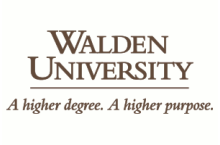

2020

Relationship Between Specific Security Concerns and CIO Intention to Adopt Cloud

Johnathan Francis Van Houten
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Johnathan Van Houten

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. Gary Griffith, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

Relationship Between Specific Security Concerns and CIO Intention to Adopt Cloud

by

Johnathan Van Houten

MS, Walden University, 2018

BS, University of Phoenix, 2015

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2020

Abstract

Cloud computing adoption rates have not grown commensurate with several well-known and substantially tangible benefits such as horizontal distribution and reduced cost, the latter both in terms of infrastructure and specialized personnel. The lack of adoption presents a challenge to both service providers from a sales perspective and service consumers from a usability focus. The purpose of this quantitative correlational study utilizing the technological, organizational, and environmental framework was to examine the relationship between shared technology (ST), malicious insiders (MI), account hijacking, data leakage, data protection, service partner trust (SP), regulatory concerns and the key decision-makers intention to adopt cloud computing. Additionally, the modifiers of firm size and scope were applied to verify any correlative impact. Data were analyzed from 261 participants all executive technology decision-makers across a diverse field of firms in the United States. The binary logistic regression analysis showed that ST, MI, and SP were all significant predictors $X^2(9, N = 261) = 227.055$, $p < .001$. A key recommendation is that providers should focus on the three primary areas of concern (ST, MI, and SP) for decision-makers, emphasizing mitigation, communication, and education to foster trust in the cloud paradigm, promoting greater adoption. The implication for social change includes the potential for greater adoption of cloud computing, thus providing enterprise-class operations to nonprofit and social agencies that may otherwise be unable to provide these services to their communities.

Relationship Between Specific Security Concerns and CIO Intention to Adopt Cloud

by

Johnathan Van Houten

MS, Walden University, 2018

BS, University of Phoenix, 2015

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2020

Dedication

I am dedicating this work to my wife, Melanie, my mother Patricia, and my father, Frank. Without the latter two, I would not be the person who could undertake such a journey. They instilled in me the desire to pursue one's intentions but most important, to achieve them through hard work and relentlessness. My tenacity and strength emanate from theirs. While my father did not live to see me finish, he did see me begin, and that perhaps that is enough, as he knew I would never rest until I completed this task.

Melanie, there is no way I could have begun this without your support. Becoming a doctor has been a lifelong dream of mine, one that I was sure had passed me by. You were the one who challenged me, who told me that if it was my dream then to make it a reality. I would not have made it here without your support. My life is infinitely better because I can see it through your eyes, your dreams, and your emotional intelligence.

I would also like to dedicate this to my son, Benjamin. Benjamin, I have, since becoming your dad, focused on doing my best to make you as proud of me as I am of you. To show you that it is never too late to chase your dreams and to never give up on anything you feel passionate about.

While the dream to one day earn a doctorate was mine, the acquisition is not mine alone, as my family were there to encourage and applaud for every milestone, suffering in silence without me as I invested all my time into this project. They are my reasons for achieving this, and so I dedicate this to them, Melanie, Patricia, Benjamin, and Caitlyn. Thank you for always being there for me, even when I could not be there for you.

Acknowledgments

I would like to acknowledge all the professors along this journey who excelled in their roles; always available to answer a myriad of questions with well-conceived and cogent responses to propel me along with greater insight. Whenever I needed encouragement, I thought back to my first residency wherein quite honestly and frankly the leadership noted how few would complete the program; I vowed I would be one of those few and during the darkest times I used that as fuel for the fire. I wish to thank by name Dr. Gary Griffith, my chair for this process, who may not always have had the answer (or perhaps the one I was looking for) but who was present and available to offer support and encouragement along the way. Dr. Stephen Case as my co-chair and methodologist, whose attention to detail is something I can appreciate, even when I didn't appear to be so accommodating. Lastly, Dr. Nicholas Harkiolakis, who introduced me to quantitative analytical methods that spoke to me right from the start.

Table of Contents

List of Tables v

List of Figures vi

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

Hypotheses 5

Theoretical Framework 5

Definition of Terms 7

Assumptions, Limitations, and Delimitations 9

Assumptions 9

Limitations 10

Delimitations 10

Significance of the Study 11

Contribution to Information Technology Practice 11

Implications for Social Change 12

A Review of the Professional and Academic Literature 13

Cost Savings and Ease of Use Established 17

Security Concerns as Impediment 20

Perceived Realities 31
Value to Prioritizing Perceived Risk 32
Theoretical Framework 34
Gaps in the Literature / Relationship to Prior Research 48
Transition and Summary 51
Section 2: The Project 54
Purpose Statement 54
Role of the Researcher 54
Participants 57
Research Method and Design 59
Method 60
Research Design 63
Population and Sampling 65
Ethical Research 69
Data Collection 71
Instruments 78
Data Collection Technique 82
Data Analysis Technique 83
Data Screening 86
Missing Data 88
Assumptions 88
Reliability and Validity 90

Reliability 90
Validity 91
Transition and Summary 95
Section 3: Application to Professional Practice and Implications for Change 97
Overview of Study 97
Presentation of the Findings 98
Data Reliability 100
Data Analysis Assumptions 101
Inferential Analysis Results 105
Summarization of the Findings 109
Interpretation of Results 110
Theoretical Framework Discussion 113
Applications to Professional Practice 119
Implications for Social Change 123
Recommendations for Action 124
Recommendations for Further Study 126
Reflections 128
Summary and Study Conclusions 129
References 131
Appendix A: NIH Training Certificate 172
Appendix B: Email Invitation to Participate in Research 173
Appendix C: Approvals for Use of Survey Instruments 174

Appendix D: Survey Instrument 177

List of Tables

Table 1 *Status of Research Articles* 16

Table 2 *Representation of Firm scope Among Respondents* 99

Table 3 *Representation of Firm Size Among Respondents* 99

Table 4 *Percentage of Respondents Understanding the Threat Vectors* 100

Table 5 *Reliability Statistics Using Cronbach's Alpha* 101

Table 6 *Multicollinearity Statistics* 105

Table 7 *Goodness of Fit* 107

Table 8 *Model Fitting Information* 108

Table 9 *Classification Table* 109

Table 10 *Statistics for Variables in the Equation* 109

Table 11 *Statistics for Variables in the Equation (RO – SC)* 114

List of Figures

Figure 1. TOE contexts representing the components of this study 7

Figure 2. Power as a function of sample size ……69

Figure 3. P-P Plots of all variables indicating normality ……103

Section 1: Foundation of the Study

Background of the Problem

Purchasing and maintaining an information technology (IT) infrastructure is cost prohibitive, therefore, despite the value to a business, educational organizations, and not-for-profit institutions, many IT infrastructures languish with older technology because of budgetary constraints (Nayar & Kumar, 2018). Cloud computing represents a new paradigm, providing on-demand services, self-regulation, scalability, and a simplistic interface for control while lowering the total cost of ownership (TCO), yet, regardless of these benefits, adoption rates have not grown, as decision-makers find certain aspects prohibitive (Changchit & Chuchuen, 2018). The concerns focus on security aspects of public cloud computing and specifically the lack of confidentiality and integrity of consumer data, thus discouraging the adoption of cloud for critical services (Changchit & Chuchuen, 2018). Agarwal, Siddharth, and Bansal (2016), discussed the evolution of cloud relative to security concerns, presenting various threat vectors, however, did not engage potential decision-makers in determining which threats present the largest detractors to adoption.

The cloud computing model is the most efficient, regarding cost and usability, for an organization to employ (Hashem et al., 2015). Support from the executive decision-makers within the management tiers is essential to achieve adoption of cloud resources (Alkhater, Walters, & Wills, 2018). To encourage the adoption of cloud computing for critical systems, the inclusion of decision-makers in the process of developing strategies

toward mitigating concerns increases awareness for cloud providers regarding perceived limitations (Alkhater et al., 2018).

Problem Statement

Concerns emanating from perceived realities regarding security vulnerabilities impact adoption of public cloud with findings in a Delphi study identifying security as the top concern (El-Gazzar, Hustad, & Olsen, 2016). A 2017 study examining various factors that promote or inhibit cloud adoption across the United States found that the perceived lack of security prevented growth into the cloud market (Kinuthia & Chung, 2017). Similarly, Karkonasasi, Baharudin, Esparham, Mousavi, and Suhaimi Baharudin (2016) found in their study of Malaysian enterprises that security concerns ranked highest among factors inhibiting the well-known cost-savings benefits of cloud. The general IT problem is the limited acceptance of public cloud infrastructure because of security-related perceived vulnerabilities. The specific IT problem is that some IT design architects lack information regarding the relationship between chief information officers (CIOs) and IT directors perceptions of shared technology (ST) risks, malicious insiders (MI), account hijacking (AH), data leakage (DL), data protection (DP), service partner trust (SP), regulatory compliance (RC) concerns, firm scope (SC), firm size (FS), and intention to adopt public cloud infrastructures.

Purpose Statement

The purpose of this quantitative correlational study was to evaluate the relationship between the independent variables consisting of ST, MI, AH, DL, DP, SP, RC, SC, FS, and the dependent variable intention to adopt public cloud infrastructures.

The specific population group was CIOs and IT directors from large to small enterprises within the United States. A potential element of positive social change this study may contribute to is the enhancement of service capability for consumers of nonprofit organizations (NPO) through implementation of enterprise-class services and a lowered TCO.

Nature of the Study

The methodology I used for this study is quantitative. Quantitative methods attempt to measure an objective reality, represented numerically, to determine whether a phenomenon is real and whether associations exist among variables (McCusker & Gunaydin, 2015). Quantitative research relies on numbers, both in terms of data set and statistical information garnered through processing and obtained using observation via survey instruments applying closed questions designed to elicit specific responses to quantify relationships across a large data set in a more objective and observable fashion provide the basis of contrast and comparison (Basias & Pollalis, 2018). If the research intends to measure beliefs or concepts of normative behavior, or if the goal is to reveal potential problems as input variables that are as yet unknown to interpret a phenomenon, then qualitative research is more appropriate (Hammarberg, Kirkman, & de Lacey, 2016). A mixed-methods approach combines both quantitative and qualitative methodologies to investigate both variable relations and individualized experiences to derive patterns in complex research questions (McCusker & Gunaydin, 2015). For these reasons, I decided to forego a qualitative method, as I was aware through review of extant literature of the pertinent variables and a mixed-method approach, and because the research question was

not complex and did not require personal experience. I chose quantitative methodology because I did not require an interpretation of phenomena and am aware of the dependent and independent variables. My intent was to determine whether and to what degree a relationship exists between the adoption of cloud and various security-focused impediments.

The decision toward a research design perspective is important because each approach differs in their goals and procedures, thus requiring alignment with the intent of the study. The correlational design is used to descriptively demonstrate, through the analysis of evidence gathered, whether there is a relationship between independent and dependent variables (Curtis, Comiskey, & Dempsey, 2016). I intended to use correlational designs because my study requires an understanding of the association between inclination toward adoption of cloud computing and the various security impediments as perceived by executive decision-makers toward migration to cloud resources. Causal-comparative designs focus on cause-and-effect relationships using multiple groups to vary the experiences across a control group and the target population expressing the factor under study (Van der Stede, 2014). Experimental studies typically use an intervention or treatment as the independent variable to test the behavioral impact of manipulating the independent variable on the target population (Dulmer, 2016). I did not choose either of these designs, as my intent was neither to derive causation, nor to present a manipulated variable in a pretest-posttest scenario. My correlational design used a calculation of the correlation coefficient (a bivariate correlation analysis) that determines the strength of the relationship between variables, and regression analysis to

predict the outcome of the impact of certain variables on others. The intent was to establish and measure the degree of impact the independent variables, consisting of ST, MI, AH, DL, DP, SP, RC, FS, and SC present to the key decision makers as an impediment to cloud adoption.

Research Question

RQ: What is the relationship between (a) ST, (b) MI, (c) AH, (d) DL, (e) DP, (f) SP, (g) RC, and the propensity by executive decision makers to adopt cloud computing?

Hypotheses

H_o: There is no relationship between (a) ST, (b) MI, (c) AH, (d) DL, (e) DP, (f) SP, (g) RC, and the propensity by executive decision makers to adopt cloud computing.

H_a: There is a significant relationship between (a) ST, (b) MI, (c) AH, (d) DL, (e) DP, (f) SP, (g) RC, and the propensity by executive decision makers to adopt cloud computing.

Theoretical Framework

The technology-organization-environment (TOE) framework, originally developed by Tornatzky and Fleischer (1990), as an extension to the technology acceptance model (TAM), is the process by which context influences the adoption and implementation of technological innovation at the organizational level. The TOE framework explains that three distinct elements (i.e., technological context, organizational context, and environmental context) influence technological innovation (Klug & Xue, 2015; Tornatzky & Fleischer, 1990). The inclusion of these variables provides an advantageous position for studying adoption as it provides a holistic

viewpoint for technology acceptance, implementation, chained impact, and post-adoption diffusion, in addition to business attributes toward decision-making (Gangwar, Date, & Ramaswamy, 2015). The technological context includes all relevant technologies and technologically impacting factors, whereas organizational context focuses on the organization and its characteristics (i.e., organizational structure), such as firm size and scope (Lippert & Govindarajulu, 2006). The environmental context assesses the firm's capacity to trust external resources such as technology service providers, and express concern for MI, DL, and the impact of regulation (Lippert & Govindarajulu, 2006; Wahsh & Dhillon, 2016). The three contexts represent constraints and opportunities for an organization (Tornatzky & Fleischer, 1990). The model focuses on correlative relationships between contextual constructs and an organization's willingness to adopt new and innovative technology (Lippert & Govindarajulu, 2006). In this study, I examined the relationship between these independent contextual variables and the dependent variable, cloud adoption. Figure 1 depicts the basic framework with contexts as they apply to my study parameters.

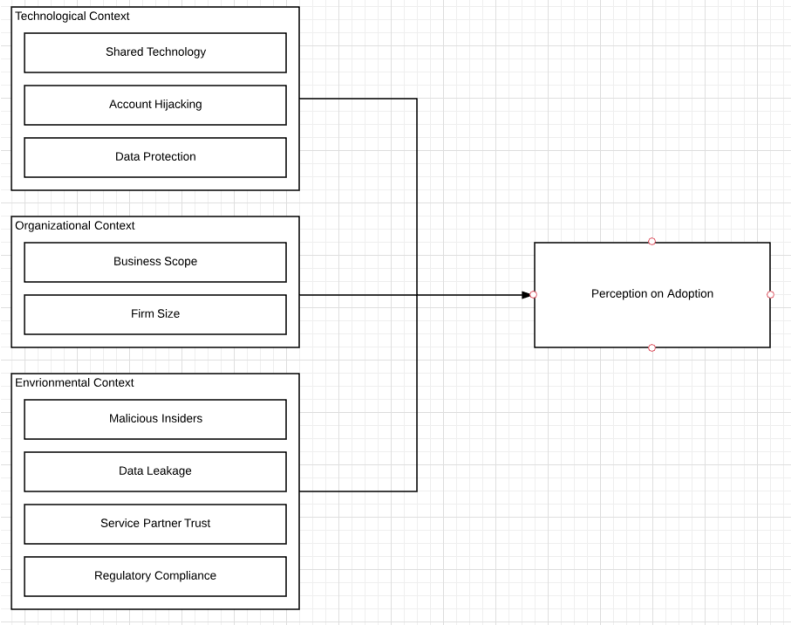

Figure 1. TOE contexts representing the components of the study.

Definition of Terms

Compliance: Refers to the implication of enforcing rules and programs that protect privacy and contribute to security of data by the enforcement of confidentiality, integrity, and availability attributes; often referred as regulatory compliance to infer state or sovereign nation rules and policies (Yimam & Fernandez, 2016).

Decision-makers: Within the scope of the IT realm in a corporation or other operating entity, the decision-maker is the key executive or appointee that ultimately chooses to invest in new technologies and adapts their decision to align with the preconceived opinions (Rezaei, 2016).

