, on the justice principle of the Belmont report, the burden of the study was minimal. The participants all worked in the IT field; they answered the same amount of interview questions. Therefore, the burden and benefit went to each person equally.

I took further precautions to minimize my personal bias. Faniel, Minor, and Palmer (2014) considered the researcher the main instrument for collecting and analyzing data. I recognized and considered personal predisposition and bias in the entire research process. As a result, I became a student who could learn with and from the study participants. I planned to mitigate my personal bias by remaining open to new thoughts on the study topic. Through this process, I sought to establish as much credibility for this study as possible.

Participants

The participants in this study included IT security managers with experience and expertise in cloud security issues. I selected all IT security managers from the government agency in the single case study, which was located in the eastern region of the United States, and they included managers using security strategies to host sensitive information in the cloud. These security managers managed cloud-based products, maintained safety on the cloud infrastructure, and maintained customer data. They had no less than 10 years' experience in IT management. These participants provided insights about internal and external data breaches in the cloud. The data provided by these participants were critical for responding to the research question and testing the theories guiding this study. I gained access to the participants by first meeting with the director of technology to explain the purpose of the study and obtain permission to interview the preselected IT security managers. I then accessed the IT security managers through e-mail contact.

I considered some of the necessary strategies to establish a working relationship with the participants. I could face many challenges concerning the participants' involvement, including their readiness to respond and their reluctance to participate in difficult environments (Fegran, Hall, Uhrenfeldt, Aagaard, & Ludvigsen, 2014). The strategic approach I used to remedy these challenges relied on Schreier's (2012) application of social skills, which aims at gaining participant trust with an informal use of language and particular dress code (Fink & Anderson, 2015). Belanger et al. (2013) and Fegran et al. (2014) also suggested formal strategies to adapt to the cultural norms of the research site, obtain permission to tape record interviews, and take into account the differences in languages and accents. Meanwhile, the informal (personal) strategies include awareness of cultural practices, values, and norms in the research area, as well as adapting to the participants' language (Fegran et al., 2014). Given that the efficiency and effectiveness of the participants' answer to the research question depended on their overall impression of the researcher, I maintained high ethics and social skills to win their trust and acceptance.

Research Method and Design

In this section, I expand on the research methods I adopted, focusing on the suitability of qualitative practice in study methods. In addition, I explain why quantitative and mixed methods were not suitable for this research study.

Research Method

The research method was qualitative. Vaismoradi, Turunen, and Bondas (2013) defined the qualitative method's focus on describing the meaning, concepts, elements,

symbols, and definitions of a phenomenon. The data sources used in a qualitative method include observation, documents and texts, and interviews. Further, qualitative researchers build on the constructivist philosophy, which considers individuals central in the creation of social reality; this philosophy requires me to adopt an empathetic stance to understand social reality from the participants' point of view. It also forces me to consider my own subjectivism, or my perspective about the social world in qualitative studies.

Recognizing my subjectivism played a key part in formulating the objectivity of this study. Endres and Weibler (2016) argued that social actors influence social phenomena through interactions. In order to understand the phenomena, I investigated the subjective meanings influencing individuals' actions. Under subjectivism, researchers consider reality a social construction that individuals create when they attach meaning to situations. Consequently, qualitative methods can be used to uncover the subjective meanings that individuals attach to phenomena.

The qualitative method also employs an inductive approach, or data gathering and analysis to aid theory development. Harrison and Kirkham (2014) elaborated on the inductive approach, pointing out how it can be used to prioritize a deeper understanding of how individuals interact with the world. This deeper understanding unfolds by collecting qualitative data using few research participants rather than large samples (Harrison & Kirkham, 2014).

I considered the quantitative method. Quantitative researchers build on the positivism epistemology, where researchers apply principles of natural science to examine a study issue. Yilmaz (2013) pointed out that the positivism epistemology uses

current theory to formulate hypotheses. The researcher tests and validates the formulated hypotheses. Epistemologists emphasize quantifiable data to carry out statistical analyses.

Objectivism guides quantitative research. According to objectivism, social actors are not involved in creating reality. As a result, I should employ naturalistic methods to gather knowledge. A researcher employing the quantitative method adopts an objective stance in the study and respondents provide anonymous opinions to the research issue using a survey questionnaire (Haegele & Hodge, 2015).

Finally, the quantitative method relies on the deductive approach, where hypotheses are tested based on the rules of natural science. Deduction includes a concentration on explaining study variables' relationships through the development of hypotheses, data gathering, and hypotheses testing. Scholars use the deductive approach controls to test propositions, ensuring changes occur between variables in the proposed relationship only, and not because of other intervening variables. Deduction requires me to employ an effectively structured research methodology; Yilmaz (2013) suggested this structured research methodology ensures reliability and replication of the research.

Another aspect of this approach operationalizes constructs to support their measurement in quantitative terms. In this regard, I should ensure that I define all of the study variables before conducting scientific analysis on them (Hughes & Short, 2013). I did not select the quantitative method for this study because the deductive approach was not applicable; I was exploring the answers to open-ended questions and was not seeking to formulate and test a hypothesis.

I also considered mixed-methods research. Mixed-methods research is an amalgamation of qualitative and quantitative methodologies. Yeh et al. (2013) argued that mixed-methods approaches include a combination of the best of both quantitative and qualitative methods by compensating for paradigmatic restrictions found in a single method. Yeh et al. proposed that mixed-methods research provides maximum elasticity for a researcher. Daigneault and Jacob (2013) claimed that the mixed-methods approach uses numerous viewpoints, involves large collections of data, requires extensive analysis, calls for skilled interpretation of procedures, needs comprehensive commitments of scope, necessitates profundity of understanding, and requires validation. Mehl-Madrona, Mainguy, and Valenti (2013) argued that adequate researcher knowledge of both approaches can help to ensure effective conceptualization and implementation of mixed-method designs, preserving the strengths of each in any given research endeavor. As a beginning researcher, however, I found the qualitative research method an accessible and effective approach for a first-time research study meant to observe formal, informal, and technical strategies to secure cloud data.

Based on the examination of the differences between quantitative and qualitative methods, I relied on the qualitative method. I used the qualitative method to explore what strategies IT security managers use to host sensitive information in the commercial cloud and how those strategies have been effective or ineffective. Therefore, using the qualitative method enabled me to obtain insights I could not have acquired using a quantitative method. In addition, the qualitative method allowed me to adopt a subjective

stance while interacting with the participants in data collection; these data determined IT managers' strategies for protection from insider and external threats in cloud computing.

Research Design

I used the case study design in this study to address the research questions adequately. Tsang (2014) surmised that the case study is preferable when investigating a contemporary event without manipulating the relevant behaviors. In addition, Wohlin and Aurum (2014) explained that a case study's strength is how it provides scholars with the ability to explore various evidence sources, including observations, interviews, artifacts, and documents. The case study's design supports the exploration of an issue through multiple lenses; the result is that the case study design enables the discovery and understanding of multiple components of a phenomenon. Furthermore, Bjercknes and Bjork (2012) pointed out that the case study analysis includes an exploratory approach that does not carry the consequences of extensive research found in alternative qualitative approaches like ethnography, narrative, and phenomenological studies.

The case study approach avails as an important tool in carrying out social science research; it provides the descriptive accounts of one or more cases. Qi and Gani (2012) highlighted how I could apply the case study approach intellectually and experimentally to isolate one or more selected social factors within a real-life context. In IT, the application of this technique is important in the sense that it ensures comparison between past and current events. That way, I can draw the best solution.

A case study is a valid tool in the conduction of research. For instance, the case study has many advantages, such as forming a point of reference to rely on in challenging

theoretical assumptions and when studying rare phenomena. Some fields rely on the case study approach. Organizational theorists, for example, rely on the case study as a way of challenging underlying assumptions. The application of the case study in this research acted as an approach to challenge theoretical studies. The case study is one of the most flexible study designs; Stake (2013) illustrated its applicability in exploring different theoretical predictions founded upon set theoretical frameworks. A case study is suitable to analysis and general interpretation. The approach presents lower levels of validity as well as reliability. Lee et al. (2013) pointed out the process of gathering data may take a considerable amount of time. Stanley and Nayar (2014) echoed Lee et al., noting that for in-depth analysis to occur, scholars must interview participants for 1 to 2 hours, multiple times. The extensive time requirements of phenomenology to achieve data saturation means was not viable for this study.

I did not use an ethnographic study. Schober, Gerrish, and McDonnell (2016) asserted ethnographers qualify data based on personal observation and depicted events. Lewis (2015) suggested that ethnographic studies also include shared accounts to draw descriptive conclusions about a particular culture. An ethnographic study's disadvantages made it less appropriate for this particular research, however. For instance, Yin (2013) pointed out that the ethnographic technique requires a substantive amount of time. This challenge did not necessarily render the method unsuitable for conducting research because I could have accomplished the completion of some ethnographies in a reasonable amount of time. De Costa (2014) explained that the longer the length of time taken during a research study, the more the information gathered on the topic in question.

Ethnography's insight into consumer behaviors proves valuable, and I used data collection methods familiar to ethnography, including interviews and direct observation. Hjorth and Sharp (2014) suggested that there is a difference between borrowing from ethnography and doing an ethnographic study. Ethnography narrows from a particular kind of participant observation with anthropological roots (Baskerville & Myers, 2015). I did not use ethnography because I did not study workplace culture. I did not directly observe how the participants interacted within their workspace; instead, I explored the strategies that IT security managers use to protect the cloud environment. I trusted that their experience, coupled with member checking, would establish the validity of the themes.

Finally, I did not use the narrative approach in this study. The narrative approach includes photos, diaries, and recounted interviews to create stories of to form meaning (Alves et al., 2013). Lewis (2015) described the narrative study as unanalyzed stories and accounts using interviews, notes, letters, and conversations put together by a researcher. The use of the allegorical account is this approach's greatest strength; it gives an account of a situation and captures the necessary information around the issues the participant and researcher discuss. The narrative study ensures that a scholar fully captures the situation. The strength of the narrative approach is its capability of chronologically identifying the different issues that make up a situation. Lewis (2015) pointed out, however, that the disadvantage of using narrative inquiry is that it changes its explanations and frames of orientation. This disadvantage was counterproductive to the study's goals.

Saturation of data was an important aspect of this study. Lee et al. (2013) suggested that when researchers reach the point of theoretical saturation during the analysis process, they should conclude the analysis. Data saturation occurs when I am unable to cover new information, coding, or themes, and other researchers are able to replicate the findings (Fusch & Ness, 2015). The research design elements of a case study include the research question, units of analysis, proposition, link between the proposition and the data, and the criteria for interpretation of the results (Hassan, Reza, & Farkhad, 2015). I familiarized myself with the interview data and triangulated the participant responses with field notes from the direct observation of a training seminar and organizational policies and documents. I processed this information into interpretations during the data analysis process. I met with the participants again to share the interpretations. This second meeting was meant to increase the study's chances at data saturation. Data saturation occurs when no new information or themes surface (Fusch & Ness, 2015). The participants either corroborated or added their own experiences to the interpretations; this process was member checking. Houghton et al. (2013) suggested that member checking would be more helpful in increasing the rigor of the study because participants are more likely to contend or contribute to their ideas when I interpret them as opposed to when I repeat their statements verbatim. I completed as many member checking interviews as necessary until the participants had no new information to offer, thereby helping to enhance data saturation. I stopped reviewing here due to time constraints. Please go through the rest of your section and look for the patterns I pointed out to you. I will now look at Section 3.

The units of analysis in this study were the elements the selected IT security managers identified in a discussion about cloud security. Specifically, the items examined in this study related to vulnerabilities in cloud computing, types of insider and outsider attacks in the cloud, impacts of external and internal attacks, and security challenges the IT security managers faced. Finally, linkages between the theories and data came together through qualitative data analysis. Notably, a thematic analysis aided in data analysis, and I used the findings to explore identified theories.

Population and Sampling

Snowball sampling is a type of non-probability sampling approach to choose potential participants in a study. It is commonly used in cases where it is difficult to locate the participants (Lecy & Beatty, 2012). Snowball sampling is appropriate if the study sample is rare or limited to a small subgroup of the population. The sampling method is similar to a chain of referral. Once I observe initial participants, I request their assistance to identify people with similar interests. The procedure of snowball sampling requests participants to nominate another individual with the same interest as the subject. Then I observe the nominated participants and continue until I achieve the required sample size. For instance, to obtain consensus sampling for this study, I asked Participant One about other potential participants. Participant One stated that there were there were 10 ISSM managers for the from a government agency in the eastern region of the United States that were all members of the ISSA. Using Participant One's information, I was able to contact other ISMM's. Out of the 10 ISSM's, 3 did not participant, while 7 respondents contributed to this research. Although snowball sampling gives me less

control, the chain of referral enables me to contact people of the population that are hard to sample. Snowball sampling is suitable for this research because it is not only cost efficient but straightforward. Unlike other sampling techniques, snowball sampling requires less planning and fewer research assistants.

Ethical Research

The term *consent* in research refers to a state where the participant is free. Johnson et al. (2014) pointed out that people taking part in a study have the freedom of acting according to their own wishes. Drazen et al. (2013) expounded, suggesting it is the participant's right to know the objectives of the study, as well as the potential risks and benefits that go along with it. If I clearly inform the participant about the study, the decision to participate should hinge on the feelings that participant has towards the study. Participants might refuse or agree. The importance of this policy is that I respected the participant's rights.

Once selected, a person could have chosen to withdraw at any time from this study. I accomplished this withdrawal process in an official way to ensure I followed certain procedures. Zhang and Creswell (2013) asserted that the withdrawing participant should inform the chief researcher about their change of plans. The factors that led a participant to decide to withdrawal vary from one person or another. However, in the interest of maintaining the ethics of the Belmont Report, all participants could leave the study freely at any point. I asked that the participant inform them of their intent to leave in the consent form, at which point I would acknowledge and respect their choice.

Before providing consent, I briefed the participants on the significant information related to the research. This information included the participants' responsibilities, any risks in the study, research objectives, and the way I used the information I collected. Furthermore, I informed participants of their freedom to stop participating in the study, devoid of negative repercussions. I captured all this information in a consent form located in Appendix A. The participants signed the consent form before the interviewing process began. Furthermore, the consent document stated the research posed no risk to the participants; I asked them only to share their experiences and perspectives about the study topic, without revealing sensitive information. Nishimura, Carey, Erwin, Tilburt, Murad, and McCormick (2013) found low participant-risk an important part of the research process.