Firm scope: Broadly defined by the industry or breadth of product offering and geographical diversification (Kovach, Hora, Manikas, and Patel (2015).

Firm size: Although extant literature often fails to define the term across the study landscape, the definition has often presented in terms of number of employees and annual revenue as determinants (Dang, Li, & Yang, 2018).

Malicious insiders: While the standard definition indicates current or previous employees from the business entity, extending that to cloud services, wherein an organization's data and systems (to include potentially sensitive information) extends to the provider organization (Alassafi, Alharthi, Walters, & Wills, 2017).

Regulatory compliance: Regulations may originate as governmental (host country or any country in which the entity operates and all governmental requirements contained therein) or emanate from within the corporate structure as guiding policies (Hsu & Lin, 2016; Senyo, Effah, & Addae, 2016).

Service partner trust: The degree of confidence in a provider of services unique to the business entity and necessary for both operations and management regarding the confidentiality, integrity, and availability of data and services (Alassafi et al., 2017; Phaphoom, Wang, Samuel, Helmer, & Abrahamsson, 2015).

Shared technology: Inherent in the shared cloud platform space (as opposed to private cloud) provisions services via shared technology frameworks without the opportunity for complete isolation of resources, whereas other concerns stem from the control platform or hypervisor (Ali, Khan, & Vasilakos, 2015; Kazim & Zhu, 2015).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions exist as conditionals that are considered true, founded in a pre-existing belief structure and preference relation as it associated to a lexicographic conditional probability system (Dekel, Friedenberg, & Siniscalchi, 2016). Founded in a wide array of abstractions, assumptions may originate from cultural, political, social, or historical constructs within the individual conceptualizing them (Wolgemuth, Hicks, & Agosto, 2017). As such, assumptions may set the agenda for research and thus, forming a self-fulfilling reinforcement that must receive redress to remain critically impartial and retain objectivity (Sharpo, Lawlor, & Richardson, 2018). Haegele and Hodge (2015) noted that major assumptions of quantitative research define evidence of a hard reality and the ability to discover the nature of it while reporting accurate statements during the research investigation designed to predict relationships. Researchers must remove themselves from the study to remain unbiased, which is possible in quantitative research when a researcher considers the variance between values and facts (Haegele & Hodge, 2015). While attempting to not inject personal theory into the selection process, I assumed first that the respondents would provide accurate and complete results. Secondly, I assumed that each participant would fit the profile of a key decision-maker within their organization, as previously defined. My third assumption contributes to the first in that each respondent finds value in the results, thus proving a relatable interest in the outcome.

Limitations

Limitations may impact validity, both internally for study design and integrity and externally as generalizations within the scope of reported results (Greener, 2018). Identifying limitations and exporting the potential for adverse impact on the study results displays a sense of academic and scientific rigor in addition to providing clarified direction for future research (Greener, 2018). Limitations, also termed weaknesses, of a study may include sampling size or technique employed which then impacts the ability to generalize the findings adequately (Astroth & Chung, 2018). An imposed limitation I intentionally included was the absence of randomized sampling in favor of nonprobability convenience sampling as my selections will be provided by a service that is outside the scope of my control. The lack of randomized sampling confers the limitation for generalizing my findings across a broader spectrum of decision-makers. The sampling size must be a consideration for limitations moving forward, as are the inherent factors within quantitative method studies, such as the focus on empirical as opposed to contextual data (Quick & Hall, 2015). There are inherent limitations in the nature of the study, in that respondents may answer dishonestly or provide responses that do not align with their personal biases as a result of misunderstanding the subject.

Delimitations

Delimitations are established boundaries or constraints placed by the researcher on the study to include its collection of findings and reporting as to define what material is acceptable and within scope (Wiesmann, Snoei, Hilletofth, & Eriksson, 2017). I attempted not to limit the geographic scope of the respondents in this study to a single

state, so as to achieve greater activity from often singular entities in an organization responsible for decision-making, a broad view is necessary. For the purpose of this study, the United States will serve as the only geographical boundary and delimitation, thus also limiting the degree of influence by the researcher. I chose specific threat variables derived from repeated mention within the corpus of literature, removing those that were repetitive or rarely noted.

Significance of the Study

IT organizations that offer cloud computing services benefit from a larger adoption rate in several key areas. Workload prediction and consolidation enables a provider to more efficiently utilize hardware within their datacenter, employing fewer resources to provide dynamic growth under load and the management benefits associated with virtualized containers (Dabbagh, Hamdaoui, Guizani, & Rayes, 2015). Migrating more of the single-space solutions to cloud enablement eases the burden of platform management while reducing overhead costs for the provider.

Contribution to Information Technology Practice

Decreasing costs while increasing efficiency is a contemporary problem facing all IT enterprises; the purchase of hardware, the cost to maintain, and the cyclic requirement to refresh and begin the process anew is a challenge (Nayar & Kumar, 2018). Migrating services into cloud operations environments permits rapid development, deployment, ease of managing resources that precludes the necessity of specialized personnel and reduces cost as such services exist as on-demand enablement (Nayar & Kumar, 2018). The research is significant to IT personnel from both the purveyor and procurer of cloud

computing resources. Cloud operations require a reduced requirement for specialized personnel to manage the base systems or the virtualized roles as software-defined environmental controls allow for single updates to images and execution of migration. Cloud virtualization simplifies the managerial roles for the customers' IT departments as well, reducing the necessity of employing infrastructure personnel in favor of simplified interface controls to enable reduction of the virtualized resources.

The research enables cloud service providers the opportunity to receive direct influence from potential customers across a variety of businesses across a diverse size structure. The data will present, by the degree of importance, those security impediments to adoption deemed most impactful by decision-makers in executive roles, thus enabling IT practitioners to drive a path toward cloud adoption.

Implications for Social Change

The implications for positive social change include enabling non-profit and not-for-profit organizations access to the same enterprise-class architectures currently in use by only those entities large enough to afford on-premises workloads. Decreased costs and required specialists allow such cost-focused operations to focus on development as opposed to management of resources. A reduction in the IT budget allows for the more effective use of such funds toward the goals and intentions of the organization, thus offering two prime benefits, increased reach and capability as well as reduced costs for overhead.

Another benefit to social change, specifically with nonprofit and not-for-profit organizations, is the cloud enablement of cognitive analytics and big data. Analytics

provides organizations with the capability to understand and respond to consumer needs, garnering market share, or engage more meaningfully with patrons (Tan, Zhan, Ji, Ye, & Chang, 2015). Analysis of structured and unstructured data from social media outlets provide businesses with essential data used to navigate customer needs and maximize efficiencies; the same would be available for NPOs (Feng, Du, & Ling, 2017).

Investment and enablement of cloud operations also reduce the carbon footprint an entity produces for similar or extended operational capabilities (Singh, Mishra, Ali, Shukla, & Shankar, 2015). Singh et al. (2015) found that cloud enablement reduced generated carbon emissions by virtualizing their entire supply chain while lowering their TCO.

A Review of the Professional and Academic Literature

Although discussion of the advancement and promotion of cloud computing initiatives for enterprises emphasizes the potential for cost-savings and ease of use, the technology fails to attract a larger audience commensurate with these derived benefits, primarily because of security concerns (Aldossary & Allen, 2016; Balasooriya, Wibowo, Grandhi, & Wells, 2017). While I would concur with this assessment, I found the plethora of literature too broad in scope and lacking definition by which practitioners may articulate mitigating strategies in a prioritized fashion to achieve greater adoption. Therefore, I did not focus on well-established benefits as a counter to the negative aspects of security concerns but, rather, targeted the various threat vectors and prioritized those perceived security concerns by the decision-makers across a wide spectrum of enterprises. The purpose was to develop a hierarchical approach to and define the values

for each security threat to foster greater adoption thorough targeted mitigating strategies. Greater adoption of cloud confers benefits in several key measures of positive social change. Wider dissemination of enterprise-class architectures at greatly reduced cost allows NPOs to enjoy the same degree of infrastructure benefits typically withheld to those organizations that could afford on-premise workload computing. Reducing the IT budget permits organizations to focus on development as opposed to management of resources and confers innate computation benefits such as enablement of analytics and big data to assess consumer needs (Tan et al., 2015). Big data analytics involves large volumes of heterogeneous data from which one extracts valuable information. Though often attributed to dedicated infrastructure, it is more efficient and cost-saving within an open cloud landscape, thus enabling computational benefits for enterprises of all sizes (Yang, Huang, Li, Liu, & Hu, 2017).

In this quantitative correlational study, my intent was to identify and hierarchically define the extent of relationships between perceived security concerns and active adoption of cloud resources within the United States. Within the scope of the literature review, I identify the purpose and include a synthesis of the data to express the foundation of the variables included within the hypothesis, including those that are unnecessary and the rationale of focusing on perceived insecurities. Additionally, I present information on the TOE framework and the three contexts that provide a dynamic encapsulation of relevant material.

The literature review is comprised of peer-reviewed journal articles and conference papers all published between 2015 and 2019, in addition to several seminal

sources, notably conference material and books from noteworthy scholars in the field. I used a variety of mechanisms to derive the content including Walden University's library databases, which comprise publications across a number of sources (to include IEEE Xplore, ProQuest Central, Sage, the ACM Digital Library, Science Direct, and EBSCO Host's Applied Sciences), as well as Google Scholar to index references through my undergraduate library sources and alternate sources available within the medium. The search strategy used in the various databases focused on certain keywords and phrases related to the framework. Among the more common themes, the key words emphasized cloud adoption, perceived realities as influencers, security of cloud, and concerns about compliance with regulatory measures. The key words, therefore included *cloud adoption, security concerns with cloud, perceived security concerns with cloud, impeding cloud adoption, threats to cloud, benefits of cloud, privacy issues with cloud,* and *regulatory concerns with cloud*.

The study contains references from 253 academic papers and journal articles, of which 94.1% are peer reviewed (n =238), 2% are seminal works (n = 5), and 3.6% are conference papers (n = 10). In addition, 94.5% were published within the five years prior to the expected date of completion and CAO approval, and 5.7% (n = 14) were not (see Table 1). I identified whether sources were peer reviewed through UlrichsWeb Global Serials Directory.

Table 1

Status of Research Articles

Reference Data	Total Number
Total references	253
Peer-reviewed sources	238
Non-peer-reviewed sources	15
Seminal sources	5
Conference papers	10
Published within 5-years of publication	239
Published outside of 5-year period from publication	14
Percentage of peer-reviewed source material	94.1%
Percentage of material published within 5-year period	94.5%
Percentage published within 5-year period and peer-reviewed	90.5%

The review of professional and academic literature defines contexts in several key areas: (a) the TOE framework, (b) the identification of non-essential inclusion for independent variables, (c) the identification and extrapolation of key independent variables as conduits for impeding adoption of cloud, (d) the establishment of perceived realities as an important consideration and foundational for the study parameters, and (e) the value to prioritizing perceived risks. As the goal was to establish the presence and degree of relationship value between each of the perceived security impediments and the propensity for decision-makers to adopt cloud, the null hypothesis establishes a lack of

relationship between each of the independent variables and the dependent variable. Conversely, the alternate hypothesis postulates a key relationship between one or more of the security impediments as independent variables and the propensity of decision-makers to adopt cloud.

Cost Savings and Ease of Use Established

A common theme among published works focusing on the adoption or implementation decision for cloud computing are the positive aspects of the migration, notably the inherent cost savings combined with the easy-to-use interface and available options (Oliveira, Thomas, & Espadanal, 2014). Alkhalil, Sahandi, and John (2017) found that cost and agility, defined as ease of deployment and scalability, were the two foremost factors considered relative advantages to cloud adoption. Similarly, Balasooriya et al. (2017) found that cloud offers business opportunities to reduce operational costs while improving services and providing greater scalability. These perceived benefits and reduced costs should incur a significant influence on adoption, albeit the cost variable would require significant savings to offset the fees associated with migration in order to break the status quo paradigm (Fan, Wu, Chen, & Fang, 2015; Rathi & Given, 2017). There exists a certain degree of bias against deferring to new technology, or more to the point, adhere to existing and proven technology rather than risk uncertainty (Antons & Piller, 2015). Structural inertia, often referring to the specifically developed architecture, reveals a measure of entrenchment in these structures, perhaps because of or despite poor management (Fan et al., 2015).

Regardless, when factoring costs-savings, more than merely the infrastructure design impacts the financial considerations. The cost of computing will decrease, as will the necessity to engage in highly specialized labor, thus also decreasing overhead costs to the enterprise (Hsu & Lin, 2016). The ease of deployment and configuring resources simplifies the approach significantly to achieve the scalable design. The pay-as-you-go model ensures that costs are attributed to only those resources deemed necessary and managed through self-service interfaces offering financial efficiencies of scale, operational excellence, and continuous innovation (Phaphoom et al., 2015). Applying the theory of relative advantage, which includes cost flexibilities and improved scalability and productivity, Senyo et al. (2016) found that such variables were significant factors when considering the adoption of cloud. It is important to note that when cost-savings drive the relative advantage parameters for the adoption of cloud computing technologies, the intent was to focus on multitenancy as a means to reduce said operational costs such as those founded in specialized IT support staff (Lo, Yang, & Guo, 2015). Nayar and Kumar (2018) performed analysis directly considering the cost-benefit value, focusing on education as the consumer of cloud services and described the challenges associated with such an enterprise purchasing, maintaining, and installing both hardware and software provided by constrained budgets. Additionally, analysis into cost issues included the decreasing lifespan of system hardware, thus increasing expenditures every three to four years merely to remain viable, which does not include software update costs (Nayar & Kumar, 2018).

Cloud-based opportunities offer viable alternatives at a fraction of the short and long-term costing models associated with traditional hardware development (Nayar & Kumar, 2018; Tweneboah-Koduah, Endicott-Popovsky, & Tsetse, 2014). For NPOs or educational realms, the cost reductions regarding capital expenses and operational expenses allow these organizations to operate aligned with enterprise-class architectures, paying for only those services required by maintaining control over resources (Nayar & Kumar, 2018). Similarly, Khanal, Parsons, Mantz, and Mendelson (2016) noted that costs incurred only for those services utilized with initial investment far lower than traditional purchasing of hardware and software, allowing consumers to concern themselves less with fees and the management of the underlying infrastructure as opposed to their business operations thus making cloud operations extremely attractive. Maresova, Sobeslav, and Krejcar (2017) evaluated the cloud computing deployment model for a cost-benefit analysis within the corporate structure finding that significant benefits in terms of cost advantages, the flexibility of service renderings, and the elasticity of services as prime motivators. The overhead of computational resources and the purchase of software as well as the savings of energy consumed and the reduced staffing requirements formed the foundation of quantifiable cost and benefits (Maresova et al., 2017). Cloud services, specifically spot-based, offer opportunities for operational entities, such as NPOs or educational enterprises, to defer costs even further for time-flexible, interruption-tolerant tasks such as those for computational measurements, further reducing the operational costs and pay for services as required (Al-Badi, Tarhini, & Al-Kaaf, 2017). Such operations offer tangible benefits to organizations that operate

with reduced margins and budgetary constraints such as NPOs of reduced size thus proffering inherent value (Rathi & Given, 2017). Computational elasticity (i.e., the ability to scale both horizontally and vertically) to create new instances within a platform space infer a cost-savings with the aforementioned scalability benefits, while reducing the expenditures associated with hardware and controls for maintenance and focusing on the application tier as opposed to the entire stack (Akkaya, Sari, & Al-Radaideh, 2016).

Despite the prevailing data purporting the cost and scalability of cloud architectures for enterprises, adoption has not been commensurate. The potential target variables preventing the more widespread adoption of cloud must exist outside the scope of financial viability and management considerations.

Security Concerns as Impediment

Privacy and security concerns are key barriers to adoption of cloud services by individuals and enterprises, often interpreted by decision-makers as immaturity because of a lack of viable standards, or a failure to comprehend the security threats inherent in cloud (Balasooriya et al., 2017; Kalaiprasath, Elankavi, & Udayakumar, 2017). Security concerns, defined as privacy issues and DP indicate as the highest rationalization to impede the progress of cloud adoption by decision-makers within enterprises (Khan & Al-Yasiri, 2016). Due to these concerns, a mere 10% of U.S. organizations (19% of European organizations) employ cloud and those that do, utilize it for only the most innocuous of services, while 70% of participants in a survey on cloud adoption noted their intentions to forego migration for fears emanating from data security and privacy concerns (Balasooriya et al., 2017). In another survey performed by Rao and Selvamani

(2015), 70% of respondents considered security issues critical as a factor under consideration for adoption, while an additional 25% noted such factors as very important.

In the same study wherein Senyo et al. (2016) provided ample evidence and analysis of survey data to prove a relative advantage as a predominant factor in the adoption of cloud, the second proven context variable was cloud security (or lack thereof) as a significant impact on perceived viability. Similarly, perceived security (defined as the extent to which the enterprise believes the service is risk-free) ranked highest in a study performed by Hsu and Lin (2016), particularly in the manufacturing sector, but relevant across the various scopes. Furthermore, Fan et al., (2015) and Wu (2016) prove that status quo biases such as perceived risk because of uncertainties with data security, exacerbate the limitation of adoption. Phaphoom et al. (2015) determine security and privacy (denoted as two distinct objectives in the study) are critical barriers to adoption while offering extended views into perceptions by examining the variances between those who already adopted cloud to some extent, and those that have not. A lack of clarity or ambiguity of security perceptions potentially reduce the overall inclination to adopt cloud operations, the authors suggest a greater degree of transparency regarding cloud security control mechanisms as one means of identifying the gap between security objectives and security perceptions (Phaphoom et al., 2015). A notable requirement toward increasing the understanding of those that decide upon cloud adoption was to develop a basic understanding of general security and to understand the perceptions of those in a position to formalize adoption (Alkhalil et al., 2017). In the analysis of their study investigating factors impacting government adoption of cloud computing technologies, Wahsh and

Dhillon (2016), aside from proving the absolute impact of security factors, were prescient in their inclusion and interpretation of perceptions as factors. However, they did not include security perception among them. The introduction of the concept of perception as an influencing factor is important, as it implies a degree of knowledge (correct or otherwise) relied upon by the decision-maker in determining the viability of the technology. In a study exploring the factors that have prevented more widespread adoption of cloud, Rai, Sahoo, and Mehfuz (2015) noted the impediment of security issues on the adoption rate. Similarly, Rao and Selvamani (2015) found that security issues were critical consideration across 70% of responses to their quantitative study and an additional 25% considered security as very important to decision-making.

Shrivas, Singh, and Dubey (2016) approach the security concerns across the various types of cloud interpretations, again grouping the majority of threats into the data security construct and adding privacy as a separate concern. The impetus for self-awareness and communication with the provider is an imperative regarding security as a prime motivating factor against adoption, specifically the criticality of applications and sensitive data (Kaur & Singh, 2015). Security, to include privacy and trust, were found to be significant factors, directly impacting organizations' decisions to adopt cloud services, and differed slightly based on FS and SC, offering insight as to the mitigating circumstances provided by these two variables (Alkhater et al., 2018). Continuing the idea of perception becoming a factor in the decision process Gangwar, and Date (2016) note that as prior work indicates, cost and ease of use define relative advantage (RA), driving intent to adopt, yet security risks decrease the RA as well as the perceived

usefulness of the technology. Indeed, perception of low-security impact consumers' view toward the technology, and those with a lower tolerance for risk would, therefore, prefer to forego adoption. The study performed by Gangwar and Date proves that despite the perceived relative advantages of cloud adoption, organizations were unwilling to invest because of perceived security concerns without some standardization or procedural mitigations in place. It is also apparent that data privacy is becoming more relevant as laws protecting individuals increase in complexity, potentially causing managerial issues for the enterprise. Key to a successful implementation of the cloud is the assurance using documented processes and procedures of protection mechanisms. Investigating the scope of education, Arpaci, Kilicer, and Bardakci (2015) note that student's attitudes toward the risks involved with the cloud (security and privacy) are less inclined to utilize cloud, that the perceived security (or lack thereof) will have an impeding influence on adoption. The results indicate that providers will need to increase the security and privacy perceptions of the users, be they enterprise clients, students, governments, or NPOs, in order to achieve greater adoption rates for cloud (Arpaci et al., 2015). Security and confidentiality added to a lack of service controls thus promoting a concept of regulatory disconnect highlight as considerable drawbacks to cloud computing services (Kreslins, Novik, & Vasiljeva, 2018). Perceptions influence decisions and arise from an understanding, or lack thereof, for a particular subject (e.g., security) for which education is of vital importance in providing a greater degree of understanding leading to wider adoption (Alkhalil et al., 2017).

Security, in the context of threats and vulnerabilities, is a primary impeding factor when considering the migration to the cloud. The very fabric of the information service landscape increases in complexity for the service provider, thus promoting more complex threat vectors (Coppolino, D'Antonio, Mazzeo, & Romano, 2017). Privacy, a factor deemed most significant in the healthcare industry, is the primary expressed concern and thus delays adoption within that industry (Akkaya et al., 2016). Additionally, perceptions of security risks by those in decision-making positions are equally integral to the intention to adopt cloud. Therefore, to successfully mitigate both the actual and perceived threats against cloud-based infrastructures, practitioners will require knowledge as to the specific concerns that drive negative intentions. A hierarchical approach will permit a priority-based mitigation path, allowing practitioners to investigate and resolve issues that impact the greater number of potential customers initially. However, first, it is necessary to discern the parameters that drive security concerns to acquire well-established and documented vulnerabilities. A study performed by Arpaci et al. (2015) indicates it is the responsibility of providers to increase security perceptions on their user base, regardless of scope or size of the enterprise in order to achieve saturation for cloud adoption.

Security parameters. Many studies and peer-reviewed journal articles encapsulate threats into data and network varieties, while others group data and privacy concerns as distinct items. Many of the attack formations and threat vectors that exist in traditional operations also present in the cloud, the difference lay within the scope of the virtualization and how the least secure tenant impacts co-inhabitants (Singh, Jeong, &

Park, 2016). Additionally, internal communications within the cloud are subject to a lack of formalized zone defense mechanisms, such as encountered in traditional operations, instead, cloud operations rely on open communication and crosstalk within the same security zone, thus diminishing the least access right advantage (Ali et al., 2015; Gholami & Laure, 2016). Therefore, the breakdown of security vectors and vulnerabilities encapsulates as broad a scope of threat categories as defined by the ingress vectors, which could, therefore, approach similar mitigation techniques.

Data risks. Within the scope of data risks, are data leakage, protection, and loss (Ali et al., 2015; Balasooriya et al., 2017; Kazim & Zhu, 2015). Further dissection of these data risks is necessary to promote them as different ideologies and as such, require different mechanisms to mitigate.

Data leakage. The term *data leakage* may refer to both a network or system vulnerability, as it includes malicious sniffing within the network segment or utilizing tools and functions to acquire information through illicit means (Ali et al., 2015). Within the confidentiality, integrity, and availability triad of security posture, leakage exists in the confidentiality realm, as it exposes private data to unauthorized persons (Alassafi et al., 2017; Cayirci, Garaga, De Oliveira, & Roudier, 2016). Kazim and Zhu (2015) consider a data breach as the leakage of sensitive information without expressed authorization.

Data protection. The protection of data confers the necessity to remove or prevent the capability to alter information by unauthorized persons and as such, represents a lack of integrity for the system information (Alassafi et al., 2017; Warth et

al., 2017). While it is entirely plausible that unauthorized modifications can and may occur in addition to either leakage or loss, it is not necessarily required. The ingress may be programmatic, as opposed to network based (Kalaiprasath et al., 2017; Phaphoom et al., 2015; Rao & Selvamani, 2015).

Data loss. Similar to protection, it is a vital component of any security posture to prevent the loss of data, however, unlike leakage, the data does not transmit to unauthorized persons, but rather, disappears entirely with no means of recovery either through data corruption, malicious encryption, or deletion techniques (Kazim & Zhu, 2015). Loss conforms to the lack of availability, specifically for the information that is either missing or locked and represents a physical disruption of operations (Alassafi et al., 2017). The loss may either be a function of network-based intrusions or user-focused malware. Whereas DL is potentially malicious, is often restricted from studies which consider the theft of information of greater importance, however, an inability to access critical data could potentially present unique problems for any enterprise (Coppolino et al., 2017).

Multitenancy or shared technology – lack of isolation. A prime concern of multitenancy is the risk to data visibility across user bases in addition to a trace of operations causing an operational dependency and reliance on optimum protection across consumers of the same resources (Ali et al., 2015; Phaphoom et al., 2015; Shrivas et al., 2016). Within the scope of the cloud paradigm, data visibility is a paramount issue caused by the merging of consumers into a single platform space all of which consume the same resource stacks (Aldossary & Allen, 2016; Hussain, Fatima, Saeed, Raza, &

Shahzad, 2017; Indu, Anand, & Bhaskar, 2018). The issues arise from the relative security and service roles for authentication and access controls found in traditional cloud operations (Indu et al., 2018). Additionally, an attacker's virtual machine may coexist on the same platform as a victim's virtual machine, allowing for more significant network-based attacks, such as brute force (repeated attempts to achieve a breach), or a side channel attack that gathers information from a probe of adjoining systems (Alassafi et al., 2017; Kalaiprasath et al., 2017). The internal source, either operated by an external attacker with an internal virtual host that co-exists on the same platform space to perform side channel or brute force attacks, while probing laterally for information (Hussain et al., 2017). Insecure hypervisors, or the foundation from which virtual machines generate and implement, are also vulnerable to attack and could, therefore, allow unauthorized access to any virtual machine derived from the affected hypervisor (Farahmandian & Hoang, 2016; Kalaiprasath et al., 2017; Kaur & Singh, 2015; Kazim & Zhu, 2015). Confidential information in one virtual machine may leak to another from the lack of controlled isolation utilizing cache side attacks that draw information even across cores (Raj & Dharanipragada, 2017). A virtual machine manager, such as a hypervisor, provides attackers with a broad platform including the access to metadata regarding the virtual machines and thus, a greater number of ingress vectors (Ali et al., 2015; Islam, Manivannan, & Zeadally, 2016).

Malicious insiders. Another major threat to cloud operations are MI, defined as an employee or business partner with the cloud provider or within the network scope of the operation with access to the cloud network (Gangwar & Date, 2016; Kazim & Zhu,

2015; Shrivas, et al., 2016; Singh et al., 2016). A malicious insider may impact storage, infrastructure capacity, or software using local, authenticated access or unprivileged escalation to perform malicious tasks (Singh et al., 2016). MI are listed as the third highest priority by the Cloud Security Alliance (CSA) regarding their list of top threats and potentially could employ their access to negative consequence on capacity, escalation, or storage that in-turn affects brand, productivity, and financial losses (Mahajan & Sharma, 2015; Ramachandra, Iftikhar, & Khan, 2017). Between 2014 and 2015 the frequency of insider attacks increased according to 62% of security professionals (Noonan, 2018). The gateway to increased activity within cloud surfaces from the more prominent footprint of access controls and the complexity in management across a virtualized framework (Aldossary & Allen, 2016; Sohal, Sandhu, Sood, & Chang, 2018). While similar attacks exist within the scope of traditional operations, the shared systems and hypervisor access allow for access (unauthorized or other) across virtualized entities (Kalaiprasath et al., 2017). Insider threats emanate both from the business entity, and those requiring access to perform nominal functions, in addition to those within the cloud provider platform, thus increasing the degree of threat through a significant increase in necessary access (Ali et al., 2015).

Account hijacking. The more individuals with access, the greater the risk of AH through phishing and fraud techniques (Kalaiprasath et al., 2017; Kazim & Zhu, 2015; Suryateja, 2018). Account or service hijacking also occurs programmatically across networks and the impact to cloud is increased over traditional operations because of the shared ecosystem of the hypervisor and a lack of intrusion prevention across the

virtualized environments (Gangwar & Date, 2016; Kazim & Zhu, 2015; Phaphoom et al., 2015). Both integrity and confidentiality are impacted by AH, specifically programmatic vulnerabilities derived from operational software such as man-in-the-middle, or session attacks (Singh et al., 2016). Hijacking occurs through social engineering foundations (social engineering), programmatic (man-in-the-middle), or a combination of the two (injection of malware) to interrupt the integrity of confidentiality of information (Albadrany & Saif, 2018).

Service partner trust. Trust, within the scope of the relationship between the cloud services provider and the business entity, are essential and confer several key patterns including longevity of services, capabilities, hiring practices, platform maturity, and policies both documented and auditable (Alassafi et al., 2017; Ali et al., 2015; Balasooriya et al., 2017). When a business entity must decide to engage a third-party provider, that decision is impacted by the degree of trust between the two organizations and begins with reputation (Alkhalil et al., 2017; Jegadeeswari, Dinadayalan, & Gnanambigai, 2016). Trust encapsulates the multidimensional factors including those of humans (employed by the company and the provider), the ability to retain and analyze forensic data or provide audit compliance, the reputation of the cloud provider, the shared governance models, and any trusted third-parties employed by the business or the cloud provider (Singh et al., 2016; Wahsh & Dhillon, 2016). Certainly, the capabilities of the provider to provide transparency about hiring policies, retain forensic data, governance, and reputation are integral to the decision-making process (Sidhu & Singh, 2017). Trust moves beyond that of the relationship between provider and enterprise and therefore must

include the perceptions by the consumers that utilize the enterprise services. The consumers' degree of trust in the cloud as a technology platform that maintains their information will impact the organization (Wahsh & Dhillon, 2016).

Regulatory concerns. Relinquishing some measure of controls or sharing said responsibilities with a cloud provider incurs not merely performance assurances, but compliance with RC within the scope of the business operations markets and geographical jurisdictions (Alassafi et al., 2017; Ali et al., 2015; Brandas, Megan, & Didraga, 2015). Any enterprise that operates in a geography with specific laws governing privacy and data compliance must ensure their cloud provider is capable and experienced with such policies and is a key indicator of adoption impedance (Alkhalil et al., 2017; Phaphoom et al., 2015). All RC are operational factors that encompass data privacy laws (identifying access controls and shared resource controls) and also define rules for compliance with audit controls and physical security, thus engendering caution for those deciding upon adoption (Alkhater et al., 2018; Kaur & Singh, 2015; Klug & Xue, 2015).

Ancillary modifiers. The various threat vectors presented may alter their priority depending upon several modifying factors from an organizational perspective that examine the firm's depth and breadth as predictors to a predilection toward adoption (Jia, Guo, & Barnes, 2017).

Firm scope. A firm's scope indicates the area of responsibility or operational direction of the enterprise. A larger firm, with operations entities spanning the globe, may be more likely to adopt cloud for the rapid and geographical dispersion of hosts

within the virtualized framework (Alkhater et al., 2018; Senyo et al., 2016). Through emphasizing the horizontal extent of an enterprise's business operations, scope breaches a geographical dispersion both regarding business operations and customer bases and may find cloud as a competitive advantage, dispelling concerns over some types of security threats (Jia et al., 2017; Senyo et al., 2016).

Firm size. The term *firm size* refers to the magnitude of the enterprise and reflects the market size, capital investment capability, or employee count (Senyo et al., 2016). Larger entities are more likely to adopt a new technology because of their ability in adjusting to risk. Smaller firms, lacking the multifaceted capabilities are drawn to cloud for the cost-savings alone, thus promoting them to accept a degree of risk (Alkhater et al., 2018; Senyo et al., 2016). Large firms tend toward movement inertia, and thus are less flexible and agile than their smaller counterparts, which may indicate a hinderance toward cloud adoption (Jia et al., 2017). FS is also represented as an enterprise's degree of centralization and the complexity of its managerial structure to include the quality and availability of human resources to achieve the adoption of cloud migration efforts (Gangwar et al., 2015; Katunzi & Ndekwa, 2016).