Another issue captured in the consent document was that I did not provide the participants monetary benefits for participating in this investigation. Researchers allot incentives to participants through two main ways: the researcher gives something to all people taking part in the study, or the researcher rewards after dividing participants into a group, thus issuing the award to the group (Harriss & Atkinson, 2013). In this study, I did not use rewards. I encouraged participation to be voluntary. I informed the participants, however, that their involvement in the study could benefit other IT security managers in cloud computing. The participant information may help provide improvements to the security of sensitive information hosted in the cloud environment.

In this research study, I wanted to ensure that I gave the participants adequate ethical protection. Lewis (2015) recommended defining how I will maintain privacy and

confidentiality when researching to establish ethical protection. Confidentiality maintenance is crucial because it builds a trustworthy relationship between the participant and myself; it reduces participant concern. Wanting to adhere with Belmont principles, I maintained the participant's dignity. One of my goals in achieving participant confidentiality was to avoid revealing the names of the participants. Marshall and Rossman (2016) stated that unless given an order by the government, the student should make sure that nobody receives permission to gain access to the participants' names. In short, I was obligated to keep their information safe.

Considering the fact that I collected and recorded data, I intended to treat the information I collected with confidentiality. Confidentiality entails the protection of the participant's identity in a study (Gergen, Josselson, & Freeman, 2015). Doody and Noonan (2016) suggested the researcher protect participant identities with codes. I kept these codes (Participants A, B, and so on) on an excel spreadsheet encrypted with Viivo encryption software. I stored the encrypted document in a Dropbox to ensure that the data would not be lost. Schmidlin et al. (2015) recommended that I hold participant information for 5 years. I held their information for 5 years, and then I destroyed all data. I conducted this study under Walden IRB approval number 11-14-16-0457592.

In this qualitative research, I employed two strategies to make sure the identity of participants and organizations were confidential. The first strategy ensured I ignore instances where I could use names in the report. Gutmann (2014) assured generalization of the participants is one of the best ways to achieve confidentiality. The second strategy, as I have mentioned previously, required codes. I assigned the participants code names

entirely different from their original ones. I also assigned organizations names in the form of letters. For example, organization A, organization B, and so on.

Data Collection

Elo et al. (2014) defined data collection as the systematic process of gathering ideas on a study's meaning, concepts, and definitions of a phenomena; this information answers the research questions and evaluates the outcomes. I used semistructured interviews and analysis of organizational policies and documents. I used the organizational policies and documents for triangulation purposes of the semistructured interview. In the following three subsections, I discussed the instruments, collection techniques, and organization techniques that went into the data collection process of this study.

Data Collection Instruments

The researcher is the main instrument used in the process of data collection (Yin, 2013). In a qualitative study, I have to recognize my role as the primary instrument in order to ascertain any assumptions that might keep me from achieving as much objectivity as possible (Barnham, 2015).

Lim et al. (2013) and Yin (2013) also suggested that a collection of evidence should include a minimum of two of six sources. These sources comprise of direct observation, documents, physical artifacts, interviews, archival records, and participant observation (Yin, 2014). In addition to myself as the researcher and the primary data collection instrument, I used semistructured interviews, direct observation field notes, and analysis of organizational policies and documents.

The main instrument I used are the semistructured interviews. Mendoza (2014) suggested that a good instrument considers construct, validity, reliability, and design. An interview protocol helped me better adhere to these four criteria. Thus, I conducted interviews following the interview protocol presented in Appendix B. Petty, Thomson, and Stew (2012) made clear that I am supposed to ensure that all questions I ask are the same for all participants. Following the interview protocol helped ensure I was asking all the participants the same questions, thereby improving the reliability of my semistructured interviews; I also planned to use member checking follow up interviews for the same goal. The original interview questions are located in the *Research Question* section of the study.

Hyett, Kenny, and Dickson-Swift (2014) suggested that a researcher should choose observation as an instrument because evidence arises by watching participants more than listening to them. Furthermore, Houghton et al. (2013) surmised that observation opens me to collecting data, such as verbal and physical behavior, in a natural setting. I prioritize the communication I expect to have with the participants in the semistructured interviews of this study. I do argue, however, that I can supplement those conversations with observations and conversations in a natural work setting. I used direct observation field notes as a second instrument. I observed a quarterly security training meeting. The meeting was a security training session led by two ISSMs. The audience included SharePoint and web designers, system administrators (SA), network administrators (NA), information system security engineers (ISSE), and information system security officers (ISSO).

Document analysis is the methodical evaluation of documents both virtual and in print (Vaismoradi et al., 2013). I used organizational documents and policies as the third instrument of this study for triangulating purposes, hoping it could provide insight, clarification, or confirmation to the responses I collected in the semistructured interviews. Vaismoradi et al. (2013) suggested that I could be more confident in the credibility of my conclusions if the documents corroborate me. I therefore hoped that document analysis, paired with the field notes from the direct observation of a government training meeting, would enhance the overall validity and reliability of the study.

Data Collection Techniques

Semistructured interviews were the primary method of data collection. I used an interview protocol, located in Appendix B, to gather data from the research participants. The interview protocol contained instructions that should take one to two hours. I decided on this time to provide the participant an adequate amount of time for their subjective responses. The instructions I developed in the interview protocol included the open-ended questions and prompts to remember, such as a prompt to watch for nonverbal cues and probe for clarity.

The process of qualitative interviewing begins when the I explain the purpose of the investigation to the sampled participants (Petty et al., 2012). I read the consent document to the participants to ensure they understood what I expected of them in the data collection process. The participants signed the consent document. After the participants met the consent document requirements, I obtained permission from each participant to audio record the interview session, then posed the open-ended questions

(section one). Taylor et al. (2016) claimed that open-ended questions encourage discussion on the research topic. In addition to these open-ended questions, I used probing questions to encourage deeper interpretation of the participants' responses. Franke et al. (2015) suggested that probing questions illuminate a particular answer for clarification. I used rephrasing techniques to ensure that I accurately captured the participants' meanings. After exhausting all the open-ended questions in the interview protocol, I thanked the participants for their time.

When the interview process was complete, I performed member checking within ten days of the original interview. Member checking occurs when the researcher offers up findings for the participants to validate (McConnell-Henry et al., 2011). The participant and I completed another interview for the purpose of member checking. The interview protocol provides instructions for the member checking interview as well. In the follow-up interview, I shared a concise summary of the responses from the original open-ended questions and allowed the participants to respond. The participants either confirmed or corrected my interpretations. I also clarified any unclear points that might have impeded data interpretation. If it was necessary, I scheduled another member checking interview with the participant to go over the summaries I discovered in the first and subsequent interviews.

I used direct observation and organizational documents to triangulate the data with the data from the semistructured interviews. Stuckey et al. (2014) pointed out that direct observation can correlate or complicate information from a semistructured interview, while also clarifying particular workplace behaviors. I used direct observation

by attending a quarterly training session to observe organizational strategies to secure the cloud environment. I took direct observational field notes during the session. Anderson et al. (2014) suggested a researcher using organizational policies as a data collection technique is better able to recognize, record, and relay organizational practices with better environmental and contextual background. I used organizational documentation to elucidate any strategies relating to privacy, strategy, and data security in the commercial cloud. The organizational documents are available publically through the National Institute of Standards and Technology (NIST) and the United States D.O.D. Chief Information Office websites. I received all other documents with permission from the organization's Director of Technology.

Data Organization Techniques

I recorded the interview data in an audio format that required transcription. The transcription process involved converting the audio-recorded interviews into an accessible and readable format. I completed the transcription process within ten days of initial data collection. Sloan and Bowe (2015) argued that data analysis begins by repeatedly exposing one's self to the data via the transcription process. Therefore, I familiarized myself with the data through the transcription process. I typed out the interviews and placed them in data storage for protection.

Houghton et al. (2013) also suggested I create a database for recording the raw data to transcribe the interviews and store field notes. I kept the interview information on an Excel spreadsheet encrypted with Viivo encryption software. I stored the encrypted document in a Dropbox to ensure that the data would not be lost.

I maintained hard copy notes from the semistructured interviews, the interview transcripts, and the interpretations from the member checking interviews in a similarly confidential manner as the meeting observation notes, company documents, and company policies. I made copies of company documents and policies, as necessary and if possible. If I cannot create copies, Liu, Wang, Yuan and Li (2012) recommended I categorize notes based on a data label. I stored hard copy documents in a locked file cabinet in my home; these hard copy documents included interview transcripts, direct observation field notes, and copies or notes from organizational documents. I clearly labeled the documents into readily discernable categories and created an organized system for easy retrieval. I organized documents in a system most helpful to the data analysis process. Once I had analyzed all the data from the interviews, observation field notes, and organizational documents, I recorded the themes on Excel, encrypted the information with Viivo, and stored the encrypted documents into a Dropbox. I created a backup of the data on a USB drive, encrypted the information, and stored the drive in a locked file cabinet in his home. I kept all data, both hardcopy and electronic, for five years before deleting or destroying it. I completely removed all data stored in the Dropbox; I shredded any hard copy documents kept in the locked file cabinet.

Data Analysis

The data analysis technique selected for this study is thematic analysis. Cruzes, Dyba, Runeson, and Host (2014) claimed that thematic analysis entails identifying, analyzing, and reporting patterns or themes found in the collected data. The labels I created in the data organization process could improve the ease of data analysis.

Furthermore, the interpretations I created in the member checking interviews could further feed into the development of particular codes.

Triangulation was key to the success of this study. In this study, I focused on methodological triangulation over data triangulation. Data triangulation implies that time, location, and an individual can all influence data results; I should achieve variety in these three factors to ascertain how they are influencing the results (Hussein, 2015). I did not collect research over an extended period of time and did not interview IT security managers from different spaces. I used methodological triangulation in the data analysis process. Methodological triangulation uses at least two collection methods to explore and analyze a similar phenomenon (Hussein, 2015; Bekhet & Zauszniewski, 2012). To clarify, I used within-method triangulation through semistructured interviews with open-ended questions, field notes from direct observation of a training meeting, and analysis of organizational documents and procedures related to managing and strategizing cloud security.

For my data analysis process, I took the concepts and ideas from raw data to find key concepts. Vaismoradi, Turunen, and Bondas (2013) stated the process of thematic analysis, as related to qualitative descriptive study, breaks down into six steps: establishing familiarity with the data, generating initial codes, searching for themes in the data, reviewing those themes, defining and naming the themes, and finally, producing the report. In the initial step of thematic analysis, I read each interview and member checking transcript to establish familiarity with the data. Afterwards, I performed initial coding by dissecting the transcripts into distinctive words, phrases, or paragraphs. Weidmann

(2015) recommended I carry out axial coding by linking data, classifying it, establishing the major categories and subcategories, and finding associations between the categories. I analyzed organizational and company documents in a similar procedure, dissecting the information into categories and subcategories; this process repeated all six steps of thematic analysis with the observational notes I took during the quarterly training meeting. I organized and analyzed all distinctive words, phrases, or paragraphs from the data to confirm methodological triangulation during data analysis. Ryan (2013) pointed out that observation and document analysis, done in concordance with in-depth interviews, could improve the overall quality of the interviews.

The final step was when I organized overarching themes in Excel to establish the major themes for identification. These themes formed the results of the study. I should report the data linked with every theme (Vaismoradi et al., 2013; Weidmann, 2015).

Reliability and Validity

Rather than focusing on the truth behind the research, researchers use reliability and validity to unpack a study's quality. Reliability and validity in qualitative research can be broken down into four criteria: credibility, transferability, dependability, and confirmability (Trochim, 2006). Validity assesses the tools, processes, and data to determine if the conclusions are appropriate to the study; reliability relates to how replicable the study's process and conclusions are (Leung, 2015). Sinkovics and Alfoldi (2012) claimed trustworthiness is a necessary aspect of qualitative research, and one of the methods to achieve trustworthiness is through the development of a chain of

evidence. The methods I took to establish that chain of evidence and trustworthiness follow.

Reliability

Reliability relates to dependability. To obtain dependability of research data, I must audit my entire research process. If a change occurs in the research setting, I am responsible for acknowledging that change and deciding how it might affect the research (Trochim, 2006). Barnes (2015) argued a process should demonstrate the findings' reliability.

In this same vein, I paid attention to the study's confirmability. Confirmability calls researcher bias into question and asks if I am being objective by confirming or corroborating the results (Trochim, 2006). First, I admitted my biases and assumptions in the research process. Next, I performed member checks during the research process to receive participant feedback. Participants either confirmed or denied my conclusions, increasing the trustworthiness of the results. Using multiple interview participants minimized the possibility of researcher bias shaping the findings; verifying the interviews with organizational documents and observation notes provided another source in the confirmability process; I also used these sources for methodological triangulation. Finally, I provided an audit trail to represent how the data formed into its conclusion; Zitomer and Goodwin (2014) suggested an audit trail was integral to confirmability because it provides a clear and concise map of my deciding process.

An audit trail allows other researchers to evaluate the methods, decisions, documentation of data, and study findings and apply them to their investigations to attain

reliable results (Gutmann, 2014). Gutmann (2014) went on to say the audit trail has to cover important issues in the research process, such as describing the planning and execution of the study design and information about the process of data collection. I followed a detailed interview protocol in Appendix B. I also detailed my member checking process in the same protocol.

Validity

Validity does not question the authenticity of the participants' responses; rather it asks if my conclusions prove feasible in the eyes of the participants (Lub, 2015).

Credibility focuses on the feasibility of the results from the participants' perspectives. I can establish credibility through methods including prolonged engagement, debriefing sessions, member checking, iterative data collection, and triangulation of data sources (Wren & Barbara, 2013; Yin, 2013).

The primary method of data collection was the semistructured interviews. In this study, allocating one to two hours for interview conduction opened me to adequately collecting enough information about security strategy issues in the cloud environment. Also note that some initial interviews took longer than two hours to obtain additional information.