Perceived Realities

Practitioners may address actual threat vectors, and in the security realm, do so daily. However, more difficult to derive are the perceived risks inherent in the minds of those that do not practice system integration and implementation but who do possess the authority to drive or delay new technologies. Non-experts' mental models often differ from those of experts, and their perceptions based on those models vary accordingly,

often resulting in a disconnect between the real and the imagined (Botzen, Kunreuther, & Michel-Kerjan, 2015). Narratives, real or imagined, can create perceived adversities and measure success differently, such as defining a reliable or operational system (Botzen et al., 2015). In a study by Sand and Nilsson (2017) to evaluate the power of perceived realities conceived through false priming, they determined that perceived realities drove decisions. In another study by Martin, Mortimer, and Andrews (2015), perceived risk was found to be tightly coupled to trust. Whereas the impact of the study focused on consumer services, the psychology remains valid for commercial enterprises when managed by a human. The inclination to follow the "herd mentality" is inherent in those who lack certainty and promotes decisions founded on perceptions of unmitigated security concerns and thereby prohibiting the acceptance of cloud (Haghani & Sarvi, 2017). Often these perceptions originate as a loss of control manifesting as a real threat vector, although that loss may be misunderstood and therefore invalid (Liu, Sun, Ryoo, Rizvi, & Vasilakos, 2015). Perceived realities drive decision-making and originate with a single false priming or inaccurate piece of information (Sand & Nilsson, 2017).

The value of assessing perceived risks, therefore, is important to any strategic or technology-focused goal, but that information is formless and without context. The next phase should be one of hierarchically defining pertinent values as a prioritized list, replete with contextual values assigned.

Value to Prioritizing Perceived Risk

Risk prioritization forms the foundation of risk reduction planning across the business spectrum and generally takes into consideration both hazards and potential

consequences permitting an educated decision-making process (Thokala et al., 2016). The value of categorizing, analyzing, and prioritizing risk is not a new concept, having been previously employed for a study on evaluating risks in a hierarchical matrix toward the adoption of ERP systems (Huang, Chang, Li, & Lin, 2004). The framework proposed by the study determined the actual risks and inform their prioritization on the perception of decision-makers to focus their attention on a resolution to achieve adoption (Huang et al., 2004). More recently, Euchner and Ganguly (2014) propose that to drive innovation, several key steps in that process are the assessment and prioritization of risks to focus on those that presented the largest concerns more immediately. Perceived risk reduction was the foremost response when decision-makers responded to an inquiry to rate the top drivers of security investment, and immediately following, an analysis of how prioritization helps decide upon which programs or policies enact more quickly than others (Kucukaltan, Irani, & Aktas, 2016). Upham, Oltra, and Boso (2015) found that risk perception is an important variable to consider when determining the social acceptance of new energy technologies. The same theory would exist for acceptance of any new technology, such as cloud computing, thus permitting practitioners the opportunity to devise or construct mitigations and drive understanding amongst executive decision-makers with a defined strategy for adoption (Tweneboah-Koduah et al., 2014). Kucukaltan et al. (2016) found in their study that regarding decision-makers, reducing perceived risk received a top-tier driver of security investment followed closely by how prioritization enables rapid decision-making according to policy interpretation.

Establishing a litany of threats and determining through perception and prioritization those that require more immediate attention will provide an avenue for practitioners to migrate into the cloud. However, other factors require consideration, such as how to best utilize the space and enhance the social consciousness of the operation.

Theoretical Framework

The TOE framework, originally developed by Tornatzky and Fleischer (1990), as an extension to the TAM, is the process by which context influences the adoption and implementation of technological innovation at the organizational level. The foundation of the TOE are the three distinct contexts (i.e., technological, organizational, and environmental) that provide influencers regarding the adoption of innovative technology (Tornatzky & Fleischer, 1990; Klug & Xue, 2015). The three contexts provide the inclusion of varied perspectives from which conclusions regarding the adoption of technology originate, thus providing a more holistic view than relying on a singular approach, while offering malleable and dynamic containers of influence (Tornatzky & Fleischer, 1990).

Technological, organizational, and environmental. In the following sections, I provide rationale as to the factors motivating me to opt for the TOE, followed by an explanation of alternatives and reasons for eliminating them as options for my study. The three-tiered approach of the TOE presents three distinct contexts derived from varying perspectives from which one will draw conclusions regarding the adoption of new technologies: technological, organizational, and environmental. The contexts apply to

organizational-level theory to explain, in malleable and dynamic terms, the influence each imparts to a technology adoption decision (Tornatzky & Fleischer, 1990). The TOE encapsulates, within its contextual model, internal and external technologies that are influential for the business to include current and future technology practices (Martins, Oliveira, & Thomas, 2016). The organizational context specifically refers to factors such as scope and size to describe the firm, while the environmental context defines the limitations and opportunities that may impact the decision process such as regulatory measures (Martins, Oliveira, & Thomas, 2016). Originally developed as an extension to the TAM, it adopted some of the technology attributes common to the diffusion of innovation (DOI) framework, encapsulating perceptions of specific factors that influence adoption (Hsu & Lin, 2016; Lal & Bharadwaj, 2016). Lal and Bharadwaj (2016) further noted that support from top management is essential for success as they establish the climate, specifically for adoption of cloud services. The TOE is advantageous compared to competing models because of the inclusion of multiple contextual ingress variables that are each individually accounted for in alternate methods thus proving a holistic view for adoption from a perspective of implementation, challenges, and the impact on operations (Gangwar et al., 2015). Senyo et al., (2016) applied the TOE methodology to their study on critical factors inhibiting cloud adoption in developing countries. Klug and Xue (2015) also applied the TOE toward a study focusing on cloud adoption within universities. Hsu and Lin (2016) promoted dissecting security implications in a further study from their work that also utilized the TOE to examine adoption influencers for cloud computing technologies. Security is discovered as the prime demotivating factor in

another TOE-based study for adopting cloud resources and suggest that decision makers lack appropriate information or knowledge to make informed choices without proper extrapolation by practitioners (Alkhalil et al., 2017). The model targets correlative relationships between contextual constructs and an organization's willingness to adopt new and innovative technology, while each of the three contexts represent constraints and opportunities (Lippert & Govindarajulu, 2006; Tornatzky & Fleischer, 1990).

Technological. The technological context focuses entirely on technologies and their impacting factors (Tornatzky & Fleischer, 1990). The technological context includes all relevant technologies and technologically impacting characteristics (Chiu, Chen, S., & Chen, C.L., 2017). As Gangwar et al., (2015) and Klug and Xue (2015) noted in their studies on cloud adoption utilizing the TOE framework, extant literature provides for three variables within the technological construct: relative advantage, compatibility, and complexity. Awa, Ukoha, and Emecheta (2016) extended the three foundational areas into five functional constructs, dissecting complexity into knowledge, security, and infrastructure, while retaining the remaining two but allowing for perceptional influencers. Hsu and Lin (2016) stated that perceived security integrates into perceived attributes within the innovation diffusion theory (IDT) which can be considered attributes of the technological context within the TOE. Senyo et al. (2016) also defined security parameters for influencing adoption of cloud within the technological construct of the TOE. The challenges and complexities inherent in the new technology are indicated by the technological context, which for this study are represented by three different security-focused threat vectors, namely ST, AH, and DP.

The relative advantages of cloud adoption are prolific across the extant literature and would serve no additional purpose for this study and as such, will be removed.

Shared technologies. From a technological perspective, ST or multitenancy involves the side-channel or adjoined systems concerns relative to coexistence within the same architecture (Alassafi et al., 2017). Access controls relative to cross-platform access contained the same resource stack is also a technological concern (Aldossary et al., 2016; Hussain et al., 2017). Data visibility in this context pertains to the lack of isolation between operating resource platforms (Ali et al., 2015; Shrivas et al., 2016). Examples provided by Raj et al. (2017) and Islam et al. (2016) also include virtual machine management functionality as a common metadata ingress vector.

Account hijacking. A function of a shared ecosystem involves the access by a greater number of individuals as opposed to the narrow field often accompanying a traditionally hosted environment, thus increasing the risk to illicit access via fraudulent techniques (Kazim et al., 2015; Suryateja, 2018). Session attacks or other programmatic vulnerabilities impact the sanctity of operating platforms if an account is consumed across a common virtual machine (Albadrany et al., 2018; Gangwar et al., 2016).

Data protection. The term *data protection*, which to consolidate similar variables includes data loss, involves the alteration or deletion of important data which does not involve the transmittal of said information (Kazim et al., 2015; Alassafi et al., 2017; Warth et al., 2017). Loss may also include the programmatic and malicious encryption of data by an unknown threat actor operating across the platform space (Alassafi et al., 2017).

Organizational. Organizational context focuses on the internal organization and its characteristics such as organizational structure, such as firm size and scope (Lippert & Govindarajulu, 2006; Tornatzky & Fleischer, 1990; Chiu et al., 2017). Several key studies investigate as ancillary correlative information the impact of firm size and scope on adoption. Alkhalil et al. (2017) provided detailed analysis of size as a juxtaposition of scope increases or decreases the demand for innovation (specifically cloud adoption) based ion parameters such as assumption of risk, capital investment and the direction relationship between greater adoption and broader scope. Awa et al. (2016) noted the size of the firm is an imperative factor within the organization context, then divide scope across more defined variations; scope of business operations, demographics, and subjective norms. Senyo et al. (2016) added top management support and technological readiness in addition to firm scope and size as indicators of influence, while Klug and Xue (2015) combined such factors into a single perceived barriers construct. Additional constructs such as readiness and management support are unnecessary for this study, as the participant pool will consist only of top management decision-makers in an effort to derive their perceptions on the security variables while focus on the security aspects eliminates the requirement to derive organizational readiness. As noted by Lal and Bharadwaj (2016) support from top management is a necessity for successful introduction of cloud services as they establish the technological landscape via capital investment. Therefore, further justification for the elimination of management support from the organizational context as only executive management will participate and clearly if they opt to invest, they provide support.

Firm size. Within the confines of the organizational aspect of the TOE, the extant literature abundantly provides for the variable for FS, defined as the magnitude of the enterprise (Senyo et al., 2016). The size is a representation of the enterprises' degree of centralization and complexity of managerial structure as it relates to the adoption of new technologies, and therefore a useful consideration as a modifier in any TOE framework (Amron, Ibrahim, & Chuprat, 2017).

Firm scope. The SC defines the operation direction of an enterprise and implies both a geographical dispersion and areas of responsibility (Alkhater et al., 2018). Ray (2018) noted that scope is widely accepted as a standard variable within the TOE's organizational context and may be useful in determining the degree of risk acceptance within an organization.

Environmental. The environmental context assesses the firm's ability to access, utilize and trust external resources such as technology service providers, concern for MI, DL, and the impact of regulation (Lippert & Govindarajulu, 2006; Tornatzky & Fleischer, 1990; Wahsh & Dhillon, 2016). Awa et al. (2016) considered environmental contexts to include operational facilitators and inhibitors, which encapsulate support infrastructures, the notation of which confers the addition of insiders and cross communication (leakage). Klug and Xue (2015) limited their model structure to regulatory policy and service provider support, however, such support implies a measure of trust, both in the capabilities and management the provider offers to the environment. Lal and Bharadwaj (2016) indicated that from an environmental perspective, the trust in the service partner (vendor credibility) encapsulates the concerns regarding all aspects of

provider servicing. Other aspects often included in the environmental context is the intensity of the competition, the impact on the perception of adoption, and the interest of rapidly generating opportunities (Hsu & Lin, 2016). However, as this study is not interested in alternative impediments to adoption, instead focusing entirely on security, it is not necessary to gauge the impact of competition to garner a hierarchical perceived threat vector matrix. When considering the adoption of new technological innovations, various dimensions exist which restrict or invest the opportunity for the key decision-makers, such as the nature, the complexity, the motivation, and the timing of the innovation (Hoti, 2015). Respectively, they form the following characteristics: process as opposed to product, radical versus an incremental change, a technological push or a market pull, and planned versus incidental (Hoti, 2015). The consumption, therefore, must traverse and encapsulate all the various dimensions of influence to confer any intent to adopt and are thusly incorporated into the TOE framework (Hoti, 2015).

*Malicious insiders***.** As an environmental context, malicious insiders represent the employees, for the business, the provider, and the network partner as potential exploitative vectors (Gangwar et al., 2016; Shrivas et al., 2016). The addition of the service partner and the network provider exponentially increase the risk value and are considered the third largest security risk priority by the CSA (Mahajan et al., 2015; Ramachandra et al., 2017). The introduction of the cloud operations environment from a technological perspective confers the environmental aspects of wider participation in defines management access within the framework (Aldossary et al., 2016, Sohal et al., 2018).

Data leakage. The term *data leakage* is defined as an environmental consideration as it is grossly impacted by active sniffing across the network segment (Ali et al., 2015). The addition of excessive network pathways for access, management, and reporting involved with a cloud architecture expand the possibility of illicit acquisition of data streams (Cayirci et al., 2016).

*Service partner trust***.** More so than in traditional hosting environments, SP within the cloud landscape involve greater relative interaction, such as auditing policies, hiring practices, longevity, and maturity of service architecture (Alassafi et al., 2017; Balasooriya et al., 2017; Jegadeeswari et al., 2016). Trust in the environmental context involves the multidimensional factors facing humans and shared governance models in addition to the ancillary degrees of trust the service provider endows upon their partners that impact the business (Sidhu et al., 2017l Singh et al., 2016).

Regulatory concerns. Another common theme across all the reviewed literature pertaining to the TOE framework is the inclusion of regulatory concerns as an environmental factor, as some controls must be shared or relinquished to the provider and therefore must be geographically aware (Alassafi et al., 2017; Brandas et al., 2015; Ray, 2016).

Alternative theories. There are several competing and supporting theories that researchers utilize to study technology adoption. I provided details regarding several of these competing theories and justify their negation as an operative framework.

Theory of reasoned action (TRA). According to Ajzen and Fishbein (1980), a measure of behavioral intention will predict the outcome of a decision provided said

intention measurement corresponds the specificities of the action. While the TRA as theoretical construct focuses on the individual motivational factors, it assumes that attitude and intention are the best predictors of a specific behavior (Montano & Kasprzyk, 2015). Intentions are indicators of the level of effort expended toward a certain behavior as it tends toward the subjective norm, which itself is defined as a perception regarding the degree of pressure to execute the specific behavior (Kim, Lee, & Yoon, 2015; Sheldon, 2016). Attitude in this case, refers to the degree of positive or negative appraisal for the specific behavior (Kim et al., 2015; Sheldon, 2016). The two primary indicators for TRA are attitude toward behavior and social normative perceptions and the central tenet is the individuals' intent to engage in a specific behavior (Paul, Modi, & Patel, 2016).

One of the key issues with using TRA is the assumption that determinants of behavior is intention which is limited to those items under volitional control (Montano & Kasprzyk, 2015; Paul et al., 2016). Additionally, subsequent studies have shown the reliance on social norms as an indicator is weak (Lai, 2017). The TRA limits the ingress of nominal dimensions to attitude, directed both as determinants of beneficial qualities and social norms (Kim et al., 2015; Sheldon, 2016). Moreover, the TRA possesses limitation in predicting future usage behavior (Tarhini, Arachchilage, & Abbasi, 2015). As such, these were not sufficient to encapsulate the complexities of the various threats and determine the exact nature of influence from each of the contexts as opposed to a belief in a particular technology.

Theory of planned behavior (TPB). The TPB is an extension to the TRA, adding an additional construct for the non-volitional determinants in intention, that is, it incorporates perceive control over the behavior thusly including scenarios wherein one may not have complete control over said behavior (Montano & Kasprzyk, 2015; Paul et al., 2016). Therefore, it contains three cognitive antecedents: an individual's attitude toward the behavior, the subjective norm that incorporate the social group mindset toward a particular behavior, and perceived behavior control that denotes the ease (or lack thereof) to implementing or performing said behavior (Kautonen, van Gelderen, & Fink, 2015). Within the TPB, the primary determinant of a specific behavior is intention, which is then influenced by subjective norms and perceived behavioral control (Steinmetz, Knappstein, Ajzen, Schmidt, & Kabst, 2016).