I also used member checking to establish my credibility. Harper and Cole (2012) claimed that I should use member checking as a quality control process when I look to improve the precision, integrity, and legitimacy of what I documented during an interview. Member checking provides a clear interpretation by confirming accurate reporting of the meanings intended by the participants for authentication (Houghton,

Casey, Shaw, & Murphy, 2013). In my investigation, after I completed the process of transcribing the interviews, I analyzed my data using the thematic analysis process. A researcher using thematic analysis must identify, analyze, and then report the themes he or she found in the data. I established familiarity with the interview notes and transcripts in order to more easily find distinctive words and phrases in the data. These phrases represented the themes I compiled and brought to the follow-up member checking interview with the participants. Cheng (2014) claimed a positive outcome of member checking is that it not only enhances the data's credibility but also establishes me as attentive, respectful, and serious, which can inevitably aid in building a trusting relationship between the interviewer and interviewee. Member checking guaranteed another conversation; this additional conversation aided in confirming data saturation.

I also established similar familiarity with the field notes and organizational policies to further the study's credibility through methodological triangulation. In both these forms of data, I highlighted and recorded distinctive words and phrases, and then I compared the distinctive words and phrases from all data sources, including the interview notes and transcripts from the initial and member checking interviews, to discover themes. Finally, I compiled these themes in a final step for report.

Confirming transferability asks me to consider if I have provided enough information for other researchers to transfer findings (Barnes, 2015). Houghton et al. (2013) suggested I could increase transferability by thoroughly presenting my research findings and using *thick description* of the background, data collection methods, and data

sources. Marshall and Rossman (2016) pointed out that the transferability of the research is ultimately determined by another researcher looking to transfer the findings.

Transition and Summary

This section presented the methodology I used in this investigation. Overall, I have chosen the qualitative case study methodology; I considered it the most suitable research methodology for achieving the study's purpose. This methodology supported the collection of data from IT security managers using semistructured interviews and historical records. Thus, using this methodology allowed me to discover the strategies IT managers use during internal data and external breaches in cloud computing. The next section of the paper provides the results of this investigation in a more detailed form.

Section 3: Application to Professional Practice and Implications for Change

This study's focus was exploring the strategies that IT security managers use to host delicate data in the commercial cloud. In this section, I focus on the use of these findings in professional fields to bring about change. It includes a synopsis of the study, the presenting results, an application of specialized practice, the potential effect for social change, a recommendation for action, proposals where further study is needed, and the reflection and study conclusion.

Overview of Study

I set out to demonstrate the importance of security management in cloud computing. Through this study, I hoped to affirm just how necessary it is to safeguard cloud information from all fronts to ensure attackers do not compromise organizational data. According to the participants, hackers exploit the cloud's security through Wi-Fi hotspots and password cracks. Nonetheless, service providers are not legally obligated to provide adequate encryption services, subjecting corporations to risk (King & Raja, 2012). As referenced in the conceptual framework model, unauthorized access to the management interface, account and service hijacking, vulnerabilities in application programming interfaces, and vulnerabilities in virtualization complicate the security narrative in cloud computing. Through the use of formal, technical, and informal strategies, however, an organization might manage data breaches and head off future attacks and security holes.

Insider attacks pose significant risk to an organization. In most organizations, insiders who exfiltrate information can enhance access to external cloud hackers (Chang

et al., 2016). Insider access to these platforms could lead to security holes that external hackers can exploit. Whether the attack is internal or external, most organizations spend hefty amounts on security management (Reinmoeller & Ansari, 2015). Organizations should enact concrete policies to safeguard their sensitive data. A missing policy framework could influence cloud providers to institute insufficient measures to safeguard information. These observations are further detailed in the findings.

Presentation of the Findings

At the onset of the study, I sought to answer the following research question: What security strategies do IT security managers use to host sensitive information in the commercial cloud? This section encompasses a dialogue of the five main themes and one subtheme I identified through the study. I used methodological triangulation to analyze the data from semistructured interviews with follow-up member checking interviews, field notes from direct observation of a training meeting, and organizational documents and procedures related to managing and strategizing cloud security. Five major themes emerged during my analysis: avoiding social engineering vulnerabilities, avoiding weak encryption, maintaining customer trust, training to create a cloud security culture, and developing sufficient organizational policies. In addition, there was one subtheme that derived off weak encryption, vulnerabilities caused by weak passwords. These themes illustrate potential strategies related to securing sensitive information in the commercial cloud.

Theme 1: Avoiding Social Engineering Vulnerabilities

The first theme to emerge from data collection was avoiding social engineering vulnerabilities. These types of attacks are powerful because they rely on human trust and intimacy; they are not easily mitigated through technical strategies. According to the study findings, the participants experienced challenges in securing the cloud against social engineering attacks. Participant A reported that attackers use simple tactics like acquiring and using birthdays to obtain access to information beyond their jurisdiction. Participant G shared that social engineering attacks are common among enterprises and SMBs and that these attacks are increasingly sophisticated. Participant F reported that hackers use free Wi-Fi hot-spots and falsified login pages to share and receive information and free cloud storage. I found similar acknowledgments of phishing risk in the organizational documents. For example, according to DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems, IT security managers should protect unclassified DoD information with, at minimum, one electronic or physical barrier, including but not limited to logical authentication or logon procedure. This policy offered a way to mitigate potential social engineering attacks through logical authentication but failed to consider ways to mitigate motivation. In my direct observation of a training session, I failed to find any insights in terms of social engineering, which could reveal an absence in the consideration of the theme in cloud security strategies. Scholarly literature coincided with the methodological triangulation to illuminate the extent of social engineering vulnerabilities.

In the intersections of the literature and the data, I uncovered strategies to minimize or avoid social engineering vulnerabilities. One of the most common social engineering vulnerabilities is caused by phishing. Jansen and Leukfeldt (2016) focused on online banking victimization and concluded that measures against phishing scams could reduce customer risk; however, phishing eases an attacker's means of accessibility to critical information. In fact, six respondents from Jansen and Leukfeldt's interviews were initially unable to recognize a phishing attack because the attack required no direct interaction with the victim. This observation coincided with Krombholz et al. (2015), who found that minimal direct contact with numerous tools to obtain personal information made social engineering attacks effective against companies like the RSA and the New York Times. The findings of both these studies align with the participants' reports; Participants A, B, and E all reported phishing in their interviews, pointing out its manipulation of unsuspecting employees or home users. In my review of organizational documents, DoD Instruction 8550.01 recommended disabling HTML web links from government e-mails to stop phishing attacks. The direct observation provided no data relevant to this theme. The literature and data from methodological triangulation provided some solutions to social engineering attacks.

Security cultures could be effective at minimizing social engineering vulnerabilities. Bullée et al. (2015) suggested that the development of a security culture could be a countermeasure against social engineering vulnerabilities. Current countermeasures against social engineering typically include outside parties performing technical tests (vulnerability assessments) or user-oriented tests (phishing tests).

However, these strategies do not consider persuasion techniques. Bullée et al. concluded that intervention reduced the effect of subject compliance, with 62% of the control group complying versus 37% of the intervention group. In short, creating a security culture helps to minimize social engineering vulnerabilities. In the organizational documents, the DoD offered no policy for combatting social engineering attacks, but a DoD memorandum, Questions Regarding Social Media and the Hatch Act (2015), did recommend training employees on social media use to create awareness against social engineering attacks. Participant A aimed at the center of the DoD memorandum, recommending against password and personal information sharing, especially on social media. Participant E and G warned against sharing personal information with anyone. The literature provided some gravity to the theme but revealed a hole in the RAT.

Although social engineering aligned with the tenets of the RAT, the RAT did not include attacker motivation. Social engineering attacks aligned with the RAT because these attacks manipulated known vulnerabilities in the cloud to monitor the hosting software (Claycomb & Nicholl, 2012). Social engineering eases accessibility, manipulating privileged access to the cloud infrastructure to put accounts at risk (Krombholz et al, 2016). Participants A, B, and E all claimed that attackers are motivated to access sensitive data. However, routine activity theorists did not define motivation and, without a way to mitigate attacker motivation, security strategies will continue to lack a holistic approach. From the organizational documents, the United States Army Social Media Handbook, Executive Order 12333, and DoDI 8530.01 all suggested that offenders were willing to participate in social engineering attacks to target valuable information,

such as network defenses and sensitive data. This hole in security strategy methods can be compensated by relating social engineering to other theories.

The RAT, theory of planned behavior, and neutralization theory all aligned with the theme of social engineering and attacker motivation. According to the theory of planned behavior, intention precedes behavior and is influenced by attitude, subjective norms, and perceived behavioral control (Ifinedo, 2012). Bulgurcu et al. (2010) reviewed the theory of planned behavior to formulate their model for antecedents of ISP compliance. Bulgurcu et al. claimed that employees' attitudes toward compliance depended on an assessment of benefit of compliance, cost of compliance, and cost of noncompliance. This three-part assessment allowed for neutralization theory, which includes five neutralization techniques: denial of responsibility, injury, and victim; condemnation of condemners, and appeal to higher loyalties (Rocha Flores & Ekstedt, 2016). A multipart assessment of the benefits and costs of compliance/noncompliance eased the execution of neutralization techniques. For instance, Participants A, E, F, and G all suggested benefits of noncompliance are a significant motivating factor because social engineering attackers are influenced by greed. Participant B suggested denial of responsibility and an appeal to higher loyalties was responsible for social engineering attacks, pointing out the presence of state-sponsored actors, those individuals who are authorized by their states of allegiance to commit these attacks. The RAT included the suitability of the target and the benefits of noncompliance (Bulgurcu et al., 2010; Kajtazi, Bulgurcu, Cavusoglu, & Benbasat, 2014). Both the theory of planned behavior and neutralization theory relate to the RAT because they disprove Cohen and Felson's (1979)

suggestion that motivation is constant. IT professionals should consider the motivations behind social engineering attacks because these attacks are demanding issues for sensitive items in the commercial cloud.

IT security professional should consider social engineering in their cloud security strategies because it compensates for the shortcomings of the RAT. IT professionals might head off social engineering attacks by focusing on criminal motivation. In further engagement with organizational policies, I discovered in DoDI 8582.01 that adequate encryption could safeguard unclassified DoD information. Although this policy still failed to mitigate motivating factors, encryption could be a significant strategy in cloud security.

Theme 2: Avoiding Weak Encryption

Another theme to emerge was the necessity for adequate encryption. Encryption can be used to secure data moving in and out of the cloud (Hashizume et al., 2013). Hashizume et al. (2013) performed a systematic review of literature related to the SPI (SaaS, PaaS, and IaaS) model and its vulnerabilities and concluded that encryption could secure data during transfer, if the encryption methods were strong.

The participant responses echoed Hashizume et al.'s (2013) conclusion. Participant B reported common security vulnerabilities in the hardware and software devices, pointing out that a common habit among hackers is to look for a weak encryption algorithm to break. Participant B stated that collaboration among hackers in sharing industry standard devices, as well as utilities, allows them to gain unauthorized access. Attackers have numerous ways to manipulate vulnerabilities in areas with weak

encryption. For example, Participant E recommended against employees storing credit card data in a browser because information breaches, exploited vulnerabilities, account hacking, and denial of service authentication make this unwise. Participant G pointed out that hackers can steal a user's cookies or CSRF to convince users to send genuine requests to arbitrary sites. Because hackers have full command of knowledge on cloud vulnerabilities, establishing an adequate level of encryption to protect the data is important. Organizational policies from the NIST could help to establish adequate encryption levels.

Among the organizational policies I analyzed, NIST SP 800-175A: Guideline for Using Crypto Standards: Directives, Mandates and Policies determined that encryption measures necessary to protect data both in transmission and cloud storage should depend on the results of a risk analysis. Participants A, B, C, and G all suggested encryption, including encryption at the provider level, was one of the best ways to protect cloud data. I failed to provide any further insight into the NIST documents in my training observation. The literature does provide some clarity on this matter.

The data aligned with current literature, and I found a connection to the theory of cryptography. Participant C acknowledged weak encryption as a security vulnerability in the cloud, citing the inadequacies of many service providers to encrypt at-risk data. Participant C's response fell in line with the findings of Rodrigues et al. (2013), who concluded that data encryption is one of several key issues customers and cloud service providers should consider. Without service provider guarantees, the burden of confidentiality, security, and privacy falls on IT security managers. Hossein et al. (2013)

expanded research of the theory of cryptography to speak to cloud service provider commitment to encryption. Hossein et al. determined that encryption at the service provider level still posed a risk and that client-side encryption could counteract the benefits of cloud services. From the organizational policies, documents DoDD 5240.06, CNSSI 1253F (Attachment 5 and 6), and DoD Cloud Computing Strategy used NIST SP800 to outline requirements for encryption and passwords that could counteract the risk mention by Hossein et al.

Rodrigues et al. (2013) and Hossein et al.'s (2013) conclusions coincided with formal controls because cloud service providers' legal regulations depend on location. For example, current compliance management and data regulation requirements were lax on the cloud service provider's end. Therefore, organizations should develop formal control strategies in concordance with their own policies. Department of Defense Cloud Computing Security Requirements, Guide Version 1 (2017), used six sections to define policy for the DoD's internal networks, external networks, and its stakeholders to ensure effective implementation of its mission and data protection. The various ways unencrypted information is exploited necessitates a close engagement with the theory of cryptography which, in relation to cloud services, considers cryptographic techniques a way to improve the privacy and security of the cloud architecture. However, these strategies do little to mitigate this theme's subtheme.

Subtheme: Vulnerabilities caused by weak passwords. Weak passwords are a subtheme to weak encryption. Weak passwords are easily guessed and can depend on information obtained through social engineering techniques. Fifty three percent of weak

passwords are easily cracked versus 27% of strong passwords (Houshmand & Aggarwhal, 2012). I found that that weak passwords posed a threat to cloud security.

Participants revealed that weak passwords could have drastic consequences. According to Participant B, weak passwords across cloud peripheral devices can contribute to cloud hackers achieving access via password crack devices. Participant F suggested weak passwords, in concordance with potential social engineering practices, could allow hackers to masquerade as IT personnel. Participant E considered the potential damages of a hacker with a default admin password *catastrophic* because of the administration levels opened to the hacker. Weak passwords could cost organizations exponentially.

In the participant responses, I found that organization leaders overlooked the need to monitor their weak security standards because it cuts the profit margin. I also discovered that organization leaders can find effective solutions to deal with internal and external threats both involving and costly. As participants noted, however, previous data breaches increase top management engagement in the adoption of security-based enterprises. In short, organization leaders should be diligent in password development from the forefront when subscribing to cloud services. This conclusion calls back to Rodrigues et al. (2013) and their findings on weak encryption, in which cloud service providers offered inadequate coverage for data encryption without legal or company regulation. Organizational leaders must ensure that their measures are comprehensive to safeguard sensitive information.

In other data from the methodological triangulation, I found that organizational leaders have little to guide them in terms of comprehensive measures. According to Participant C, organization leaders can achieve diligent measures by integrating stringent security measures that support a centralized architecture, cut down the number of privileged users, and create awareness through training. My direct observation of a training procedure failed to support Participant C's conclusions, however. In fact, my observation provided little in terms of weak password risks. Meanwhile, industry standards could prove useful in this endeavor. DoDI 8582.01, Security of Unclassified DoD information on Non-DoD Information Systems, suggested encrypted documents use at least application-provided password protected level, which falls in line with much of the literature about adequate password protection.

Current strategies toward adequate password protection focus on increasing password strength and password independence, but other methods exist. NIST documents offered some ways to increase password strength, including nonalphanumeric characters and a variety of upper and lowercase letters. Participants A, B, C, and F supported the NIST documents because it is a de facto standard the entire government upholds. According to Bonneau et al. (2015), these policies impose a high usability cost. Users also tend to reuse passwords, which means leaks in one web outlet could cause leaks in another. Bonneau et al. concluded that researchers should revisit the password's role in authentication. Bonneau et al. also concluded that the evolution of password countermeasures is in its early stages, with little to no research into the long-term results of current countermeasures.

Some researchers have tried to offer their own additions to weak password solutions. Alhadidi et al. (2016) proposed software to compensate for determining adequate password protection. Alhadidi et al. explored authentication in cloud computing over mobile devices to propose a solution that uses the One Time Password concept to increase security and use the mobile device as an authentication device. Alhadidi et al. claimed that static passwords are one of the most common methods of user authentication. Alhadidi's solution did not coincide with the suggestions from the organizational policies. The organizational policies demonstrate the success of formal strategies in the conceptual framework.

According to my analysis of organizational documents, IT managers should follow industry standards because they adhere to the RAT's tenets of formal strategies. I analyzed NIST document, Special Publication 800-39, Managing Information Security Risk Organization, Mission, and Information System View, and discovered that the document provided education on measures to combat weak encryption, legislation, policies, and programmatic initiatives. Many of the previously discussed organizational policies built off this document. The industry standard documents provided a foundation for numerous organizations, aiming to secure complete assurance. Most DoD documents did not provide a measurement of the consequences of data breach and failed to mention the repercussions of these circumstances.

Theme 3: Maintaining Customer Trust

The third theme, customer trust, focuses on the direct relationship between the organization and its customers. Information and data breaches can damage customers'

trust of the organization. Failure to establish customer trust with adequate security could inhibit customers from further interaction with the business.

Organization leaders avoid costly practices to secure information, but the participants noted that these avoidance's could have costlier outcomes. An organization's perception and brand can encounter significant damage because of breaches. Participant A had observed and shared how data breaches could cause customers to hold inadequate faith in the organization's ability to adequately secure their sensitive data. According to Participant A, organizations who lose customer faith, lose opportunities for new business. Without business, an organization will inevitably fail. Participant F recalled data breaches that had occurred huge expenses for tax payers. Participant F went on to mention that organizations can incur large fines, civil lawsuits, and criminal charges; organizational leaders might also need to purchase credit monitoring services to alert their customers about their stolen information. Both the organizational documents and training session failed to consider the role of maintaining customer trust in cloud security. The scholarly literature, however, did provide some insight.

Maintaining customer trust was an important theme in the scholarly literature about cloud security Sunyaev and Schneider (2013) surveyed 53 consumers with experience or intent to use consumer cloud services and discovered that consumers prioritized security, privacy, and availability assurances over others. Sunyaev and Schneider (2013) conclusions fell in line with social theories of interpersonal relationships. Organizations who invest in providing the assurances their customers need develop greater customer satisfaction. Failure to invest in security, privacy, or availability

assurances could be costly. In fact, the overwhelming expense of security failure suggested adequate cloud security for customers should be a priority.

Experts disagreed on which strategies are necessary to maintain cloud data security. Participant E found IT security managers too content in complex approaches to secure networks. This finding was initially in line with Waleed, Chunlin, & Naji (2014), who found simulation and modeling crucial against possible threats. However, their analysis of their own simulation experiment suggested they had taken only initial steps in mitigating security issues like data handling, management, governance, and data protection. My findings suggested IT security managers should avoid one-size-fits-all security strategies to prevent and detect insider threats. Although Participant E insisted hackers think in simplistic ways, Participant D described an overly simplistic strategy attempt in which systems were patched to provide adequate protection but not rebooted. According to this participant, the system owners were willing to accept the risk because it allowed them to maintain customer trust and support. Strategies to build customer trust are not well-considered however, so further in-depth research could clarify the views of IT security managers on this theme's importance. Certain theories could also provide further insight.

Maintaining customer trust requires a degree of visibility. As the theory of interpersonal relationships suggests, business leaders need to demonstrate an investment in customer needs to establish and maintain customer trust. Ionita et al. (2016) recognized that visibility in the whole security context was necessary to establish customer confidence, and proposed an infrastructure that could allow for the exchange of threat

information with foreign organizations. The theme of customer trust adhered less to the development of the conceptual framework than it revealed about the consequences of not adhering to it. As the data and literature revealed, a break in customer trust has costly consequences, further necessitating a strategy to ensure that a break in customer trust never occurs. Because data breaches and security measures can be costly, organizations can benefit from the right combination of cloud strategies. Informal strategies were particularly important to this combination.

Theme 4: Training to Create a Cloud Security Culture

In this study, I defined *training* in direct concordance with informal strategies from the conceptual framework. Informal strategies focus on creating a culture of knowledge in an organization.

My observation of a public quarterly information security meeting could corroborate the importance of a security culture. At the public meeting, Trainer One presented *FREQ.PY*, a program that computes the probability of the incidence of character pairing with respect to frequency assessment in DNS server logs as well as client DNS logs/cache. According to Trainer One's instruction, a number of attackers love DNS because many systems require name resolution, allow outbound traffic, have high volumes of benign traffic, and are proxied by design. Again, Trainer One noted that adversaries are aware that security is hooked on Blacklist; therefore, attackers use rapid return and programmatic generations of fake websites to infect users. Organizations can invest in log monitoring to minimize attacks on the DNS. Logs provide high-degree visibility. Organizations should associate with their log source to reconstruct a reliable

event timeline and a suitable preliminary guideline for security analysts and event respondents. This reconstruction lends itself to the establishment of protocol.

I observed a need to establish a baseline. For example, whether it is standard for internet protocol one to talk to internet protocol two in reference to connections volume from enterprise to the destination. In short, an evident need exists to train network and systems administrators on DNS logs. These administrators often overlook DNS logs. As a result of training, these administrators can train other users on how to tell if a website is fake or authentic. Through this action, administrators further the cloud security culture. In the development of a security culture, organizations should consider particular theories.

A cloud security culture could also align with the theory of planned behavior. Arpacı et al. (2014) surveyed via questionnaire 200 pre-service teachers and concluded that perceived values of security and privacy had significant influence of students' attitudes towards and intent to use cloud services. In short, perceptions of security had direct influence on consumer intent. If intent is measured through the costs and benefits of compliance or noncompliance to cloud security standards, increased security culture could contribute to decreased intent to noncompliance with cloud security standards. All seven participants cited training and education as key to mitigating noncompliance with cloud security standards. The organizational policies also provided some insight.

Organizational policies are relevant to the development of a security culture because they help to establish a training protocol. Hendre and Joshi (2015) analyzed security threats from data breaches, malicious insiders, and other public documents to determine, among other security controls, cloud training and awareness programs are

necessary and should adhere to NIST 800-61[30] and ISO 17799 [24] compliance standards. The cloud security culture cannot function with protocol. To ensure employees adhere to their level of access, organizations should clearly communicate their rules and guidelines. Passing information forward is another way education embodies the informal strategies of the routine activity theory. I analyzed organizational documents that provide standards for relaying training information. These standards often form organizational policies. In fact, organizational documents and policies offered examples for establishing a security culture. For instance, NIST SP 800-137 provided a standard compliance policy to assure ISCM programs provide awareness of threats and vulnerabilities. The United States Army Social Media Handbook from the Office of the Chief of Public Affairs (2016) suggested that training occurs in two ways, formal training at the Defense Informational School and informal training sought out on one's own. According to the document, an efficient security culture requires multiple methods of training. The solutions to create an efficient cloud security culture relate to the conceptual framework.

The participants offered a variety of solutions to training models, inadvertently speaking to the conceptual framework's complexity around cloud security strategies. All participants except Participant E asserted some need to train to prevent cloud security breaches. Participant C suggested a series of strategies that included stringent security controls, centrally-managed architecture, reduced privileged users, and enhanced information assurance awareness. These strategies invoke a combination of strategies from the conceptual framework model, suggesting that a combination of formal, informal, and technical strategies best meets cloud security demands. Meanwhile,

Participant D focused on informal strategies, expressing an explicit need to train ISSMs, ISSOs (Information System Security Officers), and ISSEs (Information System Security Engineers). The focus on training integral members of cloud security asserts a need for training protocol, so that all employees receive vital information necessary to create the cloud security culture.

Theme 5: Developing Sufficient Policies

Policies should outline efforts to protect sensitive cloud information; inadequate policies make it difficult for cloud service providers to implement privacy and security protections.

NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, was a policy example I found during organizational document analysis. NIST SP 800-137 guided organizations on how to establish ISCM strategies, implementing an ISCM program that provides awareness of threats and vulnerabilities. The policy relied on all three forms of security strategies from the framework model. For example, NIST SP 800-137 assessed and offered the effectiveness of deployed security controls, adhering to the technical strategies portion of the framework, while also meeting the need for informal strategies by training readers how to respond to security risks in a timely manner. During the training session I observed, Trainer One gestured at the importance of developing policy as protocol baselines, specifically when determining the standard for internet protocol one to talk to internet protocol two as previously mentioned. Strong policies combine strategies to

sufficiently secure sensitive cloud data. Failing to instate and adhere to a strong policy could have disastrous results.

A lack of proper backup policies can result in cloud data compromise. As previously stated, Participant D described a system patch meant to reduce threats, but without a policy in place to reboot the system, error fixing failed. Three participants offered policy suggestions that could meet technical and formal strategies, including stronger passwords, strong cyber regulations, IAVA and security patching, and tightening firewalls to allow one-way traffic. Participant A suggested expanding a higher degree of Transport Layer Security (TSL) while removing Secure Sockets Layer (SSL), and that point to point encryption could eliminate attacks on all data levels. A clear policy becomes necessary to categorize the array of cloud security strategies, and scholarly literature provides insight into the development of clear policies.

In the literature, I found theories that are relevant to the way organizations form clear guidelines. Metheny (2017) presented a short case study of how NIST RMF can apply to FedRAMP while still adhering to the values of rational and incremental theories. Metheny concluded that the NIST RMF is a continuous document that will need regular reviews and changes, while still expecting NIST standards to establish implementation of a program that considers costs and benefits. In short, organizational policies should strive toward NIST standards. By focusing on some theories relevant to policy development, these standards become more readily achievable.

Rational theory, incremental theory, and the routine activity theory were all relevant to the development of organizational policies. According to rational theory, a

policy's benefits should far outweigh the costs. A policy should also align with incremental theory and be cohesive and comprehensive enough to be added to over time without significant revision. The DoD Social Media Policy was an example of a policy that met these theoretical needs. The Directive Type Memorandum (DTM) added to the policy sets the guidelines that those under Pentagon jurisdiction should follow in their social media use. Cole-Miller et al. (2016) performed an assessment of the DoD Social Media policy and concluded that DoD policies are adequate in promoting responsible social media use and in guarding against social media risks. They then offered four potential recommendations to further the overall effectiveness of the documents. One of Cole-Miller et al.'s recommendations were considering monitoring and risk in relation to in overall organization risk management. This aligned with Participants F and G, who asserted that an inadequate understanding of sensitive data could create inadequate policies, and that policy makers should be trained on the sensitivity of cloud data and their role to keep it safe. According to the tenets of the routine activity theory, the manner in which routine activities take place provided opportunities for hackers (Barclay, 2014). From the data, I observed that the most successful policies covered all three forms of security strategies in the framework model: formal, informal, and technical strategies. For example, policies to educate users could meet the need for informal strategies while also clarifying users' responsibilities to ensure data safety. Policies need clear guidelines to inform users what to do or not do.

Applications to Professional Practice

The IT impact of this issue is that the findings may benefit information security practice by increasing understanding. Again, researchers could benefit in major applications of the findings of this research, particularly those that require special management oversight due to significant risk of harm due to loss, unauthorized access, or misused data. Major applications include software applications, such as integrated consumable brands. Several software applications carry out single goals, like payroll, while mixtures of software and hardware carry out roles like Global Command and Control System, Defense Enrollment Eligibility Reporting System, and so forth (Chander, Jain & Shankar, 2013). The findings of this study may be beneficial in professional practice by helping IT security managers to increase their understanding of the complex elements surrounding external and internal threats and breaches.

Implications for Social Change

General organizations and IT professionals might develop a shared consciousness on the intricacy of internal and external attacks in the cloud from this study. Wider society may also benefit from the potential to strengthen their sensitive information with informal, formal and technical approaches (Mohamed & Pillutla, 2014). The social impact belies on the benefits of cloud services, and the need to secure these services to continue their benefits.

Platforms such as YouTube and Google are a testament to a paradigm shift in modern interaction. With modern technology, viewers can share a viral event worldwide almost immediately. As globalization reaches its height, citizen journalists emerge, able

to report anything, anywhere, at any time. Viewers' live-stream news instantly. Via social media sites like Twitter and Facebook, individuals find forgotten acquaintances and friends. Political icons and high profile images run through social media platforms as well, reaching a wider public and shaping opinions towards a certain end (Suo, 2013). Firm employees gather information from social media networks, coupled with cloud-centered data resources, to gain exceptional insight on prospective services, novelty, and clientele demands. But just as businesses and politicians can use social media to obtain clientele information, so can potential attackers. In fact, Wagner et al. (2012) found that Twitter users interact comfortably with strangers. User comfort increases the chance of Twitter users offering information susceptible to social engineering attacks.