However, criticisms regarding the TPB are considerable surrounding the adequacy of the theory in predicting certain behaviors, or the static nature of the model, not considering future behaviors subsequent to periodic and perhaps critical updates (Rich, Brandes, Mullan, & Hagger, 2015). Strongest of the criticisms perhaps is the intention-behavior gap, wherein a person fails to conform with their intentions, thus proving it is superior at indicating intention, but not behavior (Rich et al., 2015). The intent for my study was to examine what if any degree of influence on behavior each of the security variables possesses and the individual impact on adoption and will provide clarity for practitioners to engender cognitive change. Therefore, my study is not aligned with the TPB.

Technology acceptance model (TAM). Davis (1989) proposed TAM as an extension to the TRA, to investigate two critical factors to adoption; perceived usefulness and perceived ease of use and noted them as the most important aspects of influence of behavioral intention. The usefulness factor stipulates the extent that an individual within the organization believes that a certain technology will enhance their work effort, while perceived ease of use denotes a minimal effort to employ and operate said technology (Lal & Bharadwaj, 2016). Davis (1989) argued that perceived usefulness and ease of use mitigated any effect of external variables on behavioral intention, omitting subjective norm form the original version. TAM as a framework, is widely accepted and utilized in the study of adoption for technology innovation (Awa et al., 2016; Yeou, 2016; Yoon, 2016). The perceived usefulness and ease of use variables are often conjoined with externalized factors which attempt to explain the variations in observation of perceived usefulness and ease of use to include: subjective norms, self-efficacy, and facilitating conditions, though applied different and to varied degrees (Scherer, Siddiq, & Tondeur, 2019). Extensions to the TAM, such as TAM2 and TAM3 include cognitive instrumental processes and social influencers as constructs to describe acceptance over time and influencers of subjective norms and adjustment detectors (Sharma, 2017; Sharifzadeh, Damalas, Abdollahzadeh, & Ahmadi-Gorgi, 2017).

The TAM, however, omits external variables such as demographics and economics of scale (derived from the firm scope and size) to describe adoption intentions and present a weak theoretical association between acceptance and commitment (Scherer et al., 2019). TAM has been criticized for its limited explanatory and predictive power

(accounting for only 50%), as well as a lack of practical values because of limited predictors (Lim, 2018; Chauhan & Jaiswal, 2016). Additionally, factors such as usefulness and ease of use are not viable as it is a generalized expectation of new technology (Hwang, Chung, & Shin, 2018). The latter are assumed from the extant literature to be prevalent within and without the participant pool demographic, and therefore unnecessary to investigate further, thus TAM was not a choice that aligned with my study.

Diffusion of innovation (DOI). Rogers (2003) developed the diffusion of innovation theory to explain how information flows from one to another within a social system. DOI contains four main determinants of success for the innovative process: communication channels, innovation attributes, the adopters' characteristics, and the social system (Zhang, Yu, Yan, & Spil, 2015). The attributes of the innovation are realized in five perceived qualities: relative advantage, compatibility, ease of use, observability, and trialability (Emani et al., 2018; Zhang et al., 2015). Relative advantage indicates an evaluation of greater benefit for adoption, while compatibility examines the consistency of service with the core beliefs of the constituency (Min, So, & Jeong, 2018). Complexity or ease of use describes the functionality and the degree of cognizance it requires to fully understand and implement (Kiwanuka, 2015). Observability and trialability focus on how visible the innovation or the results of the innovation are upon the user population and trialability indicates the social acceptance or the ability for the system to be broadly accepted without commitment or investment (Zhang et al., 2015). Rogers (2003) concluded that the structure of the social system contributes to an

individual's attitude regarding the innovation and thereby impacting the adoption of said innovation. Zanello, Fu, Mohnen, and Ventresca (2016) utilized the DOI theory to examine the creation and diffusion of innovations in developing nations, utilizing each of the five factors while noting the social aspect of the study but does not seek to investigate non-social factors. Min et al. (2018) applied the diffusion of innovation theory in conjunction with the TAM to discern social processes that initiates and spreads innovation as the five factors that encapsulate the DOI are not indicators of social factors. Rogers (2003) pointed out that a person may reject an innovative concept because they lack adequate knowledge regarding the specifics of the innovation. While this may seem to align with the perceived issues concept raised in this study, it is not intended to derive the catalyst for rejection, but rather identify those areas of the greatest (and subsequently, least) concern. The results then may be employed by the practitioners to educate or mitigate those concerns.

The DOI, while providing adequate investigatory factors into the determinants of innovation, it does not examine specifically the characteristics beyond those of relative advantage, ease of use, compatibility, trialability, and observability (Emani et al., 2018). Two of these factors (Ease of use and relative advantage) are adequately proven in extant literature, and compatibility is not a necessary investigatory data point. Trialability relies too heavily on social acceptance, which provides more rationale for adoption than against, and as this study is intended to determine security concerns prohibiting adoption, it was also unnecessary. The DOI is focused on defining innovation adoption via social constructs (Larosiliere, Carter, & Meske, 2017; Rakic, Novakovic, Stevic, & Niskanovic,

2018). The foundational perceptions of cloud security concerns impeding adoption are not, as the literature shows, a social construct, but rather a technological and environmental one.

Unified technology acceptance and use technology model, extended (UTAUT). The UTAUT (and subsequent extensions, such as UTAUT2) consists of four core constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions (Williams, Rana, & Dwivedi, 2015). It was formed as a synthesis of propositions from prior models including TAM, TRA, TPB, and DOI (Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2017; Venkatesh, Morris, Davis, G.B., & Davis, F.D, 2003). Each of the four constructs examines perceived influencing variables. Performance expectancy directly relates to the derived benefits while executing activities, while effort expectancy associates to the degree of ease in which the innovation is implemented (Dwivedi et al., 2017). Social influence is the degree to which an individual in a position to accept the innovation perceives how others (customers or peers) believe in the new system (Venkatesh et al., 2003). The degree to which an individual believes their infrastructure may support such a system is the context of facilitating conditions (Dwivedi et al., 2017). Hoque and Sorwar (2017) utilized the UTAUT model to examine the factors that influence the elderly in their decision to adopt mobile health services, however, felt necessary to expand the variable set to include alternate factors, such as technology anxiety and resistance to change. Tarhini, El-Masri, Ali, and Serrano (2016) also extended the UTAUT model to include specific factors as

they relate to their study investigating factors debilitating the adoption rate of Internet banking in Lebanon.

However, as Busse, Kach, and Wagner (2017) note, extending arbitrarily contexts within theories could potentially damage accuracy if relevant generalizability is not maintained. A study by Williams et al. (2015) on the efficacy of UTAUT as a methodology found that the collative predictive power of each independent variable was not consistent, save for two: performance expectancy and behavioral intention. A key point is that UTAUT focuses on intention, as opposed to actual behavior and does not delve into the correlational relationships between the impacting factors as a bridge between intention and consumption and is therefore, limited in its usefulness toward explaining which single interventions impact acceptance (Fadzil, Nasir Syed Mohamad, Hassan, Hamid, & Zainudin, 2019). Performance efficacy relates directly to the expected results, and as noted in the extant literature, performance, side from security implications is already noted as understood and available. The remaining variables are also unnecessary as there are not social constructs regarding the security of a service, aside from the widely held misperceptions, which are not the intent of this study, but rather provide practitioners with a path to acceptance.

Gaps in the Literature / Relationship to Prior Research

Prior studies focusing on the adoption rates for cloud technologies targeted security as a single construct, establishing the entirety of the security paradigm as cause for the lack of cloud adoption utilizing the TOE theory (Alkhalil et al., 2017; Hsu et al., 2016). Al-Hujran, Al-Lozi, Al-Debei, and Maqableh (2018) applied the TOE framework

to discover the factors preventing adoption within Jordan and found that security-related issues including privacy and trust were the primary impediments. While the latter divests privacy and SP into distinct categories, it does not identify the individual components within the over-arching security term and the former consolidates all security aspects into a single entity. Senarathna, Wilkin, Warren, Teoh, and Salzman (2018) similarly divided the technological security barriers to the technology aspect of the construct, while including regulatory measures and service providers into the environmental focus of the TOE, and while their relationship between security and adoption was deemed limited, their method was designed to limit reporting on the positive aspects of assimilation as opposed to the negatively impacting factors within their survey instrument.

Fu, Chang, Chang, and Liu (2016) investigated factors that influence or deter adoption of cloud utilizing the TOE method per key decision-makers, dividing the concept of security into data access security, information transmission security, and management security within the technological aspect, while including regulatory compliance in environmental and SC, FS, and SP within the organizational component. Fu et al. (2016) noted the primary impedance toward new adoption were the security aspects rated highest among the negatively impacting factors followed by the environmental considerations immediately following.

The gap noted and filled by Senyo et al (2016) referring to the dearth of security-inclusive studies investigating the limited cloud adoption among enterprises within their TOE framework, suggests a new gap; one that investigates the specifics of the security-related components. The largest contributor to negative adoption across a landscape of

business operations from the perspective of decision-makers within the study focused on the security-related factors contained in the technological context, while FS and SC (both within the organizational aspect) provided no significant results, they were investigating these factors as individually contributing to adoption.

Security and privacy were the top-rated concerns among decision-making executives impeding the adoption of cloud computing in a TOE framework study wherein each were defined (loosely) as protection from unauthorized access and confidentiality of personal information (Sohaib, Naderpour, Hussain, & Martinez, 2019). Encapsulated within the technology aspect, Sohaib et al. (2019) included both security and privacy, albeit as a single entity, while defining SC and FS within the organizational context and again, RC within environmental.

Amron, Ibrahim, and Chuprat (2017) reviewed prior works to determine the most impacting factors toward adoption across a variety of enterprise types: health, education, and public sector businesses. The study found the factors that impeded the adoption rate the greatest across all three sectors included security, privacy, RC, and SP concerns (Amron et al., 2017). Ray (2016) also reviewed more than 14 prior works utilizing the TOE framework to derive a consolidated approach in the application of the TOE and an aggregated view of the result set. The largest contributing factors included security (which included data privacy) and RC, however it also does not delve into the specifics of security as a construct.

The aggregated references all denote security and regulatory concerns among the chief impediments to adoption of cloud computing. While cloud offers greater cost

savings (Alkhalil et al., 2017; Balasooriya et al., 2017; Fan et al., 2015; Oliveira et al., 2014; Rathi et al., 2017) and is well established as a simple technology to execute (Lo et al., 2015; Nayar et al., 2018; Phaphoom et al., 2015; Senyo et al., 2016) enterprises remain reluctant to adopt given the perceived risks involved from a security perspective (Fu et al., 2016; Senarathna et al., 2018; Sohaib et al., 2019). My study intended to dissect the use of "security" as a consolidated moniker into the various components of perceived risk. Understanding the impact of each security parameter will allow practitioners to resolve, explain, or otherwise mitigate these factors toward greater adoption rates for cloud computing initiatives and facilitate the transformation of operating services toward lower cost and greater access capabilities. The gap identified in prior works fails to adequately identify those patterns of security implications and hierarchically define the prioritization of risk perception and my intent was to contribute to filling this gap.

Transition and Summary

Addressed within the analysis of research contained herein exists value in accessing, analyzing, and hierarchically prioritizing threat vectors for cloud operations, offering the advantages of understanding the perceived realities decision-makers employ when opting for cloud adoption. Understanding the propensity for human beings to utilize their perceptions as bias indicators for decision making, and upon recognizing that fact, working to mitigate negative factors is essential. Deriving a hierarchical list of proposed threats applicable to those that are key executives in the decision-making

process will permit practitioners insight into how to address those of greatest concern, thus potentially enabling greater adoption rates. Should the development of a hierarchical structure for perceived threats drive adoption, the benefit to nonprofit and not-for-profit organizations (in addition to business enterprises) will help drive social change in the wider scope of capabilities provided and a reduction in carbon emissions.

The actual derived benefit from the perspective of the practitioner/decision-maker symbiosis is unknown, and as such, this study would act as a catalyst to provide practitioners with the tools necessary to spawn mitigations for those preconceived risks held by key decision makers.

The first section introduces the topic of cloud computing and the associated dearth of adoption, despite the presumed benefits such as cost and ease of use. The section also relates the purpose of the study; to determine if and to what degree, a relationship exists between various security concerns such as shared technology ST, MI, AH, DL, DP, SP, RC, FS, and SC with key decision makers' intention to adopt cloud computing. The application of the TOE theoretical framework provides a malleable approach to contextual information that examines how the independent variables relate to the dependent variable. The literature review provides context for the various patterns of influence within the security focus, the value of perception, the promotion of risk analysis, in addition to defining the TOE and how each apply to the study parameters.

In section 2, I restate the purpose of the study, define my role as the researcher, describe the participants, and justify the use of a quantitative method and correlative design. I discuss the population and sampling methods, and provide details on ethical

study execution, and provide details on instrumentation. Finally, data collection methods and techniques, analysis, and discussion on study validity completes the second section. Section 3 presents the findings (stating the test procedures and how they relate to the hypotheses and all relevant statistics. In addition to the findings, section 3 will also present the application to professional practice, implications for social change, and recommendations for future actions and research.

Section 2: The Project

In the following section, I provide more detailed information on the research models, methods, designs, and execution for the purpose of the study. Aside from restating the purpose, I explain my role as the researcher in this quantitative study, discuss the means and requirements for the selection and execution of participant identification, describe the population sampling, and establish criteria to ensure ethical research. Subsequently, I explain the data collection methods, the organizational attributes and analysis mechanisms, and provide a statement about the reliability and validity of the study.

Purpose Statement

The purpose of this quantitative correlational study was to evaluate the relationship between the independent variables consisting of ST, MI, AH, DL, DP, SP, RC, SC, FS, and the dependent variable intention to adopt public cloud infrastructures. The specific population group will be CIOs and IT directors from large and small enterprises within the United States. A potential element of positive social change this study may contribute to is the enhancement of service capability for consumers of non-profit organizations (NPO) through implementation of enterprise-class services and a lowered total cost of ownership (TCO).

Role of the Researcher

From an epistemological approach, quantitative perspectives explain through analysis the observation or manipulation of variables and the relationship between them

using empirical means, whereas a qualitative focus is one of interpretivism, analyzing the experiences of people as they interact with one another and broader social systems that include the researcher (Antwi & Hamza, 2015). Quantitative methods permit relative objectivity while increasing efficiency through the comparison of statistics versus a more narrow and subjective style utilizing qualitative methods (McCusker & Gunaydin, 2015). In addition, qualitative methods lack a hypothesis at the onset, instead developing one during the initial stages of research indicates the potential for a lacking insight or objectives (McCusker & Gunaydin, 2015). However, contextual information regarding the interactions are lost within the purely objective and statistical analyses employed by quantitative methods, thus relying on the knowledge of the researcher to define conditions under a given hypothesis. Qualitative approaches describe phenomenon for that which little is known (Antwi & Hamza, 2015; Yin, 2014).

Despite common knowledge of the great financial advantages, ease of use, and availability benefits within the cloud landscape, enterprises remain fixated on security and privacy threats that border on a lack of technical knowledge and a lack of empirical evidence identifying the important issues to those in a position to decide on adoption (El-Gazzar et al., 2016). In my more than 25 years of experience in the field, I have obtained formal and informal education on the subjects of both security and cloud computing. I was part of an architecture team that first developed the concept of migratory workloads and automated workload development; a precursor to Platform as-a Service (PaaS) and Infrastructure as-a Service (IaaS), as well as DevOps approaches. Part of my initial responsibilities as chief architect I developed a sustainable infrastructure that remains

active, even under cataclysmic activity, which includes approaches to secured deployment. Prior to this engagement, I worked for the Department of Defense as a security engineer and what is now termed, penetration tester while also developing security policies still in use by the Department of Defense.