Presidents of academic institutions have been fast to grasp the benefits of cloud technology. Institutional leaders who embrace cloud technology better obtain the capacity for their learners to access information ubiquitously, to join online classrooms, to increase involvement in team-related activities (Czerkawski, 2016). Learners in emerging economies benefit from cloud computing by curtailing expenses and coalescing business-robotics processes to restructure subscription, class registrations, and task tracking.

Institutional leaders balance their storage clouds to keep about 2.5 quintillion bytes of information under lock and key, without the need for another structure (Barclay, 2014). However, the benefits of academic cloud sharing do not come without risks. Further understanding of cloud security strategies could benefit the continued growth of education in first-world and emerging economies.

These benefits do not extend to education alone; various sectors in banking, agriculture, health, and science have also reaped enormous benefits from cloud computing. User adoption of smartphones in developing nations enhanced economic progress far better than what historians witnessed during the traditional wired telephone system. Still, organizational leaders who benefit from cloud computing share the same risk as any cloud user when it comes to protecting their precious data.

For example, it seems that small business owners are better able to compete globally with cloud computing. To propitiate new markets being generated by the cloud, startup owners will utilize cloud computing to gain an edge in a highly competitive market. A single community cloud underpins workers with intricate travel itineraries, synchronizing variations in hotel bookings and reservations (Adjei, 2015). Regardless of the shoestring budget on which small business owners operate, they would be able to globalize cost effectively by wielding the power of cloud computing (Ray, 2016). With cloud computing, firm owners will likely move away from the old mantra of creating a physical data hub. Instead, through established service purveyors, firm owners may be able to access infrastructure as a service in little time, an aspect that presents a latitude advantage over slower rivals.

In terms of healthcare, cloud technology could influence how physicians practice. Cloud computing enables hospital workers to more easily manage non-stored patient information. They may also share patient information among other healthcare professionals; patients are more easily able to follow through with their treatment processes. In the long run, operational expenses are usually negligible. Cloud computing

allows healthcare professionals to implement quick solutions in a safe environment while still adhering to the Health Indemnity Portability and Accountability Act Standards (Trulove, 2015). Apart from the many challenges that come with integrating antique technology with modern applications, and the analogous level of services, the advantages the cloud presents outweigh the laxity to embrace the status quo. Still, healthcare providers could face serious legal repercussions if they fail to adequately encrypt their information and protect the confidentiality of their patients' information on the cloud.

The way various organizations can benefit from the cloud fosters a significant influence on social change. Technological advances influence modes of life. For example, institutional success occurs because technological development removes technological constraints around an organization (Freeman, 2016). Therefore, the technological benefits from cloud computing can better enable federal agencies, state agencies, and private organizations to improve sectors like banking, agriculture, and science. These sectors are important to the success, growth, and comfort of society at large. These same technological benefits lend themselves to the creation of social movements (Ward & Pede, 2015). The development of social movements within an organization, for example, creates more chances for the organization to adopt strong leadership; it encourages employees to commit to the recommended strategies, duties, and responsibilities developed to uphold the organizational standards. Therefore, the technological benefits seen in the various industries above can be said to be essential in

the facilitation of societal improvement. The obvious benefits of cloud technology in social spheres necessitates cloud security.

An enhanced cloud security method is integral because of its social impact. Those who embrace cloud security enable themselves to engage in a social conversation with involved organizations or groups; they also enable chances for security intelligence (Linsay, 2015). An organization that creates security intelligence can improve their performance in all organizational sectors. They can also develop a security culture that protects the various groups in the social conversation. For example, in the corporate world, members of an organization that focuses on using security strategies to maintain their sensitive cloud data can remember the information their management team presents them (Rüegg, Gries, Bond-Lamberty, Bowen, Felzer, McIntyre, & Weathers, 2014). This observation occurs because a properly secured cloud structure allows relevant or authorized members to access information whenever they want. Security is an integral portion of the social culture, especially in business. An organization that focuses on cloud security might expect more profitable outcomes.

Cloud computing could alter the way firm owners sell products and services to clients. With the advents of cloud computing, customers engage in more cloud-based transactions. They construct their opinions of an organization's products and services through online communities (Suo, 2013). The cloud could provide small niche retailers the capability to modify their offers and closely survey their clients' demands. Organization leaders could make propositions anchored not just on a given activity on one platform, but across various platforms, e.g. what is watched on Web TV,

YouTube, and other interfaces (Weber & Carblanc, 2014). Small niche retailers will need to protect their brand through proper security protocol.

By and large, cloud computing can enable people to make informed decisions via mobile gadget use. Many people now have easy access to the processing power the cloud requires; they are able to evaluate virtually any type of data, regardless of the distance or remoteness (Suo, 2013). Users can pool together real-time market information, weather forecasts, new storylines, tweets, and blog opinions on their mobile phones. Individuals and businesses gain a glimpse into strategic data through real-time market information to pave the way for prudent decision-making processes. Moreover, individuals and businesses with improved processing power allow for swift, original research on a broad range of themes and coalescing sales forecasts. The increased accessibility of shared information feeds into one of the four properties of the routine activity theory, thereby increasing the risk of external attack. In fact, thieves steal over 10, 000 laptops from US airports on a weekly basis (Lee et al., 2015); laptop theft subjected multiple firms to humiliation and financial risk, especially when the thieves leak critical information. Traditionally, individuals who carry laptops leave all pertinent information at risk. While encryption is the surest way to secure information, certain jurisdiction disallows the importation of encrypted laptops. In general society, to continue the benefits of cloud services on various sectors, security is a priority.

Recommendations for Action

Due to the largely unregulated nature of cloud policy, organization leaders should exercise caution when subscribing to cloud services. To reiterate many of the

participants' suggestions, organizations should integrate stringent security measures, use centralized infrastructures, train employees on security protocol, and minimize the number of privileged users to ensure data assurance. Organization leaders should stipulate policies and consistently categorize data and controls to ensure users appropriately handle their data categories (Weber & Carblanc, 2014). Organization leaders should create awareness about the sensitivity of the information and the need for users to ensure its security. The awareness programs for cloud computing should involve ISSMs, ISSOs, and ISSEs. To effectively protect sensitive data in the cloud, organizations should educate users on the need to protect sensitive data, use strong passwords, adopt cyber laws and certificate-based access, integrate with ACLs layered with encryption, and hire third-party firms to provide centralized security. These changes toward action could give firm leaders a greater sense toward cloud security.

Recommendations for Further Study

Insider threats could obliterate useful data, meddle with critical data, reduplicate information, and mine illegally. Insider attacks possess a number of motivations. Therefore, the element of insider threats in cloud computing should be investigated further to help determine IT managers' perceptions concerning this issue. The limitations of this study lie primarily in the study sample. The results depend largely on participant experience. To increase the chance that IT research reaches various participant experiences, I recommend that researchers interview participants outside the government or in private industry. Also, researchers in the routine activity theory do not consider social engineering in the theory's foundation. They do not consider hacker motivation or

social status. Research into human behavior could further illuminate comprehensive strategies in cloud security. Researchers might also consider customer trust in those human behavior endeavors: how to maintain customer trust and the extent of the impact of losing customer trust. A quantitative study of organizational loss factors could also further the information I have accumulated here.

Reflections

The research process was an involving endeavor, as such; I took necessary precautions to reduce personal bias. I am the main tool for not only gathering but also reviewing the information. As such, I acknowledged and considered individual bias throughout the study process. I endeavored to learn from the participants and the study. I sought to ensure the credibility of this study. I opened myself to the new ideas that arose in this study. For example, I discovered that because many attackers focus on DNS, a number of systems require outbound traffic and high volumes of benign traffic. I learned that logs present high-degree visibility and that a relationship among sources of logs is essential in reconstructing reliable incidence timelines and appropriate preliminary guidelines for incident responders and security analysts.

Summary and Study Conclusions

In endeavoring to establish the problematic security management in cloud computing, I hoped to affirm how imperative it is to ensure organizations securely maintain data to prevent encroachment. IT security managers should secure Wi-Fi hotspots to allow authentic entry alone. If service providers offered strong encryption services, they could thwart password penetration and curtail organizational risk. Firm

leaders can manage security breaches with formal, technical, and informal approaches; they should develop a strong policy framework that ensures vendors attach a high premium on securing data.

The advents of cloud computing represent a paradigm shift in the way things are done, from healthcare delivery to education and e-commerce. Despite the cost benefits, cloud computing faces major security concerns that could threaten the sustainability of various businesses. Although people using the internet are clearly at risk of identity theft, those that use apps to make online purchases are similarly vulnerable (Adjei, 2015). IT security officers have underscored the fact that criminals have altered conventional places of executing crimes. Most criminal activities have now shifted from streets onto decentralized networks like the internet. These criminal activities are better explained through three models, namely the lifestyle exposure theory, human ecology theory, and the routine activity theory. In responding to the study objectives, I adopted security approaches that were imperative in bolstering the organization's cloud security. Adding of layers to the security strategy concrete model was one of the approaches that would make the model somewhat complex. Complexity should make it more difficult for external intruders to advance hacking activities. Augmenting a security layer is also critical when it comes to monitoring the operation of the whole system.

Hackers exploit routine activity concepts such as visibility, inertia, value, and accessibility. They manipulate these concepts to wage viral attacks, hurting sensitive customer information. Phishing is, for instance, one of the dominant cloud security issues. However, most attacks depend on insider privileged access. As such,

organizations should impose and communicate security guidelines to their employees, outlining how employees might thwart internal and external attacks (Weber & Carblanc, 2014). Moreover, policies should guide how to access organization resources. Organization leaders should also clearly outline the consequences of policy violation. Effective risk management is, therefore, an integral aspect when it comes to the governance and execution of corporate processes. In the end, while adherence to legal issues associated with data in cloud framework is a substantive challenge, service providers in cloud computing should evaluate acquiescence demands that arise in the deployment of their services (Clarke, 2013).

References

- Ab Rahman, N. H., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security, 49*, 45–69.
doi:10.1016/j.cose.2014.11.006
- Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 17*(1), 54-67. doi:10.1108/info-09-2014-0042
- Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*, 357–370. doi:10.1007/s10845-012-0683-0
- Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications (IJNSA), 6*, 25–36.
doi:10.5121/ijnsa.2014.6103
- Ahuja, S. P., & Komathukattil, D. (2012). A survey of the state of cloud security. *Network and Communication Technologies, 1*, 66–75. doi:10.5539/nct.v1n2p66
- Akeel, F. Y., Wills, G. B., & Gravell, A. M. (2014). Exposing data leakage in data integration systems. *Internet Technology and Secured Transactions (ICITST-2014)*. doi:10.1109/icitst.2014.7038849
- Alhadidi, B., Arabeyat, Z., Alzyoud, F., & Alkhaldeh, A. (2016). Cloud computing security enhancement by using mobile PIN code. *Journal of Computers, 11*, 225.
doi:10.17706/jcp.11.3.225-231
- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing:

Opportunities and challenges. *Information Sciences*, 305, 357–383.

doi:10.1016/j.ins.2015.01.025

Alves, D., Fernández-Navarro, P., Baptista, J., Ribeiro, E., Sousa, I., & Gonçalves, M. M.

(2013). Innovative moments in grief therapy: The meaning reconstruction approach and the processes of self-narrative transformation. *Psychotherapy Research*, 24, 25–41. doi:10.1080/10503307.2013.814927

Research, 24, 25–41. doi:10.1080/10503307.2013.814927

Ambre, A., & Shekocar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, 45, 436–445.

doi:10.1016/j.procs.2015.03.175

Anandarajan, M., D'Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud: Examining data breach notification legislation through the lens of routine activities theory. *International Data Privacy Law*, 3, 51–60.

doi.org/10.1093/idpl/ips035

Anderson, C. A., Leahy, M. J., DelValle, R., Sherman, S., & Tansey, T. N. (2014).

Methodological application of multiple case study design using modified consensual qualitative research (CQR) analysis to identify best practices and organizational factors in the public rehabilitation program. *Journal of Vocational Rehabilitation*, 41, 87-98. doi:10.3233/JVR-140709

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

Arntfield, M. (2015). Toward a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of*

Communication, 40, 371–388. doi:10.22230/cjc.2015v40n3a2863 Your references look great!