In conducting this research, I adhered to the principles of the Belmont Report. The purpose of the Belmont Report is an attempt to summarize the basic ethical principles identified by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, created as a function within the National Research Act (Pub. L. 93-348), signed into law in 1974 (Health and Human Services, 2016). The term "basic ethical principles" refers to three foundational aspects: respect for persons, beneficence, and justice. The first entitles persons with diminished autonomy to protections, and reflects that everyone is an autonomous agent, whereas the second principle ensures respect for decisions and protection from harm for all participants (Health and Human Services, 2016). The last ensures an even distribution of both burdens and benefits, in terms of research, to assure no disparity among the population for the problem under study (Health and Human Services, 2016). Though clearly focused on the imperfections within the field of medicine and biomedical engineering, several key tenets follow for any research, such as the ethics of preventing harm to participants and safeguarding their decisions. However, there is concern regarding transparency, given the evolution of approaches to research, the composition of review boards, and limitation of controls founding in the original report to compensate for new technologies (Friesen, Kearns, Redman, & Caplan, 2017), for example, the broad consent allowable under the

original report as opposed to informed consent of the individual (Friesen et al., 2017). For these reasons, my intent was to limit the quantity of personal information, as it will not require great specificity, and to inform each individual of the necessity to confirm consent through the submission of the survey instrument.

Participants

The participant pool from which this study derived its analysis includes CIOs and IT directors with the authority to decide on adoption of cloud within large and small enterprises in the United States that do not currently but have considered employing public cloud for public offerings and interactivity. Any key decision-maker from a corporation or nonprofit entity would have sufficed, but the respondents must be in a clear position to decide for the entire organization on the adoption of cloud. The research utilized a survey instrument to collect data and within that data set, a single criterion upon which the selection inquired as to the subject's capability as decision-maker within their organization to ensure validity. Moreover, the invitation email requesting participation stipulates the requirement as decision-maker for the organization (see Appendix B). The sample area must be large enough to accommodate the lack of entities at each operation; presumably there is a limitation of a single individual in each that decides on the adoption of cloud, hence the entire United States as a resource pool. As McCusker and Gunaydin (2015) emphasize, it is more often the lack of specific knowledge or preconceived ideas about a particular subject that cause the decisions to sway as opposed to any true technical explanation. Therefore, it is imperative to obtain the potentially biased results from those in a position to impede the greater adoption of cloud. Furthermore, Cycyota

and Harrison (2002) stated that executive roles are key informants for strategic processes, such as resource planning and structural alignment. Cobb (2016) suggested that executive decision-making relies on both organizational (internal) focus and market strategies (external) to reduce risks and enhance capabilities.

I used LinkedIn Professional and personal contacts to find the email addresses of people in a, IT director or CIO role. I then emailed individuals in these roles and specified the intent for only those with the authority and responsibility to decide future technology direction to respond. The study presents a difficulty apart from other similar works, in that the participants must be executives or directors within their respective organizations. Cycyota and Harrison (2002) in their seminal work on enhancing the responses from executives, noted that executive respondents are necessary to provide the appropriate data toward a firm-scope hypothesis and to test broad conceptual frameworks. Furthermore, the acquisition of responses does not benefit from established theories that focus on practitioners or users, and the means to ensure success within the executive level detours from the seemingly universal approach and must be interesting, relevant, and efficient in design (Baruch & Holtom, 2008; Cycyota & Harrison, 2002).

There must exist a degree of trust not merely between the researcher and the participants, but between the participants and the organizational institution from which the researcher operates (Guillemin et al., 2018). The foundation of a successful working relationship is trust (Boies, Fiset, & Gill, 2015). As Guillemin et al. (2018) stated, it is important not to underestimate the value of trust realized between participants and educational institutions, aligning with such an organization implies a degree of

transparency and regulatory measures for both quality research and ethical procedures. I emphasized the purpose of the study as an educational exercise within the scope of a higher learning organization that already maintains a high standard of ethical considerations is a primary method of establishing a positive working relationship with each participant. Additionally, a statement of consent prefaced the link to the survey tool, establishing a trust contract between myself, the institution, and the participants, thus broadening the degree of trust and improving the already established relationship. Such examples of ethical practice evinced by higher learning institutions include the protection of identity and assurances that participation is voluntary allowing for withdrawal at the participants' discretion (Whicher et al., 2015).

The focus of attaining participants with a position of authority over decision-making for the enterprise aligns with the scope of the study: to discover which security-related considerations relate to the decision on adoption of cloud and to categorize in a hierarchical fashion the factors to establish a means for practitioners to develop strategies to compensate and mitigate.

Research Method and Design

I conducted a quantitative correlational study to discern the relationship between those in a decision-making capacity to adopt cloud computing architectures and the main contributing factors to security risks. The effort is twofold: (a) to discover what, if any, relationship exists between the decision-maker as the dependent variable and the various threat landscapes as the independent variables, and (b), to hierarchically define those of greater impact for practitioners to prioritize mitigation. Whereas qualitative research

seeks to understand the “what”, “how”, or “why” of a phenomenon and risks the biases of the researcher as an active participant, quantitative focuses on the “how much” or “how many” to infer a numerically significant response from quality raw data (McCusker & Gunaydin, 2015). Furthermore, McCusker and Gunaydin (2015) noted that explaining observations consisting of previously informed topics by the researcher in an objective fashion that adequately tests hypotheses, are the primary features of quantitative research. Conversely, in qualitative research, a relationship exists between the researcher and research participant as the former is an active participant in the research and the potential outcomes are relatively unknown, thus answering questions regarding experiences and normative behavior (Hammarberg et al, 2016; O’Grady, 2016). When the requirements exist to identify then quantify via integration consisting of the benefits for both methodologies, mixed methods provide an avenue to describe data in at least four ways; the explanation of quantitative results qualitatively, embedding one within another, the merger of the two result sets, or building from qualitative results a quantitative instrument (Guetterman, Fetters, & Creswell, 2015).

Method

The method most appropriate for my analysis is a quantitative study. Quantitative studies involve the empirical and systematic analysis of phenomena and the associated relationships via numerical data derived from observation expressed through mathematical expression (Basias & Pollalis, 2018). Each research paradigm is intrinsically linked with three distinct dimensions of thought regarding the relationship between practice and thinking that define the foundation of enquiry: ontological,

epistemological, and methodological (Antwi & Hamza, 2015). Within the scope of ontology, or considerations of the form and nature of reality, exist two distinct and converse positions of an independent reality (objectivism) and that reality is manufactured via social process (constructionism), whereas epistemology targets the relationship between the researcher and the research also consisting of two paradigms: positivism and interpretivism - constructivism (Antwi & Hamza, 2015). When approaching a methodology, it is vital to interpret the foundation of the research and the terms of interaction between the framework and the researcher in addition to these philosophical orientations or research paradigms (Abutabenjeh & Jaradat, 2018). The characteristics of the paradigms align (ontologically and epistemically) with certain research methods. For example, the scientific paradigm positivism assumes a single, objective reality with a detached impartiality while post-positivism, based on positivism, explains the complexity of human behavior as it contends with the absolutes, though drives toward the utmost in objectivity and impartiality and therefore aligns to the quantitative methodology (Davies & Fisher, 2018). Data collection and repeatable processes are key attributes of quantitative research methods (Groeneveld, Tummers, Bronkhorst, Ashikali, & Van Thiel, 2015; Munn, 2016). In addition, the research question within the proposed study informs the methodology; focusing on "how much" or "to what degree" a set of variables impacts another signifies a quantitative approach (Hales et al., 2016; McCusker & Gunaydin, 2015).

The intent of my study was to objectively and impartially examine through empirical means the relationship between security-related variables as impediments to

adoption of cloud services and the decision-makers who ultimately have the responsibility to pursue these innovative technologies. A primary goal during the data collection and analysis process is repeatability in design and function and to define "to what degree" each factor is a perceived impediment to adoption.

I did not intend to utilize the qualitative method for my study. The qualitative method, that involves interpreting realities with socially constructed knowledge, more strongly associates with behavioral methodologies (Abutabenjeh & Jaradat, 2018; Davies & Fisher, 2018). Qualitative research investigates phenomena using behavior and relations interpreted by the researcher (Basias & Pollalis, 2018). Should the research question in the proposed study inform the methodology toward a "how' or "why" query, thus offering insight into understanding, it would confer a qualitative methodology (Hales et al., 2016; McCusker & Gunaydin, 2015). Active listening provides insights to the researcher regarding the subject matter in qualitative constructs (Groeneveld et al., 2015; Munn, 2016). My study parameters did not include social constructs nor how these items are impacting. The factors have been drawn from extant literature as demotivating variables and the intent is not to determine why they are considered impacting, but instead to what extent. The qualitative method is, therefore, inappropriate for my study, and for these reasons I opted to forego the qualitative method as my objective was to analyze the relationship between the defined independent variables and the decision-makers' intention to adopt cloud computing.

I found the mixed-method approach also incorrect for my study. The mixed method framework integrates both the qualitative and quantitative approaches into a

single research tool with each component interdependent upon the other (Guetterman et al., 2015). One of the prime considerations is the nature of the study and the reported findings as both empirical and conceptual, taking inquiry from both statistically causal inferences across a generalized spectrum and the exploration of a specific phenomenon from an individual's perspective (Guetterman et al., 2015). From an epistemological perspective, the identification and description of the data is rendered from both analytical and philosophical approaches (Sparkes, 2015; Tricco et al., 2016). However, Sparkes (2015) noted that utilizing mixed methods without adequate cause may produce disjointed and unfocused research.

Therefore, I also chose to negate a mixed method approach as I did not require any of the qualitative components, nor did I need to discover the important variables. For my study parameters as post-positivist and objective, wherein the independent variables derive from self and documented knowledge, and objectivity is more aligned with the intent to achieve knowledge to what extent the dependent variable is impacted, I opted for the quantitative methodology.

Research Design

My study utilized a non-experimental, cross-sectional correlational design employing a survey instrument to gather the necessary data. Correlational research focuses on defining relationships between two or more variables in a single population or multiple populations and measures the strengths of those relationships (Curtis et al., 2016). That relationship may be negative, indicating the rise of one measure the decline of the other, positive, as one increases the other follows, or indicate the non-existence of

any relationship (Gogtay & Thatte, 2017). Furthermore, the study will feature a cross-sectional design analysis, wherein multiple variables receive analysis at a single point in time, as opposed to a longitudinal study, wherein continuous or repeated measures over a prolonged period execute (Caruana, Roman, Hernandez-Sanchez, & Solli, 2015). In addition, cross-sectional designs are inherently flexible, allowing for multiple insights into a single core construct (Martin et al., 2019). Correlational designs, however, are prone to bias because of self-reporting measures, so one must ensure to incorporate only objective data (Martin et al., 2019).

The design option aligns with the intent of the study, which is to assess the degree of impact within the scope of the relationship between the variables for ST, DL, DP,MI, AH, SP, SC, FS, and the intention to adopt cloud computing.

Alternate options include a longitudinal design, as previously noted. However, such designs are generally observational or experimental, and could be formed from repeated cross-sectional studies, prospective studies (over time), or retrospective wherein the data are collected after exposure (Caruana et al., 2015).

It is not necessary to repeat my cross-sectional study, nor accompany the participants over time to determine if their views change as the intent of the study was to determine which factors currently prohibit the implementation of cloud from a decision-maker perspective.

Experimental design is another option that is used to isolate the phenomena under controlled conditions in which the experiment executes and consists of a control group and a minimum of one experimental group (Rutberg & Bouikidis, 2018). The variance

across groups for participants is controlled via a randomization process to compare results across for variances (Rutberg & Bouikidis, 2018). However, the precise conditions between experimental operations must exist to validate the findings, save for the influential variable (Anderson, Wennberg, & McMullen, 2019).

My study required only a single instance and no control group to validate the perceptions of the decision-makers as there exists no single influential variable upon which to garner data to determine causation with the decision-makers. The selected pool will not be precisely random, instead a convenient sampling, consisting of those that respond positively to the invitation.

Population and Sampling

The specific population targeted for this study consist of IT directors and CIOs who maintain the key deciding control regarding the adoption (or lack thereof) for cloud. The intent was to restrict the population to only key management roles within the United States, and to focus entirely on those that have not yet fully implemented a cloud-based solution in order to gauge the security perceptions this population uses to formulate their decision to impede adoption. I employed a non-probabilistic, convenience sampling method to acquire my data as willingness, broad accessibility, and a constraint limiting the population to key decision-maker within the organization, are the sole participant criteria.

The extant research identifies a gap in participant acquisition as the studies to date explore the limitations and impact of vulnerabilities through the lens of the security practitioner (Hsu & Lin, 2016; Senyo et al., 2016; Wahsh & Dhillon, 2016). While valid,

the restricted viewpoint does not account for the perceptions on the part of key decision-makers and how that perceived reality impacts or impedes entirely cloud enablement. There is a tendency toward a disconnect between the real and imagined in the non-expert's mind wherein narratives provide a framework upon which perceived adversity exists and thus, impedes change (Botzen et al., 2015). Therefore, the direction of this study was to define the decision-maker's perspectives and concerns in a hierarchical and graded matrix, permitting security practitioners a path to mitigation, either by education or resolution. Establishing the context of perceived impacts as impediments to adoption aligns with the study participants as key, managerial decision-makers.

The primary difference between a probabilistic and non-probabilistic sampling approach is the instantiation of absolutes. In probability sampling, every subject within a population is provided an equal opportunity to represent the sample and conversely, non-probabilistic sampling determines the inability to determine such opportunity (Martinez-Mesa, Gonzalez-Chica, Duquia, Bonamigo, & Bastos, 2016). Probabilistic samples allow for generalization and therefore, conclusions drawn to the population as a whole with testing for statistical significance albeit at great expense in both time and resources whereas conversely, non-probabilistic samples cannot generalize data but operate at reduced resource consumption (Landers & Behrend, 2015). As it will be impossible to assure that every possible subject receives notification and access, this study will employ a non-probabilistic approach. Within the scope of non-probabilistic sampling are several types: convenience, purposive, quota, and "snowball". Snowball sampling relies on a select group of participants indicating avenues to attain potential candidates to further the

study participant pool, while quota sampling confers a series of requirements for specific characteristics (Martinez-Mesa et al., 2016). Furthermore, according to Stivala, Koskinen, Rolls, Wang, and Robins (2016) snowball (or chain referral) sampling, employing this seeded method, may generate biased samples as the preferred participants exhibit similar characteristics. Purposive sampling more closely aligns with qualitative research, as the intent is to identify key participants as a deliberate action based on qualities possessed or by virtue of knowledge to produce a sound response (Setia, 2016). Convenience sampling requires only the most practical of criteria, such as proximity, ease of accessibility, or willingness to participate and is an affordable method to obtain data, until total participants reaches sample saturation or time saturation (Martinez-Mesa et al., 2016; Setia, 2016). The only constraint within this study's participant pool parameters is that it must consist of executive-tier decision-makers to garner the proper perceived risks, a practical requirement. No other restrictions exist and while the data will capture the size and scope of the organization, it is not a limiting factor. Therefore, convenience sampling within the non-probabilistic approach is appropriate for the study, as I was unable to ensure access to or responses from every potential subject and is cost prohibitive, and therefore, opted for an affordable option that provides a greater ease of access. However, as Jager, Putnick, and Bornstein (2017) stated, it is possible to redefine and improve upon the value of convenience sampling by defining a sociodemographic framing to improve generalizability. Focusing my study on a single, yet imperative qualification factor (the capacity of decision-maker for the entire organization) increases the homogeneity factor, thereby improving the generalizability. The disadvantage of

such a narrow generalizability is more of an impacting factor for describing an entire population (Jager et al., 2017). For my study, the focus is directly placed upon those in such a capacity, and it not a limiting factor as the entire participant population consists of those qualifications.