Arpaci, I., Kilicer, K., & Bardakci, S. (2014) Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, 45, 93-98. doi:10.1016/j.chb.2014.11.075

Australian Bureau of Statistics. (2013). Census and sample. Retrieved from <http://www.abs.gov.au/websitedbs/a3121120.nsf/home/statistical+language+-+census+and+sample>

Bacon, J., Eyers, D., Pasquier, T. F. J.-M., Singh, J., Papagiannis, I., & Pietzuch, P. (2014). Information flow control for secure cloud computing. *IEEE Transactions on Network and Service Management*, 11, 76–89. doi:10.1109/tnsm.2013.122313.130423

Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). *IEEE Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World—Impossible Without Standards?*, 275–282. doi:10.1109/kaleidoscope.2014.6858466

Barnes, J. (2015). Qualitative research from start to finish (2nd edn.). *Neuropsychological Rehabilitation*, 1–3. doi:10.1080/09602011.2015.1126911

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

- Bartolacci, M. R., LeBlanc, L. J., & Podhradsky, A. (2014). Personal denial of service (PDOS) attacks: A discussion and exploration of a new category of cyber crime. *Journal of Digital Forensics, Security and Law*, 9, 19–36.
doi:10.13052/jcsm2245-1439.335
- Belanger, K., Buka, S., Cherry, D. C., Dudley, D. J., Elliott, M. R., Hale, D. E., & Triche, E. W. (2013). Implementing provider-based sampling for the national children's study: Opportunities and challenges. *Paediatric and Perinatal Epidemiology*, 27, 20–26. doi:10.1111/ppe.12005
- Bekhet, A., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse Researcher*, 20, 40–43.
doi:10.7748/nr2012.11.20.2.40.c9442
- Bjerknes, M. S., & Bjørk, I. T. (2012). Entry into nursing: An ethnographic study of newly qualified nurses taking on the nursing role in a hospital setting. *Nursing Research and Practice*, 2012, 1–7. doi:10.1155/2012/690348
- Bonneau, J., Herley, C., Van Oorschot, P.C., & Stajano, F. (2015) Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58, 78-87.
doi:10.1145/2699390
- Bosler, A. M., & Holt, T. J. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, 29, 420–436. doi:10.1177/1043986213507401

- Brandas, C., Megan, O., & Didraga, O. (2015). Global perspectives on accounting information systems: Mobile and cloud approach. *Procedia Economics and Finance*, 20, 88–93. doi:10.1016/s2212-5671(15)00051-9
- Branic, N. (2015). Routine Activities Theory. *The Encyclopedia of Crime and Punishment*, 1–3. doi:10.1002/9781118519639.wbecpx059
- Braswell, M., McCarthy, B., & McCarthy, B. (2015). *Justice, Crime, and Ethics* (8th ed.). Retrieved from <http://www.tandfebooks.com/isbn/9781315721538>
doi:10.4324/9781315721538
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34, 523-A7.
- Bullée, J. H., Montoya, L., Pieters, W., Junger, M., & Pieter, H.H. (2015) The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), 97-115.
doi:10.1007/s11292-014-92229-7
- Bunch, J., Clay-Warner, J., & Lei, M. K. (2015). Demographic characteristics and victimization risk testing the mediating effects of routine activities. *Crime & Delinquency*, 61, 1181–1205. doi:10.1177/0011128712466932
- Burmeister E. (2012). Sample size: How many is enough? *Australian Critical Care*, 25, 271–274. doi:10.1016/j.aucc.2012.07.002
- Chander, M., Jain, S. K., & Shankar, R. (2013). Modeling of information security management parameters in indian organizations using ISM and MICMAC

- approach. *Journal of Modeling in Management*, 8, 171. doi:
<http://dx.doi.org/10.1108/JM2-10-2011-0054>
- Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, 1(1). doi:10.1109/tsc.2015.2491281
- Chang, V., Ramachandran, M., Yao, Y., Kuo, Y., & Li, C. (2016). A resiliency framework for an enterprise cloud. *International Journal Of Information Management*, 36, 155–166. doi:10.1016/j.ijinfomgt.2015.09.008.
- Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *Computer Science and Electronics Engineering*, 2012. doi:10.1109/iccsee.2012.193
- Chen, H. C. J., Violetta, M. A., & Yang, C. Y. (2013). Contract RBAC in cloud computing. *The Journal of Supercomputing*, 66, 1111. doi:10.1007/s11227-013-1017-5
- Cheng, F. (2014) Using focus groups with outsider and insider approaches: Preparation, process, and reflections. *SAGE Research Methods Cases*. London, United Kingdom: SAGE Publications, Ltd. doi: 10.4135/978144627305014528633
- Claycomb, W., & Nicholl, A. (2012). Insider threats to cloud computing: Directions for new research challenges. *IEEE 36th Annual Computer Software and Applications Conference, 2012*. doi:10.1109/compsac.2012.113
- Clarke, R. (2013). Data risks in the cloud. *Journal of Theoretical and Applied Electronic Commerce Research*, 8, 59. doi:10.4067/s0718-18762013000300005

- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588. doi:10.2307/2094589
- Cole-Miller, K., Ward, W., Fruhling, A., & Cooper, K.D. (2016). Social media policies in the Department of Defense—Do they address the risk? *Journal of Information Privacy and Security*, *12*, 93. doi:10.1080/15536548.2016.1180942
- Crete-Nishihata, M., Deibert, R., & Senft, A. (2013). Not by technical means alone: The multidisciplinary challenge of studying information controls. *IEEE Internet Computing*, *17*, 34. doi:10.1109/mic.2013.29
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. doi:10.1016/j.cose.2012.09.010
- Cruzes, D. S., Dyba, T., Runeson, P., & Host, M. (2014). Case studies synthesis: A thematic, cross-case, and narrative synthesis worked example. *Empirical Software Engineering*, *20*, 1634–1665. doi:10.1007/s10664-014-9326-8
- Czerkawski, B. (2016). Blending Formal and Informal Learning Networks for Online Learning. *The International Review of Research in Open and Distributed Learning*, *17*. doi:10.19173/irrodl.v17i3.2344
- Daigneault, P.-M., & Jacob, S. (2013). Unexpected but most welcome: Mixed methods for the validation and revision of the participatory evaluation measurement instrument. *Journal of Mixed Methods Research*, *8*, 6–24. doi:10.1177/1558689813486190
- Dawson, P. (2015). Five ways to hack and cheat with bring-your-own-device electronic

- examinations. *British Journal of Educational Technology* 47, 592–600.
doi:10.1111/bjet.12246
- De Costa, P. I. (2014). Making ethical decisions in an ethnographic study. *TESOL Quarterly*, 48, 413–422. doi:10.1002/tesq.163
- Denham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, 2015(1), 5–8. doi:10.1016/s1353-4858(15)70007-3
- Drawve, G., Thomas, S. A., & Walker, J. T. (2014). The likelihood of arrest: A routine activity theory approach. *American Journal of Criminal Justice*, 39, 450–470.
doi:http://dx.doi.org/10.1007/s12103-013-9226-2
- Drazen, J.M., Solomon C.G., & Greene, M.F. (2013) Informed consent and support. *The New England Journal of Medicine*, 368, 1929–1931. doi:10.1056/NEJMe1304996
- Elhaida, J. D., & Frueh, B. C. (2015). Security of electronic mental health communication and record-keeping in the digital age. *The Journal of Clinical Psychiatry*, 1, 478. doi:10.4088/jcp.14r09506
- Elifoglu, I. H., Guzey, Y., & Tasseven, O. (2014). Cloud computing and the cloud service user's auditor. *Review of Business*, 35, 76.
- Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, 4(1).
doi:10.1177/2158244014522633
- Endres, S., & Weibler, J. (2016). Towards a three-component model of relational social constructionist leadership: A systematic review and critical interpretive synthesis. *International Journal of Management Reviews*, n.p. doi:10.1111/ijmr.12095

- Ercikan, K., & Roth, W. M. (2014). Limits of generalizing in education research: Why criteria for research generalization should include population heterogeneity and users of knowledge claims. *Teachers College Record, 116*, 1.
- Erdos, D. (2014). Data protection and the right to reputation: Filling the “gaps” after the defamation act 2013. *The Cambridge Law Journal, 73*, 536–569.
doi:10.1017/s0008197314000877
- Everett, J., Neu, D., Rahaman, A. S., & Maharaj, G. (2015). Praxis, doxa and research methods: Reconsidering critical accounting. *Critical Perspectives on Accounting, 32*, 37–44. doi:10.1016/j.cpa.2015.04.004
- Fallahpour, M., & Zoughi, R. (2015). Fast 3-D qualitative method for through-wall imaging and structural health monitoring. *IEEE Geoscience and Remote Sensing Letters, 12*, 2463–2467. doi:10.1109/lgrs.2015.2484260
- Faniel, I. M., Minor, D., & Palmer, C. L. (2014). Putting research data into context: Scholarly, professional, and educational approaches to curating data for reuse. *Proceedings of the American Society for Information Science and Technology, 51*, 1–4. doi:10.1002/meet.2014.14505101016
- Farquhar, J. D. (2012). Philosophical assumptions of case study research. *Case study research for business*. London: Sage Publications Ltd.
doi:10.4135/9781446287910.n3
- Fegran, L., Hall, E. O., Uhrenfeldt, L., Aagaard, H., & Ludvigsen, M. S. (2014). Adolescents’ and young adults’ transition experiences when transferring from pediatric to adult care: A qualitative meta-synthesis. *International Journal of*

- Nursing Studies*, 51, 123–135. doi:10.1016/j.ijnurstu.2013.02.001
- Fernandes, D., Soares, L., Gomes, J., Freire, M., & Inacio, P. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, 13, 113–170. doi:10.1007/s10207-013-0208-7
- Fink, K., & Anderson, C. W. (2014). Data journalism in the united states. *Journalism Studies*, 16, 467–481. doi:10.1080/1461670x.2014.939852
- Franklin, C. A., Franklin, T. W., Nobles, M. R., & Kercher, G. A. (2012). Assessing the effect of routine activity theory and self-control on property, personal, and sexual assault victimization. *Criminal Justice and Behavior*, 39, 1296–1315. doi:10.1177/0093854812453673
- Freeman, I. (2016). Cross-Cultural Awareness and the Practice of Corporate Social Responsibility in Canada: The Case of Target. *i-Manager's Journal on Management*, 9, 10.
- Freitas, L., & Watson, P. (2014). Formalizing workflows partitioning over federated clouds: Multi-level security and costs. *International Journal of Computer Mathematics*, 91, 881–906. doi:10.1080/00207160.2013.820282
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20, 1408.
- Gergen, K. J., Josselson, R., & Freeman, M. (2015). The promises of qualitative inquiry. *American Psychologist*, 70, 1. doi:10.1037/a0038597
- Ghilic-Micu, B., Stoica, M., & Uscatu, C. R. (2014). Cloud Computing and Agile Organization Development. *Informatica Economica*, 18, 5–13.

doi:10.12948/issn14531305/18.4.2014.01

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing, 1*, 1–18.

doi:10.1186/2192-113x-1-11

Grbich, C. (2015) Narrative analysis: The socio-cultural approach to analysing short participant stories. *Sage Research Methods Datasets*. Sage Publications Ltd.

doi:10.4135/9781473947498

Green, C. A., Duan, N., Gibbons, R. D., Hoagwood, K. E., Palinkas, L. A., & Wisdom, J. P. (2015). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health and Mental Health Services Research, 42*, 508.

doi:10.1007/s10488-014-0552-6

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. (2013). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. *e-Service Journal, 9*, 106–138. doi:10.2979/eservicej.9.1.106

Grenier, R. S., & Dudzinska-Przesmitzki, D. (2015). A conceptual model for eliciting mental models using a composite methodology. *Human Resource Development Review, 14*, 163–184. doi:10.1177/1534484315575966

Gutmann, J. (2014). Qualitative research practice: A guide for social science students and researchers (2nd edn). *International Journal of Market Research, 56*, 407.

doi:10.2501/ijmr-2014

- Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *Physical Educator*, 72. doi:10.18666/tpe-2015-v72-i5-6133
- Haimes, Y. Y., Horowitz, B. M., Guo, Z., Andrijcic, E., & Bogdanor, J. (2015). Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems. *Systems Engineering*, 18, 284–299. doi:10.1002/sys.21303
- Hammond, M. (2013). The contribution of pragmatism to understanding educational action research: Value and consequences. *Educational Action Research*, 21, 603–618. doi:10.1080/09650792.2013.832632
- Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report*, 17, 510.
- Harrison, N., & Kirkham, J. (2014). The application of reflexivity in small business research and implications for the business practitioner. *Industry and Higher Education*, 28, 439–447. doi:10.5367/ihe.2014.0232
- Harriss, D., & Atkinson, G. (2013). Ethical standards in sport and exercise science research: 2014 update. *International Journal of Sports Medicine*, 34, 1025–1028. doi:10.1055/s-0033-1358756
- Hart, J. (2013). Feature: Why the traditional approach to information security is no longer working. *Network Security*, 2013(1), 12–14. doi:10.1016/S1353 4858(13)70019-9
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and*

Applications, 4(1), 5. doi:10.1186/1869-0238-4-5

- Hassan, H. M., Reza, D. M., & Farkhad, M. A.-A. (2015). An Experimental Study of Influential Elements on Cyberloafing from General Deterrence Theory Perspective Case Study: Tehran Subway Organization. *International Business Research*, 8. doi:10.5539/ibr.v8n3p91
- Hathcoat, J. & Nicholas, M. (2014). Epistemology. *The Sage Action Research*, 5, 303-307. London: Sage Publications Ltd. doi:10.4135/9781446294406.n108
- Hawley, A. H. (1950). Human ecology: a theory of community structure. *American Sociological Review*, 15, 684. doi:10.2307/2086931
- Hemalatha, N., Jenis, A., Cecil Donald, A., & Arockiam, L. (2014). A comparative analysis of encryption techniques and data security issues in cloud computing. *International Journal of Computer Applications*, 96, 1–6. doi:10.5120/16875-6873
- Hendre, A., & Joshi, K. P. (2015). A Semantic Approach to Cloud Security and Compliance. *2015 IEEE 8th International Conference on Cloud Computing*. doi:10.1109/cloud.2015.157
- Henson, B., Reynolds, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, 29, 475. doi:10.4398/6213507403.
- Hjorth, L., & Sharp, K. (2014). The art of ethnography: the aesthetics or ethics of participation? *Visual Studies*, 29, 128. doi:10.1080/1472586x.2014.887261

- Hollis, M. E., & Wilson, J. (2014). Who are the guardians in product counterfeiting? A theoretical application of routine activities theory. *Crime Prevention and Community Safety, 16*, 169. doi.org/10.1057/cpcs.2014.6
- Holtfreter, K. (2015). General theory, gender-specific theory, and white-collar crime. *Journal of Financial Crime, 22*, 422. doi:10.1108/jfc-12-2014-0062
- Hong, X., & Rong, C. (2014). Multiple data integration service. *IEEE 2014 28th International Conference on Advanced Information Networking and Applications*. 860–865. doi:10.1109/waina.2014.163
- Hossein, R., Elankovan S., Zulkarnain, A., Abdullah Mohd, Z. (2013). Encryption as a service (EaaS) as a solution for cryptography in cloud. *Procedia Technology, 11*, 1202. doi:10.1016/j.protcy.2013.12.314
- Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20*, 12. doi:10.7748/nr2013.03.20.4.12.e326
- Houshmand, S., & Aggarwal, S. (2012). Building better passwords using probabilistic techniques. *Proceedings of the 28th Annual Computer Security Applications Conference*, 109. doi:10.1145/2420950.2420966
- Hughes, L., & Short, J. (2013). Partying, cruising, and hanging in the streets: Gangs, routine activities, and delinquency and violence in Chicago, 1959-1962. *Journal of Quantitative Criminology, 30*, 415. doi:10.1007/s10940-013-9209-y
- Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*,

1.

- Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being*, 9(1), 23606. doi:10.3402/qhw.v9.23606
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31, 83. doi:10.1016/j.cose.2011.10.007
- Ionita, M., & Patriciu, V. (2016). Secure threat information exchange across the internet of things for cyber defense in a fog computing environment. *Informatica Economica*, 20, 16. doi:10.12948/issn14531305/20.3.2016.02
- Islam, S., Mouratidis, H., & Weippl, E. R. (2013). A goal-driven risk management approach to support security and privacy analysis of cloud-based system. *Security Engineering for Cloud Computing*, 97. doi:10.4018/978-1-4666-2125-1.ch006
- Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79-91. doi:10.5281/zenodo.58523
- Johnson, M. E., Brems, C., Hanson, B. L., Corey, S. L., Eldridge, G. D., & Mitchell, K. (2013). Conducting ethical research with correctional populations: Do researchers and IRB members know the federal regulations? *Research Ethics*, 10, 6–16. doi:10.1177/1747016113494652
- Kajtazi, M., Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2014). Assessing Sunk Cost

- Effect on Employees' Intentions to Violate Information Security Policies in Organizations. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (3169-3177). IEEE. doi.org/10.1109/hicss.2014.393
- Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces*, 36, 759–775. doi:10.1016/j.csi.2013.12.010
- Karanasios, S. (2014). Framing ICT4D research using activity theory: A match between the IC4TD field and theory? *Information Technologies & International Development*, 10, 1–17. doi:10.1080/02681102.2014.910635
- Kazim, M., & Ying, S. (2015). A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications*, 6. doi:10.14569/ijacsa.2015.060316
- King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, 28, 308–319. doi:10.1016/j.clsr.2012.03.003
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. doi:10.1016/j.jisa.2014.09.005
- Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37, 372–386. doi:10.1016/j.telpol.2012.04.011

- Lee, C. S., McNeill, N. J., Douglas, E. P., Koro-Ljungberg, M. E., & Therriault, D. J. (2013). Indispensable resource? A phenomenological study of textbook use in engineering problem solving. *Journal of Engineering Education, 102*, 269. doi:10.1002/jee.20011
- Lee, N., Balut, R., & Stanford, J. C. (2015). Cybersecurity Training in Medical Centers: Leveraging Every Opportunity to Convey the Message. *Counterterrorism and Cybersecurity, 287–300*. doi:10.1007/978-3-319-17244-6_11
- Leonard, P. (2014). Customer data analytics: Privacy settings for ‘big data’ business. *International Data Privacy Law, 4*, 53–68. doi: 10.1093/idpl/ipt032
- Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyber Psychology, Behavior & Social Networking, 17*, 551–555. doi:10.1089/cyber.2014.0008
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*, 263–280. doi:10.1080/01639625.2015.1012409
- Leung, L. (2015). Validity, reliability, and generalizability in research. *Journal of Family Medicine & Primary Care, 4*, 324–327. doi: 10.4103/2249-4863.161306.
- Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice, 16*, 473–475. doi:10.1177/1524839915580941

- Li, J., Chen, X., Li, M., Li, J., Lee, P. P., & Lou, W. (2014). Secure deduplication with efficient and reliable convergent key management. *Parallel and Distributed Systems, IEEE Transactions*, *25*, 1615–1625. doi:10.1109/tpds.2013.284
- Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*, 28–36. doi:10.1016/j.ijinfomgt.2013.09.004
- Lim, S. S., Vos, T., Flaxman, A. D., Danaei, G., Shibuya, K., Adair-Rohani, H., Andrews, K. G. (2012). A comparative risk assessment of burden of disease and injury attributable to 67 risk factors and risk factor clusters in 21 regions, 1990–2010: A systematic analysis for the global burden of disease study. *The Lancet*, *380*, 2224–2260. doi:10.1016/s0140-6736(12)61766-8
- Lin, G. T., Lin, C. C., Chou, C. J., & Lee, Y. C. (2014). Fuzzy modeling for information security management issues in cloud computing. *International Journal of Fuzzy Systems*, *16*, 529.
- Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, *39*, 7–47. doi:10.1162/isec_a_00189
- Liu, Y., Sheng, X., & Marston, S. R. (2015). The impact of client-side security restrictions on the competition of cloud computing services. *International Journal of Electronic Commerce*, *19*, 90–117. doi:10.1080/10864415.2015.1000224
- Liu, Y., Wang, L., Yuan, C., & Li, Y. (2012). Information communication, organizational capability and new product development: An empirical study of Chinese firms.

The Journal of Technology Transfer, 37, 416–432. doi:10.1007/s10961-010-91881

Lowry, P. B., & Moody, G. D. (2014). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, 25, 433–463.

doi:10.1111/isj.12043

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods*, 14, 1–8.

doi:10.1177/1609406915621406

Mallaiah, K., & Ramachandram, S. (2014). Applicability of homomorphic encryption and CryptDB in social and business applications: Securing data stored on the third party servers while processing through applications. *International Journal of Computer Applications*, 100, 5–19. doi:10.5120/17487-7999

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

McConnell-Henry, T., Chapman, Y., & Francis, K. (2011). Member checking and heideggerian phenomenology: A redundant component. *Nurse Researcher*, 18, 28–37. doi:10.7748/nr2011.01.18.2.28.c8282

McNeeley, S. & Wilcox, P. (2015). Street codes, routine activities, neighborhood context and victimization. *British Journal of Criminology*, 55, 921–943.

doi:10.1093/bjc/azu116

Mehl-Madrona, L., Mainguy, B., & Valenti, M. P. (2013). Mixed methodology

- approaches to exploring spiritual transformation. *The Qualitative Report*, 18, 1.
- Mendoza, V. (2014). Measurement, tips, and errors: Making an instrument design in risk perception. *Research Methods Cases*. London, United Kingdom: Sage Publications, Ltd. doi:10.4135/978144627305013519224
- Mergel, I., & Bretschneider, S. I. (2013). A three-stage adoption process for social media use in government. *Public Administration Review*, 73, 390–400. doi:10.1111/puar.12021
- Metheny, M. (2017). A case study for cloud service providers. *Federal Cloud Computing*, 473. doi:10.1016/b978-0-12-809710-6.00014-7
- Miller, B., & Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology - RIIT '12*. doi:10.1145/2380790.2380805
- Miller, J. (2013). Individual offending, routine activities, and activity settings: Revisiting the routine activity theory of general deviance. *Journal of Research in Crime & Delinquency*, 50, 390–416. doi:10.1177/0022427811432641
- Mohamed, M.,A., & Pillutla, S. (2014). Cloud computing: A collaborative green platform for the knowledge society. *Vine*, 44, 357. doi:10.1108/vine-07-2013-0038
- Moon, B., Morash, M., Jeong, S., & Yoon, H. S. (2015). Gender differences in the routine activities associated with risks for larceny in south korea. *International Journal of Offender Therapy and Comparative Criminology*, 60, 1327. doi:10.1177/0306624x15578631
- Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative

inquiry. *Qualitative Health Research*, 25, 1212–1222.

doi:10.1177/1049732315588501

Mortari, L. (2015). Reflectivity in Research Practice. *International Journal of Qualitative Methods*, 14, 160940691561804. doi:10.1177/1609406915618045

Mouratidis, H., Islam, S., Kalloniatis, C., & Gritzalis, S. (2013). A framework to support selection of cloud providers based on security and privacy requirements. *The Journal of Systems and Software*, 86, 2276–2293. doi:10.1016/j.jss.2013.03.011

Mukwasi, C., & Seymour, L. (2012). Enterprise Resource Planning Business Case Considerations: A Review for Small and Medium-Sized Enterprises. *Journal of Innovation Management in Small & Medium Enterprises*, 1–15.

doi:10.5171/2012.752328

Newton, A., & Felson, M. (2015). Editorial: Crime patterns in time and space: The dynamics of crime opportunities in urban areas. *Crime Science*, 4.

doi:10.1186/s40163-015-0025-6

Nishimura, A., Carey, J., Erwin, P. J., Tilburt, J. C., Murad, M. H., & McCormick, J. B. (2013). Improving understanding in the research informed consent process: A systematic review of 54 interventions tested in randomized control trials. *BMC Medical Ethics*, 14(1). doi:10.1186/1472-6939-14-28

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterizing attacks. *2014 IEEE Security and Privacy Workshops*. doi:10.1109/spw.2014.38

Onwuegbuzie, A. J., & Corrigan, J. A. (2014). Improving the quality of mixed research

reports in the field of human resource development and beyond: A call for rigor as an ethical practice. *Human Resource Development Quarterly*, 25, 273.

doi:10.1002/hrdq.21197

O'Reilly, M., & Parker, N. (2012). 'Unsatisfactory saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, 13, 190-197. doi:1468794112446106.

Peppard, J., Galliers, R. D., & Thorogood, A. (2014). Information systems strategy as practice: Micro strategy and strategizing for IS. *The Journal of Strategic Information Systems*, 23, 1–10. doi:10.1016/j.jsis.2014.01.002

Policastro, C., & Payne, B. (2014). Can you hear me now? Telemarketing fraud victimization and lifestyles. *American Journal of Criminal Justice*, 40, 620–638. doi:10.1007/s12103-014-9279-x

Pyrooz, D. C., Decker, S. H., & Moule Jr, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, 32, 471–499. doi:10.1080/07418825.2013.778326

Qi, H., & Gani, A. (2012). Research on mobile cloud computing: Review, trend and perspectives. *2012 Second International Conference on Digital Information and Communication Technology and Its Applications (DICTAP), 2012*, 195-202. doi:10.1109/dictap.2012.6215350

Rafeeq, M. D., & Kumar, C. S. (2015). Reliable secure data storage in the cloud environments and de duplication. *International Journal of Computer Science and Engineering*, 3, 1086–1091.

- Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, 48, 204–209.
doi:10.1016/j.procs.2015.04.171
- Rathi, A., & Parmar, N. (2015). Secure cloud data computing with third party auditor control. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, 145–152.
doi:10.1007/978-3-319-12012-6_17
- Ray, D. (2016). Cloud adoption decisions: Benefitting from an integrated perspective. *Electronic Journal of Information Systems Evaluation*, 19(1), 3.
- Reinmoeller, P., & Ansari, S. (2015). The Persistence of a Stigmatized Practice: A Study of Competitive Intelligence. *British Journal of Management*, 27(1), 116–142.
doi:10.1111/1467-8551.12106
- Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, 16, 69–73. doi:10.1109/mic.2012.14
- Reyns, B. W. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50, 216–238.
- Reyns, B. W. (2015). A routine activity perspective on online victimization. *Journal of Financial Crime*, 22, 396–411. doi:10.1108/jfc-06-2014-0030
- Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none identifying determinants for online identity theft victimization with routine

activity theory. *International journal of offender therapy and comparative criminology*, 60, 1119–1139. doi:10.1177/0306624x15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as It Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, 32, 148–168. doi:10.1177/1043986215621378

Rezaeibagha, F., Khin Than, W., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal*, 44, 23–38.

doi:10.12826/18333575.2015.0001.Rezaeibagha

Riungu-Kalliosaari, L., Taipale, O., & Smolander, K. (2012). Testing in the cloud: Exploring the practice. *IEEE Software*, 29, 46–51. doi:10.1109/ms.2011.132

Riungu-Kalliosaari, L., Taipale, O., Smolander, K., & Richardson, I. (2014). Adoption and use of cloud-based testing in practice. *Software Quality Journal*.

doi:10.1007/s11219-014-9256-0

Rizvi, S., & Mitchell, J. (2015). A semi-distributed access control management scheme for securing cloud environment. *2015 IEEE 8th International Conference on Cloud Computing*, 501–507. doi:10.1109/cloud.2015.73

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

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering

through transformational leadership, information security culture and awareness.

Computers & Security, 59, 26. doi:10.1016/j.cose.2016.01.004

Rodrigues, J. J., de la Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of Medical Internet Research*, 15(8), e186.

doi:10.2196/jmir.2494

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, 39, 47–54.

doi:10.1016/j.compeleceng.2012.04.015

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

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

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

Ruegg, J., Gries, C., Bond-Lamberty, B., Bowen, G. J., Felzer, B. S., McIntyre, N. E., Weathers, K. C. (2014). Completing the data life cycle: using information management in macrosystems ecology research. *Frontiers in Ecology and the Environment*, 12(1), 24–30. doi:10.1890/120375

- Ryan, J. (2013). Book Review: Karin Olson, *Essentials of Qualitative Interviewing*. *Qualitative Research*, 13, 254. doi:10.1177/1468794112450832
- Samani, R., Honan, B., Reavis, J., (2015). *CSA guide to cloud computing*, xiii. doi:10.1016/b978-0-12-420125-5.09002-6
- Savin, F. A., Gongalsky, K. B., & Pokarzhevskii, A. D. (2006). The necessary amount of sampling for census and assessing the taxonomic diversity of large soil invertebrates in different geographic zones. *Russian Journal of Ecology*, 37, 35–40. doi:10.1134/s1067413606010061
- Schaefer, L., & Mazerolle, L. (2015). Putting process into routine activity theory: Variations in the control of crime opportunities. *Security Journal*. doi:10.1057/sj.2015.39
- Schmidlin, K., Clough-Gorr, K. M., & Spoerri, A. (2015). Privacy preserving probabilistic record linkage (P3RL): A novel method for linking existing health-related data and maintaining participant confidentiality. *BMC Medical Research Methodology*, 15(1), 1. doi:10.1186/s12874-015-0038-6
- Schober, M. M., Gerrish, K., & McDonnell, A. (2016). Development of a conceptual policy framework for advanced practice nursing: An ethnographic study. *Journal of Advanced Nursing*, 72(6), 1313–1324. doi:10.1111/jan.12915
- Schreier M. (2012). *Qualitative content analysis in practice*. Thousand Oaks, CA: Sage Publications. doi:10.1075/ssol.3.1.15aaf
- Shah, H., Anandane, S. S., & Shrikanth. (2013). Security issues on cloud computing. *International Journal of Computer Science and Information Security*, 11, 25–34.