I calculated the sample size requirements utilizing G*Power (version 3.1.9.2), applying a medium threshold of .15 to a binary logistic regression, fixed model series f-test. G*Power is a statistical software package developed by researchers at the Institute for Experimental Psychology to calculate the a priori sample size (Faul, Erdfelder, Buchner, & Lang, 2009). An a priori power analysis constraining the effect size ($f = .15$) and the power to .8 (80%) produced a sample size of 114. Increasing the power to .95 (95%), derives a sample size of 166. Therefore, the study required a sample size between 114 and 166 (see Figure 2). Additionally, I calculated sample size using the Tabachnik formula; $N \geq 50+8m$, where m is equal to the number of independent variables (Fareen, Alam, Khamis, & Mukhtar, 2019). The derived value of 122 aligns with the G*Power estimate within tolerance.

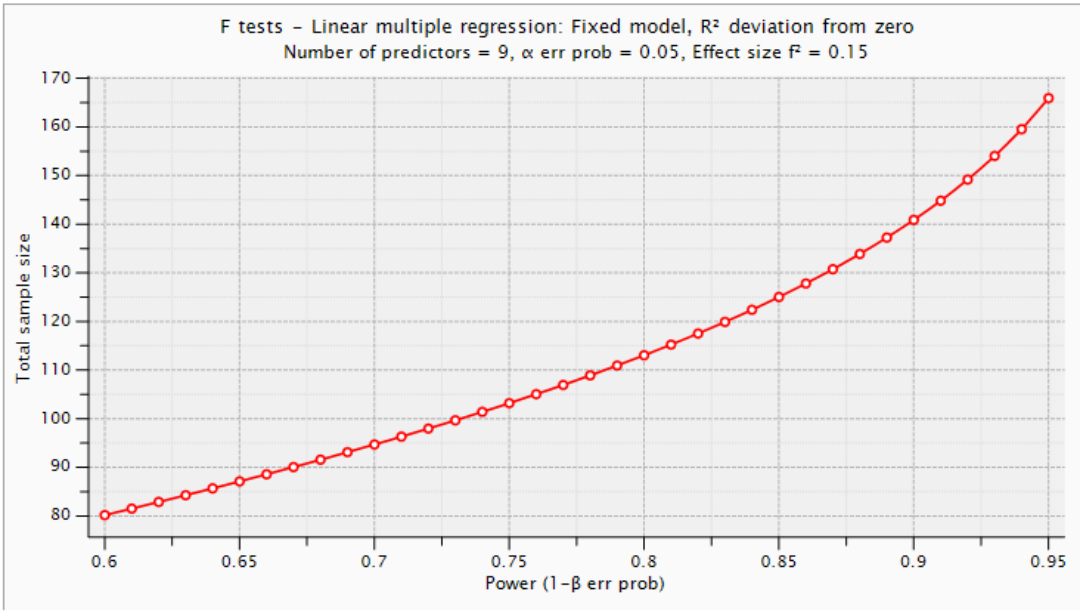

Figure 2. Power as a function of sample size.

Ethical Research

Federal regulations require researchers to obtain informed consent from all participants and is the foundation of ethical conduct in research practices (Koyfman, Reddy, Hizlan, Leek, & Kodish, 2016; Resnik, Miller, Kwok, Engel, & Sandler, 2015). Human subjects should be informed regarding the implications of the research and understand their rights throughout the process (Chiumento, Khan, Rahman, & Frith, 2016). A key aspect of any ethical position is the protection of personal information, a necessary component for a transparent informed consent document. My study did not collect any personal information as the key participants were gathered from a pool of known decision-makers without gender or age specifics and therefore, anonymous, providing no connection to a particular identity. Informed consent is a standard ethical component for any research that involves informing the participants about any potential

risks to themselves or their collected personal information while garnering their agreement to take part (Perrault & Keating, 2018). The only remaining identifiable data points will be those of scope and size of the firm from which the participant is employed, although no specifics on organizational names or geographies will exist within the survey. However, all collected data and results will be stored on a secure and encrypted USB key, stored in my personal safe for five years, at which time it will be destroyed. The survey instrument invitation will clarify these points for transparency and the consent is assumed once the link is activated to access the survey tool. Additionally, a current Certificate of Completion from the National Institutes of Health (NIH) Office of Extramural Research provides validation and evidence of training in protecting human research participants (see Appendix A).

Incentivization is often a challenge to both bias and the ethics of acquiring and representing factual data (Keeble, Baxter, Barber, & Law, 2015). Additionally, varied incentives work positively and negatively with different participants, indicating the potential for reverse bias is equal (Keeble et al., 2015). Therefore, I offered no incentives for participation in my study, reducing to zero the potential for an ethical dilemma or bias injection.

The withdrawal process is inherent in the survey instrument. Should any participant wished to withdraw, they could have chosen to disregard the invitation or disengage the survey tool by exiting prematurely without submission. The procedures for these circumstances were included in the invitation email. How the research intends to handle data after withdrawal is a necessary data point for participants to understand

(Adams et al., 2017). Therefore, I included measures for data retention, as it is all anonymous, though exclude it from the research study parameters and document this in the invitation. Once withdrawn, the data was excluded from the scope of the study. In addition, the invitation detailed the terms of participation, such that no monetary or other incentives exist for completion. As the instrument did not collect personal information, it would be impossible to offer incentives as no link between the completed form and the individual existed. A copy of the email that discussed the informed consent and requests participation may be found in Appendix B.

Data Collection

The intent of this study was to examine both the existence and degree of a relationship existing between various perceived security considerations inherent to cloud and the decision makers' intent to adopt. I decided to utilize a survey instrument to capture quantifiable data on the existence of such impeding factors and to what degree each is perceived as impacting. Additionally, I opted to apply the TOE method as my framework as it dynamically encompasses both the systems approach and the operations environments while considering data regarding the operational aspects toward a holistic view on technology adoption (Tornatzky & Fleischer, 1990). The application for the three data constructs within the TOE examines the characteristics of the technology, while the organizational focuses on formal and informal linking structures, the size, and scope of the business operation (Lippert & Govindarajulu, 2006; Tornatzky & Fleischer, 1990). Environmental contexts dissect external elements and characteristics inherent in the industry or market to include support and government regulation (Lippert &

Govindarajulu, 2006; Tornatzky & Fleischer, 1990). Wahsh and Dhillon (2016) emphasized some of the externalized factors to include MI, DL and the impact of RC. The inclusion of environmental and organizational aspects to the business decision provides a holistic viewpoint toward the acceptance and implementation of a particular technology while providing constraints for the system (Gangwar et al., 2015; Tornatzky & Fleischer, 1990). The combination of the three contexts specifically defines correlative relationships between new technologies and an organization's willingness to adopt (Lippert & Govindarajulu, 2006). The survey instrument was a modified framework derived from prior research: two focusing on adoption, the other on security perceptions (Klug & Xue, 2015; Lease, 2005; Rhee, Ryu, & Kim, 2012). I requested and received permission to utilize these survey instruments as a foundation for my composition (see Appendix C). The completed instrument derived the existence and depth of impact to perceived security concerns within cloud environments by decision-making executives. The instrument construct will utilize a Likert scale question set using ordinal values numbered one through seven. The Likert scale was developed in 1832 and is a scientifically validated and accepted method to measure attitude, defined as a preferential means of behavior or reaction under specific circumstances founded in perception and belief (Joshi, Kale, Chandel, & Pal, 2015). The survey employed both positive and negatively focused items to reduce response-set bias and allow for respondents to vary their concurrence from strongly agree to strongly disagree across seven scale values (Willits, Theodori, & Luloff, 2016). Willits et al. (2016) also noted that the consensus is at least five data points per item to accurately achieve a data construct. Joshi et al. (2015)

state that the application of a 7-point scale (as opposed to a 5-point) permits retrieval beyond the absolute, offering a means to calculate the variances and measure the distance between responses. The latter was an imperative for my study, as I intended to device a hierarchical approach to mitigation and require the more minute scales to register importance of perceptions. The original survey instrument created by Klug and Xue (2015) focused on the variables that prevented adoption of cloud in addition to those that were perceived to be beneficial from a position of lacking adequate understanding of the technology to effectively draft such a decision. Similarly, Njenga, Garg, Bhardwaj, Prakash, and Bawa (2019) examined the relevant technological, organizational, and environmental aspects as relevant factors that impeded cloud system adoption in higher learning environments, noting the importance of security concerns.

The purpose of the TOE framework is to study the adoption and implementation of innovation in technology by organizations from three contexts: technological, organizational, and environmental (Tornatzky & Fleischer, 1990). The survey instrument represents a synergy between the constructs approved for use by prior authors, thus both providing a solid and valid foundation as well as a recognized means to associate adoption parameters with perceptions. The study will emulate for format, albeit modified, as provided by Klug and Xue (2015) into distinct categories of potentially impeding factors and likewise, will also employ a 7-point Likert scale to derive the minute details of perceived vulnerability. As established by Alkhalil et al. (2017), there are three categories of influencing factors when considering the adoption of new technologies; technological, environmental, and organizational aspects determine

viability for an organization and reflects upon the influencers within each. Hsu and Lin (2016) further attribute cloud adoption concerns, and specifically note the perspective beliefs as a core component within the technological framework, to derive the innovative benefits and detriments associated with the new technology. From an organizational perspective, the firm size and scope may contribute to perceived reliability or lack thereof (Klug & Xue, 2015). Environmental concerns focus on regulatory compliance in addition to the trust an organization places upon a service partner and their ability to manage operations (Alkhalil et al., 2017; Hsu & Lin, 2016). The questionnaire consisted of forty-three (43) questions, the majority of which are a Likert 7-point scale to measure each of the following; ST, AH, SP, MI, DL, SP, RC, and attributes of the organization itself defined as SC and FS as potentially contributing factors. I inquired as to the overarching grasp the decision-maker perceives they possess regarding cloud and the security landscape as additional contributing factors.

The intent of the technological construct focuses on factors that influence or drive security concerns within that scope such as the lack of isolation within a public cloud environment or the protection of data at rest. The sharing of resources is a technological aspect, with the onus placed with the provider to ensure protected scalability and prevent misuse across cloud services (Hsu & Lin, 2016; Kazim & Zhu, 2015; Kalaiprasath et al., 2017). ST (also termed multitenancy) has been identified through extant literature as a critical issue impacting confidentiality but is an organic result of the economic benefits derived from the technology (Ali, et al., 2015). AH impacts both the confidentiality and integrity of the users and requires policies and tools implemented to detect and prevent

occurrences (Kalaiprasath et al., 2017). Additionally, it is also considered a network threat as it may employ various techniques to obtain access to an account from a management perspective, such as fraud, cross site scripting, service vulnerabilities that exist in the system, as well as software vulnerabilities (Kazim & Zhu, 2015). Alassafi et al. (2017) concluded that AH or service hijacking is statistically confirmed as a credible and persistent risk factor for cloud adoption. Kazim and Zhu (2015) state that the largest challenge is the protection of data from a platform perspective and handling procedures impact the sanctity of said data to ensure against manipulation or malicious encryption. Rao and Selvamani (2015) presented information that indicates DP equates to a high-risk challenge with a 92% impact on security concerns with technological controls. Regardless of the ingress point (internal or external via network access) programmatic means should employ to reduce the impact of these threats to modified data (Kalaiprasath et al., 2017; Phaphoom et al., 2015).

Environmental contexts include considerations for MI as the concept relates to service partner access to running services. While the CSA has established that MI (defined as both within the business and the service partner) as the third highest risk factor and include non-MI or employees of either organization that do not intend harm (Ramachandra et al., 2017). MI are considered an environmental risk factor as they are typically trusted employees (specifically third-party) that maintain access to information and services and present a risk with ever increasing and uncontrolled (by the business) access (Alassafi et al., 2017; Shrivas et al., 2016). Another environmental consideration includes DL representing a lack of data confidentiality as an externalized factor and

subject to environmental framework (Wahsh & Dhillon, 2016). The acquisition or elimination of data from externalized sources regardless of the mechanism indicates a negligence of environmental controls (Lam, 2016). Another externalized consideration is the faith and trust one imbues upon their provider or service partner. Alassafi et al. (2017) denote that trust constitutes a myriad of considerations (such as authentication and protection of the service) and requires a security culture on the part of the service partner (and the business entity) which includes training in ethics and proper security posturing. Regulatory compliance and outsourcing risks (or a lack of trust ion one's provider) are key environmental considerations when considering cloud adoption (Kazim & Zhu, 2015). Klug and Xue (2015) applied RC as well as service provider support as environmental contexts in their TOE research model.

The remaining two considerations for organizational context are FS and SC and are integral to the original framework (Tornatzky & Fleischer, 1990). Similarly, Senyo et al. (2016) reestablished both factors as organizational in their research also studying cloud adoption. Klug and Xue (2015) include institutional size as a modifying factor toward adoption of cloud, and while positive, their research indicated that technical compatibility, or the focus of the SC, was not an impacting factor. Hsu and Lin (2016) referred directly to organizational contexts as the FS and SC as a base characteristic of the organization, representing the geographical dispersal of the organization may provide greater desire for a global cloud program in additional to a larger firm possessing greater resources to facilitate adoption. The inclusion of beneficial factors, such as ease of use and cost savings, are prolifically noted in the researched extant literature both proving to

be factors that increase the likelihood of adoption for cloud and universally note the negative security implications as a limiting factor, though do not offer details sufficient for practitioners to resolve effectively (Alassafi et al., 2017; Hsu & Lin, 2016; Kazim & Zhu, 2015; Klug & Xue, 2015). For these reasons, I opted to remove these beneficial markers from the survey and focus entirely on the perceived impacts of security concerns as a detriment to adoption.

Hsu and Lin (2016) validated their survey instrument, designed to assess viability of cloud adoption, prior to execution utilizing both a pre and pilot test, cycling through top Information Systems executives and MBA students to establish reliability. Similarly, Klug and Xue (2015) conducted a pilot study to validate their instrument (also a framework establishing adoption consideration) as it applies to the TOE framework. The instrument used by Klug and Xue was foundational to my survey, albeit slightly modified to account for only security concerns. As established, my study will utilize quantitative methodology. Quantitative studies classify attributes and uses them to construct statistical models to explain observed information for which the researcher knows in advance what to look for (Landrum & Garza, 2015; McCusker & Gunaydin, 2015). I am, through experience and research, well-versed in the various archetypes of security concerns which I intended to use as independent variables. A quantitative researcher typically uses tools such as surveys or equipment to collect numerical data from which statistics are derived and is more efficient in testing hypotheses while remaining objectively distinct form the data (Antwi & Hamza, 2015; McCusker & Gunaydin, 2015). Therefore, a survey instrument is the most appropriate given the parameters of the study

and lend additional objectivity toward analysis of the results. The prior work by Klug and Xue (2015) included CIOs across the United States and Canada. The survey instrument utilized by Lease (2005) focused on a regional area within the Mid-Atlantic consisting of Virginia, Maryland, and the District of Columbia. Within their study on security information management, Rhee et al. (2012) targeting MIS executives within the United States.

Instruments

My instrument was the derived work from three prior instruments as deployed by previous researchers and proven reliable (Klug & Xue, 2015; Lease, 2005; Rhee et al., 2012). The required consent and approval to obtain and employ these instruments were garnered via email (see Appendix C). My survey, consisting of 43, 7-point Likert scale questions, will be administered via SurveyMonkey and accessed via a link provided to the participant group both explaining the intent of the study and providing for the protection of personal information. Within the 7-point scale, queries will reverse polarity across the expanse of the survey to avoid response set bias. The survey is based on Klug and Xue (2015), with security interpretations garnered through Rhee et al. (2012). I borrowed from Lease (2005) the focus on managerial attitudes as queries within the confines of the survey. The framework, as it relates to the TOE was extricated directly from Rhee et al. to attribute perceived interpretations toward the three context variables within he TOE. The format follows the Lease instrument in organization to acquire the IT manager' perceptions of biometric effectiveness. While the format of the Lease framework remained, the work by Rhee et al. introduced the security risk perceptions, as

defined in their instrument to garner security manager's interpretations of established risks. The addition of Klug and Xue forms the basis of some of the additional queries used to determine the familiarization with the concepts and their value to the organization. Klug and Xue applied their instrument to determine the adoption rate of cloud at universities and included the formation of perceived barriers to adoption.