- Silbey, S. S. (2013). Organizational challenges to regulatory enforcement and compliance a new common sense about regulation. *The Annals of the American Academy of Political and Social Science*, 649, 6–20. doi:10.1177/0002716213493066
- Sinkovics, R. R., & Alfoldi, E. A. (2012). Progressive focusing and trustworthiness in qualitative research. *Management International Review*, 52, 817–845. doi:10.1007/s11575-012-0140-5.
- Sloan, A., & Bowe, B. (2015). Experiences of Computer Science Curriculum Design: A Phenomenological Study. *Interchange*, 46, 121. doi:10.1007/s10780-015-9231-0
- Smith, G. S. (2016). Evaluating materiality in cybercrime footnotes. *Journal of Corporate Accounting and Finance*, 27, 77–87. doi:10.1002/jcaf.v27.2
- Sookhak, M., Gani, A., Khan, M. K., & Buyya, R. (2015). Dynamic remote data auditing for securing big data storage in cloud computing. *Information Sciences*, doi:10.1016/j.ins.2015.09.004.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36, 215–225. doi:10.1016/j.ijinfomgt.2015.11.009
- Stake, R. E. (2013). *Multiple case study analysis*. London: Guilford Press.
- Stanley, M., & Nayar, S. (2014). Methodological rigour: Ensuring quality in occupational therapy qualitative research. *New Zealand Journal of Occupational Therapy*, 61(1), 6.
- Stuckey, H. L., Kraschnewski, J. L., Miller-Day, M., Palm, K., Larosa, C. & Sciamanna, C. (2014). “Weighing” two qualitative methods: Self-report interviews and direct

observations of participant food choices. *Field Methods*, 26, 343—361. doi:
10.1177/1525822X14526543

Sunyaev, A., & Schneider, S. (2013). Cloud services certification. *Communications of the ACM*, 56, 33. doi:10.1145/2408776.2408789

Suo, S. (2013). *Cloud implementation in organizations: Critical success factors, challenges, and impacts on the it function* (Order No. 3576584). Available from ABI/INFORM Collection. (1467505085). Retrieved from <http://search.proquest.com/docview/1467505085?accountid=45049>

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

Tankard, C. (2015). Feature: Data classification – the foundation of information security. *Network Security*, 2015, 8–11. doi:10.1016/S1353-4858(15)30038-6

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, 316–322. doi:10.1016/j.giq.2015.05.001

Tracy, S. J. (2012). The Toxic and Mythical Combination of a Deductive Writing Logic for Inductive Qualitative Research. *Departures in Critical Qualitative Research*, 1(1), 109–141. doi:10.1525/qcr.2012.1.1.109.

Trochim, W. M.K. (2006). Research Methods Knowledge Base. *Web Center for Social Research Methods*. Retrieved from <http://www.socialresearchmethods.net/kb/qualval.php>

- Trulove, W. G. (2015). Legal Issues for the Medical Director. *Clinical Journal of the American Society of Nephrology*, *10*, 1651. doi:10.2215/cjn.0644061
- Tsang, E. W. K. (2014). Case studies and generalization in information systems research: A critical realist perspective. *The Journal of Strategic Information Systems*, *23*, 174–186. doi:10.1016/j.jsis.2013.09.002
- Tsang, E. W. (2014). Generalizing from research findings: The merits of case studies. *International Journal of Management Reviews*, *16*, 369–383. doi:10.1111/ijmr.12024
- Turanovic, J. J., & Pratt, T. C. (2014). Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization. *Journal of quantitative criminology*, *30*, 29–56. doi:10.1007/s10940-012-9188-4
- U.S. Department of Health and Human Services. (1979, April 18). *The Belmont Report*. Retrieved from HHS.gov: <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html#xrespect>
- Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2015). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*. *32*, 169–188. doi:10.1177/1043986215621379
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*, 398–405. doi:10.1111/nhs.12048
- Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: Researching

desires and realities. *Journal of Information Technology*, 27, 179–197.

doi:10.1057/jit.2012.17

Wagner, C., Mitter, S., Körner, C., & Strohmaier, M. (2012). When social bots attack:

Modeling susceptibility of users in online social networks. *Making Sense of Microposts (#MSM2012)*, 2.

Waleed, M. A., Chunlin, L., & Naji, H. A. (2014). The faults of data security and privacy in the cloud computing. *Journal of Networks*, 9, 3313-3320.

doi:10.4304/jnw.9.12.3313-3320

Wang, J., Gupta, M., Rao, H., & Raghav. (2015). Insider threats in a financial institution:

analysis of attack-proneness of information systems applications. *Management Information Systems Quarterly*, 39(1), 91–112.

Ward, P. S., & Pede, V. O. (2015). Capturing social network effects in technology

adoption: the spatial diffusion of hybrid rice in Bangladesh. *Australian Journal of Agricultural and Resource Economics*, 59, 225-241. doi:10.1111/1467-

8489.12058

Weber, V., & Carblanc, A. (2014). *Cloud computing: The concept, impacts and the role*

of government policy. Paris: Organisation for Economic Cooperation and Development (OECD). Retrieved from

<http://search.proquest.com/docview/1558355157?accountid=45049>

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014).

Security and privacy for storage and computation in cloud computing.

Information Sciences, 258, 371–386. doi:10.1016/j.ins.2013.04.028

- Weidmann, N. B. (2015). A closer look at reporting bias in conflict event data. *American Journal of Political Science*, n.p. doi:10.1111/ajps.12196
- Weisburd, D., Groff, E. R., & Yang, S.-M. (2014). The importance of both opportunity and social disorganization theory in a future research agenda to advance criminological theory and crime prevention at places. *Journal of Research in Crime and Delinquency*, 51, 499–508. doi:10.1177/0022427814530404
- Wei-Wen, W., Lan, L. W., & Yu-Ting, L. (2013). Factors hindering acceptance of using cloud services in university: A case study. *The Electronic Library*, 31, 84–98. doi:http://dx.doi.org/10.1108/02640471311299155
- Wheatley, A. (2014). Do-It-Yourself Privacy: The need for comprehensive federal privacy legislation with a private right of action. *Golden Gate University Law Review*, 45, 265.
- Wheeler, A., & Winburn, M. (2015). *Cloud storage security: A practical guide*. Amsterdam, Netherlands: Elsevier.
- Whitley, E. A., Willcocks, L. P., & Venters, W. (2013). Privacy and security in the cloud: A review of guidance and responses. *Journal of International Technology and Information Management*, 22, 77.
- Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, 56, 21–48. doi:10.1093/bjc/azv011
- Willardson, S. (2013). Strategic intelligence during coin detention operations – relational data and understanding latent terror networks. *Defense & Security Analysis*, 29(1),

42–53. doi:10.1080/14751798.2013.760249

Wohlin, C., & Aurum, A. (2014). Towards a decision-making structure for selecting a research design in empirical software engineering. *Empirical Software Engineering* 20, 1427–1455. doi:10.1007/s10664-014-9319-7

Wren, D., & Barbera, J. (2013). Gathering evidence for validity during the design, development, and qualitative evaluation of thermochemistry concept inventory items. *Journal of Chemical Education*, 90, 1590–1601. doi:10.1021/ed400384g

Yeh, H.-W., Gajewski, B. J., Perdue, D. G., Cully, A., Cully, L., Greiner, K. A., Daley, C. M. (2013). Sorting it out: pile sorting as a mixed methodology for exploring barriers to cancer screening. *Quality and Quantity*, 48, 2569–2587. doi:10.1007/s11135-013-9908-3

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: epistemological, theoretical, and methodological differences. *European Journal of Education*, 48, 311–325. doi:10.1111/ejed.12014

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

Yin, R.K. (2014). *Case study research. Design and methods*. (Fifth Edition). Alternatives (Thousand Oaks), CA: Sage Publications, Inc.

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

Zhang, J., & Zhang, Z. (2014). Secure and efficient data-sharing in clouds. *Concurrency*

and Computation: Practice & Experience, 27, 2125–2143. doi:10.1002/cpe.3395

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future*

Generation Computer Systems, 28, 583–592. doi:10.1016/j.future.2010.12.006

Appendix A: Interview Protocol

Interview Protocol	
What you will do	What you will say—script
<p>Introduce the interview and set the stage—often over a meal or coffee</p>	<ul style="list-style-type: none"> • The purpose of this study is to explore the strategies IT security manager use to host sensitive information in the commercial cloud. The research conducted in this study may benefit information security practice by increasing understanding on the complex nature of internal and external threats; security strategies that better protect sensitive information stored in the cloud. This study should provide IT security managers with a robust framework for assessing the security of sensitive information against internal and external data breaches. • Indicate that interviewer will be taking notes. • Indicate that interviewer will be recording the conversation for transcription. • Advise the participant there will be an opportunity to ask questions at the end of the interview.

<ul style="list-style-type: none"> • Watch for non-verbal queues • Paraphrase as needed • Ask follow-up probing questions to get more in-depth 	<p>1. What habits do you repeatedly see among cloud-hackers when you consider which security strategies to implement?</p>
	<p>2. What security vulnerabilities in the cloud-computing environment have you experienced?</p>
	<p>3. What types of insider or outsider attacks in the cloud has your organization experienced?</p>
	<p>4. What do you consider is the impact of these insider or external attacks?</p>
	<p>5. In what ways have insider or external data breaches affected the cloud services provided to your clients?</p>
	<p>6. What were your challenges addressing insider or external threats in your organization's use of cloud computing?</p>
	<p>7. What security strategies have you used that failed to secure sensitive information in the cloud?</p>
	<p>8. What security strategies have you used that succeeded to secure sensitive information in the cloud?</p>
	<p>9. What additional information would you like to provide that I have not already asked?</p>
	<p>10. Last interview question should be a wrap up question such as: What additional experiences have you had...?</p>

<p>Wrap up interview thanking participant</p>	<p>Ask the participant if he or she has any questions and provide responses to these.</p> <p>Highlight the potential positive aspects of working within the study.</p> <p>Describe the next steps in the interviewing process (e.g., member checks) and provide a clear timeframe for when the participant will hear from the interviewer again.</p> <p>Thank the participant for his or her participation and time</p>
<p>Schedule follow-up member checking interview</p>	<p>I would like to follow up with you in the next day or two to go over a brief summary of your answers.</p>
<p>Follow-up Member Checking Interview</p>	
<p>Introduce follow-up interview and set the stage</p>	<ul style="list-style-type: none"> • This is a follow up interview to go over previous summary of answers.

<p>Share a copy of the succinct synthesis for each individual question</p>	<ul style="list-style-type: none"> • Ask the participant if he or she has any questions and provide responses to the summary. • Reintroduce the questions and answers. • Ask if they have anything to add.
<p>Bring in probing questions related to other information that you may have found—note the information must be related so that you are probing and adhering to the IRB approval.</p> <p>Walk through each question, read the interpretation and ask: Did I miss anything? Or, what would you like to add?</p>	<p>1. What habits do you repeatedly see among cloud-hackers when you consider which security strategies to implement?</p>
	<p>2. What security vulnerabilities in the cloud-computing environment have you experienced?</p>
	<p>3. What types of insider or outsider attacks in the cloud has your organization experienced?</p>
	<p>4. What do you consider is the impact of these insider or external attacks?</p>
	<p>5. In what ways have insider or external data breaches affected the cloud services provided to your clients?</p>
	<p>6. What were your challenges addressing insider or external threats in your organization's use of cloud computing?</p>
	<p>7. What security strategies have you used that failed to secure sensitive information in the cloud?</p>

	8. What security strategies have you used that succeeded to secure sensitive information in the cloud?
	9. What additional information would you like to provide that I have not already asked?

Appendix B: Observation Protocol

The purpose of this observation protocol is to provide a step action table (job aide, checklist) to help you stay focused on the data and other details that you observe in the setting.

Directions: To start each observation, write a comprehensive description of the setting following the table below. Using the table on the next page, note the approximate time frames in which you make the observations, along with notes describing what you see occurring and any other details that you consider to be important. After the observation, review your notes and begin to identify key points (concepts and ideas) that may help you later in data analysis.

Name of Researcher	Edward Forde
Tentative Schedule	7:00pm – 8:30pm
Date:	December 1, 2016
The Background: Physical setting (Describe in thick rich detail what it looks like, sounds like, and any other details.)	Meeting was held at Training Center One. The room could hold about 100 persons. There were about 45 people in attendance. Attire was casual dress. They served Papa John's pizza prior to the meeting where patrons could mingle and network with other colleagues for about 30 minutes.
The Position: (i.e., close, distance, etc.)	I sat in the middle of the room to both observe the presentation, take audio recordings, take notes, and write down audience participation
The Action: What happens? What is the sequence? Is there a cause and effect? If so, provide details.	Training Center 1 Meeting presented Trainer One, who teaches SANS SEC511: Continuous Monitoring and Security Operations and SEC542: Web Application Penetration Testing and Ethical Hacking. He presented FREQ.PY. The program calculates the likelihood of character pairings occurrence based on frequency analysis in DNS server logs and client DNS logs/cache.

Type of Observation: (direct or participant)	The researcher conducted a direct observation of the training session.
Areas Training Focused on:	Where Blue Team tactics, system administrators, and system analysts need to look for adversaries in networks and cloud computing environments. How to look for and find character pairings occurrence based on frequency analysis in DNS server logs and client DNS logs/cache.
Time:	Observation notes:
7:30pm	Most attackers love DNS:
	<ul style="list-style-type: none"> • Most systems require name resolution
	<ul style="list-style-type: none"> • Traffic allowed outbound
	<ul style="list-style-type: none"> • Proxied by design
	<ul style="list-style-type: none"> • High Volume of Benign traffic.
	Exploitation: Required element of client side exploitation (SA's never look at client side exploits).
	Security is hooked on Blacklist. Adversaries also know this. So, adversaries employ rapid turn around and programmatic generations of fake websites were clients go to and get infected.
	Logs offer high-level visibility into events. A Correlation amongst numerous log sources is essential to reconstruct a consistent occurrence timeline and is a good preliminary point for security analysts and incident responders.
	Establish a baseline of whether it is standard for IP 1 to talk to IP 2 based on the volume of connections from the enterprise to the destination
	Educate your Blue Team tactics, system administrators, and system analysts to at the DNS logs. It is the forgotten log that no one likes to look at.
	Your Blue Team tactics, system administrators, and system analysts can train your users on those fake websites.
8:30pm	No Questions. End of discussion and meeting.