The validity and reliability of any quantitative study is characterized degree to which the concept is measured accurately (Antwi & Hamza, 2015; Cypress, 2017; Leung, 2015). The implication is that the survey instrument must adequately and precisely measure the intended concept. Additionally, the construct of validity is measured across three distinct types: content, construct, and criterion. These types measure the extent to accuracy in measurement of all aspects, extent of measurement for intended context, and the extent of relationships to prior instruments that measure similar variables (Leung, 2015). Reliability pertains to the degree of consistency of the measurement, thus a repeated operation should provide approximately the same results (Cypress, 2017). Similar to validity, there are three attributes of reliability including internal consistency, stability, and equivalence that assess the extent to which all items on the scale measure a single object, the consistency of results, and the consistency of responses (Heale & Twycross, 2015). To address content validity, the survey instrument will include multiple queries related to the same subject and adequately cover all aspects of security within the domain of vulnerability concerns as per the extant literature. There are three different means of providing construct validity: homogeneity (measuring one construct), convergence (similarity with other instruments), and theory evidence (behavior emulates

the theoretical hypotheses measured by the instrument) (Heale & Twycross, 2015). The survey instrument for my study will measure a single construct; the impact of security on decision making regarding cloud adoption, thus providing homogeneity. There is convergence as the instrument will be similar to previously referenced articles, employing both structure and content. It was difficult prior to deployment to assume the theory evidence as the survey had not yet deployed, however, applying the extant literature and prior studies on the subject of security as an impeding factor for cloud adoption, and emphasizing those that delineated between technical architects and decision makers, it was likely to converge. The final context of validity is criterion, making use of established instruments that already measure similar variables, that also divide into three types: convergent (highly correlated with prior instrument), divergent (displays poor correlation to instruments that measure different variables), and predictive (high correlation impact with future criterions) (Heale & Twycross, 2015). My study will utilize the framework of several referenced prior works, and while some of the variables are similar, it relied mostly on predictive validity, as the overarching criterion is now dissected into multiple variables with the intent to find a hierarchical matrix and future criterions meant to measure the aspects of the security criterion will match. There is also some degree of convergent validity, as all aspects of security as a criterion are detailed within the study parameters though converged for the purpose of the survey instrument. Regarding the internal consistency, assessment includes the use of Cronbach's α (or alpha) that measures the reliability of summated rating scales and is one of the most published forms of rating said reliability (Ain, Kaur, & Waheed, 2015; Taber, 2018;

Vaske, Beaman, & Sponarski, 2017). The significance of the influence quantities rates strongly between .50 and .80, though are most acceptable rated higher than .80 (Inal, Yilmaz Kogar, Demirduzen, & Gelbal, 2017). I did not perform test-retest functions within my survey, so will be unable to adequately validate stability, though I suspect that equivalency will demonstrate across the spectrum of respondents. Klug and Xue (2015) provide as a perceived barrier to adoption a single entry related to the perceived security of the platform in addition to noting elsewhere in his instrument the concerns regarding regulatory compliance and trust for a service provider. However, in the defining literature forming the foundation of his security, RC, and service provider support concerns, he notes issues with privacy and security, data security, user control (MI), DP, regulatory non-compliance, SP, and ST vulnerabilities (Klug & Xue, 2015). The survey instrument employed by Rhee et al. (2012) directly measures risk perception using a 7-point Likert scale focusing on a generalized security posture perspective also defined within the study as vulnerabilities across the shared security practices and threat landscapes. Robertson (2008) provides the similar framework, inferring trust within the partnerships with providers for environmental context. Lease (2005) focuses on biometrics adoption yet provides a sound foundation when performing a survey on adoption potential and the perception of business executives. Klug and Xue (2015) performed a pilot study to validate the content validity of the instrument and applied a Cronbach alpha to test successfully for internal reliability. Robertson (2008) established reliability and validity through the execution of Cronbach's alpha for internal consistency, the test-retest method was employed to ensure content validity, and

correlational analysis proved construct validity. Rhee et al. (2012) also performed a pilot test framework to establish content validity and reliability. Lease (2005) established reliability also employing a test-retest sequence and applied Cronbach's alpha to successfully establish validity.

As noted, my study will receive modifications to those utilized as foundational frameworks. The changes will elaborate upon the security aspects, expressing the singular or grouped risk-based perceptions of the topic as generally provided, to listing each component that comprises the security realm. The survey is presented in Appendix D, and the raw data will be available upon request.

Data Collection Technique

As previously detailed, data collection for this study is a survey questionnaire and existed on the Internet site hosted by SurveyMonkey. There are several key advantages to utilizing an online instrument such as rapid and favorable response rates and reduced cost for operation (Mlikotic, Parker, & Rajapakshe, 2016; Saleh & Bista, 2017; Toledo et al., 2015). The ubiquity of online platforms for survey material permit large quantities of data to be collected quickly and cheaply and aid in targeting specific resources (Fitzgerald et al., 2019; Raths, 2015; Rice, Winter, Doherty, & Milner, 2017). Additional advantages include real-time accumulation of data, the reduction on bias on the part of the researcher, and perhaps the largest benefit is the potential for more accurate reporting because of perceived anonymity (Rice et al., 2017; Saleh & Bista, 2017; Toledo et al., 2015). However, there are drawbacks noted with online survey instruments as well. Toledo et al. (2015) noted a reduced response rate and concerns regarding validity. More

recent studies negate these concerns as modern audiences are more adept at online tool consumption and provide a broad spectrum of user population from which to cull (Rice et al., 2017). Depending on the type of instrument, that is, the source, variations may occur which limit the feasibility or increase bias, such as the time-limitations using Amazon's MTurk, or the difficulty in ensuring a proper diffusion within the participation pool (Rice et al., 2017). Online research is also noted as measuring perceptions and not behaviors and may ingest data from non-experts in the field (Rice et al., 2017). The drawback is a benefit for my study as the intent was to measure perceived realities and to target executives that are inherently, not experts in the field.

A pilot study was not necessary given the nature of my study. The prevailing benefits are the reduction in time and cost and pre-testing the material with the target population (Kinchin, Ismail, & Edwards, 2018). There was no cost, and no time variables pertinent to my study, nor was it beneficial to pre-test the queries with a population that admittedly, possesses no actual expertise. The extant literature provided, in correlation with the foundational survey instruments establish the dissected criteria for the over-arching topic considering security concerns. The result of the study was to determine perceptions by those sans expertise but in a position to decide upon the future of cloud within their respective organizations. The measurements and queries originated within validated instruments thus negating further the necessity for a pilot study.

Data Analysis Technique

Nine variables within the three constructs of the TOE framework establish the conceptual model for determining the impediments to cloud adoption. The TOE

framework is highly adaptable and widely applicable as researches may choose contextual factors that fall within the constraints of three categories without influencing the decision toward specific variables (Yang, Sun, Zhang, & Wang, 2015). Those ten variables, consisting of seven security constructs and two organizational descriptor variables formulate the basis of the questions within the survey instrument. The origin of each security-focused qualifier is adapted from the extant literature and prior research instruments. Binary logistic regression is the most applicable method to apply to a correlation question to determine which variables are most strongly correlated to the dependent variable and has been widely employed in the analysis of influencing factors (Kohn, 2018; Lever, Krzywinski, & Altman, 2016). The use of binary regression is preferred when there are two or more independent variables and the singular dependent (nominal) variable may possess one of two states (Lever et al., 2016; Kohn, 2018). My dependent variable (adoption) is dichotomous, either negative or not, as influenced by the independent variables' attributes. Binary logistic regression offers an objective position for analyzing the impacts of multiple, and perhaps plentiful, covariates on a binary result set (Li, Morgan, & Zaslavsky, 2018). Specifically, Awa et al. (2016) concluded that binary logistic regression, when the dependent variable is dichotomous, more accurately assesses the influence by numerous factors on adoption as said dependent variable within a TOE framework. Yang et al. (2015) employed binary logistic regression to analyze the impact of various components tied into the TOE framework as impeding factors toward the adoption of Software as a Service (SaaS).

Regarding alternative options, other researchers have employed the structural equation modeling (SEM) technique of statistical analysis toward the TOE framework. Cruz-Jesus, Pinheiro, and Oliveira (2019) utilized Partial Least Squares (PLS) to analyze adoption of CRM structures, as PLS does not require normal distribution. Regardless, PLS as a derivative of SEM utilizes multiple dependent (in addition to independent) latent variables and define parameters for an entire theory (Khan et al., 2019). I neither possess multiple dependent variables, nor did I require the evaluation of a theory for my study, thus I did not choose PLS-SEM.

The analysis of variance (ANOVA) construct has also been employed by researchers utilizing the TOE. Al-Hujran et al. (2018) utilized the TOE to understand the determinants of cloud computing adoption. ANOVA worked for this research, as there was a normally distributed dependent variable and the independent variable was categorical. The dependent variable was distributed across the variances by the independent variable. The multiway (or multivariate) analysis of variance (mANOVA) requires two or more dependent variables, such as in the study by Chen, Chuang, and Nakatani (2016) concerning the adoption of cloud-computing as perceived by the adopters. Multiway (and by extension, two-way) ANOVA analysis methods rely on multiple dependent variables, or upon a combination of variables impacting the dependent, and there is no a priori research to form a hypothesis about how each influence and therefore simply seeks any form of relationship exists, thus providing a hypothesis (Cramer et al., 2016; Mertler & Reinhart, 2017). My study neither required multiple dependent variables, nor is there a dearth of a priori research available to ensure

that independent variables do not overlap or compound, therefore I did not choose two-way or multiway ANOVA.

Data Screening

Survey data collection is the most prevalent form within organizational sciences for the reasons stated above, namely the capacity to obtain large amount of data in the form of self-reporting survey input with minimal time, effort, and expense (DeSimone, J.A., Harms, & DeSimone, A.J., 2015). It is not without disadvantages, however, as researchers are unable to validate through direct observation the process and must rely on motivated participants providing thoughtful and complete responses thus requiring a data screening process (DeSimone et al., 2015; Jones, House, & Gao, 2015; Rutkowski, L., Rutkowski, D., & Zhou, 2016). The various methods of data screening attempt to identify response patterns of a lower quality and are classified in three broad types: direct, archival, and statistical (DeSimone et al., 2015). A direct screening method involves the insertion of data gathering items into the instrument prior to execution, such as self-reporting indices, specific instructions contained within the survey, or fabricated queries (DeSimone et al., 2015). The archival method include semantic synonyms (similarly worded queries designed to determine repetitive responses), semantic antonyms (dissimilar answers to similar questions), and response time (speed of completion) which helps understand the average compute time and thereby determine alacrity of answers if provided in a quantifiably shorter period (DeSimone et al., 2015). Statistical screening involves the application of calculations regarding the statistical behavior of typical responses, such as psychometric synonyms (which resemble semantic

synonyms though are dictated by the researcher prior to execution as a synonymous pair), psychometric antonyms (similar to the synonym but with polar effect), personal reliability (the averaging of two scores across the respondents), and Mahalanobis D (a multivariate version of outlier analysis, designed to compare respondent scores with sample mean to remove outliers), each to focus on descriptive statistics for individual items, such as kurtosis or standard deviation (DeSimone et al., 2015). The data screening process also involves validating the completeness and accuracy of the collected information, identifying and removing occurrences of missing data in addition to the outliers and data quality measures previously described (Flores & Ekstedt, 2016; Mertler & Reinhart, 2017).

Sharma, Al-Badi, Govindaluri, and Al-Kharusi (2016) employed multiple regression analysis in determining predictive motivators toward cloud adoption in a developing country. Similarly, Afendulis, Caudry, O'Malley, Kemper, and Grabowski (2016) utilized binary logistic regression analysis on the adoption of the Green House model for nursing home quality of care measures. Both employed multiple and significant independent variables against a dichotomous dependent variable: the adoption or non-adoption of innovation (Afendulis et al., 2016; Sharma et al., 2016). Ranganathan, Pramesh, and Aggarwal (2017) stated that binary logistic regression is a statistical technique to evaluate relationships between predictor variables and a binary or dichotomous variable. Within the parameters of my study, the various predictor variables are each of the categorizations for threat vectors, while the binary or dependent variable is the likelihood of adoption. However, for multiple regression techniques to be valid

there are several assumptions pertaining the statistical method. Unlike linear regression, homoscedasticity and normality are not relevant and therefore not required to be tested for, though multicollinearity (or the correlation between independent variables), missing data, and outliers are necessary (Solares, Wei, & Billings, 2019).

Missing Data

There are three types of missing data types: missing completely at random (MCAR), missing at random (MAR), and missing, not at random (MNAR), all of which can constitute substantial challenges with the analysis and interpretations process and if included, can weaken the validity of the conclusions (Kontopantelis, White, Sperrin, & Buchan, 2017; Pedersen et al., 2017). Mertler and Reinhart (2017) suggested as a guideline that should 15% or less of the data are missing from the survey instrument response, one may replace the data with the mean score for the measure. However, if more than 15% of the material is missing, my intent was to remove that response from the study findings. I assumed the respondents are all key decision-makers, as that is my intended target audience, so establishment of role is not an essential consideration for disqualification. Similarly, aside from environmental and organization queries regarding the particular business, there are no demographics data collected, therefore, not a qualifying point.

Assumptions

One must adhere to assumptions associated with correlation and binary logistic regression analysis techniques such as multicollinearity, outliers, and normality

(Vatcheva, Lee, McCormick, & Rahbar, 2016; Hickey, Kontopantelis, Takkenberg, & Beyersdorf, 2018; Ranganathan et al., 2017).

Multicollinearity. Multicollinearity exists when two predictor variables that are highly correlated are examined simultaneously during regression analysis, which results in biased or unstable errors and possibly interfere with the statistical significance of the predictors (Ranganathan et al., 2017; Solares et al., 2019; Vatcheva et al., 2016). A means to test for multicollinearity involves calculating for the variance inflation factor (VIF) (Chou & Chou, 2016; Klein & Luciano, 2016; Vatcheva et al., 2016). However, multicollinearity tests the variables within a linear regression model, but may be employed to examine the independent variables within a binary logistic regression model in a linear fashion to determine if the predictors are highly correlated (Khikmah, Wijayanto, & Syafitri, 2016; Vatcheva, Lee, McCormick, & Rahbar, 2016). I intended to calculate a VIF between the independent variables to determine if a relationship exists, however, the nature of the disparate vectors there is little opportunity for overlap. I also employed the bootstrapping feature of SPSS to alleviate any potential assumption values.

Outliers. Outliers consist of deviating values within a collection of observed data and are regarded as such if the value differs greatly from alternate values (Aziz, Ali, Nor, Baharum, & Omar, 2016; Mertler & Reinhart, 2017; Ohyver, Moniaga, Yunidwi, & Setiawan, 2017). Outliers in binary logistic regression analysis are identified using standardized Pearson residuals or through observation (Aziz et al., 2016; Ohyver et al., 2017). Should any result set appear to be an outlier, I first examined, then tested using Pearson residuals to ensure outlier restriction.

Normality. If the data are considered abnormal, transformation would be necessary. In binary logistic regression analysis, nesting or a hierarchical approach founded on demographics could skew the data resulting in under-or overdispersion (unexpected diverse, or clustered results) which could lead to an increased probability of null hypothesis rejection unless the data is substantiated as independent values (Solares et al., 2019; Hickey et al., 2018; Vatcheva et al., 2016). As the roles and purpose for each participant remains similar, there is little risk to under or overdispersion as the demographics are equal even across various firm sizes and scopes. If multicollinearity does exist, all independent variables would have been reconsidered and perhaps dropped or refined for a secondary survey instrument. Otherwise, assumptions were managed, as noted, through identification and mitigation.

The statistical analysis for my study will be executing using IBM SPSS software, version 24. Rasyid, Bhandary, and Yatabe (2016) formulated a logistic regression analysis using SPSS, allowing them to conduct complex analyses without the necessity of developing toolsets to drive the data. Similarly, Jamal, Ghafar, Ismail, and Chek (2018) compared the use of SPSS to other similar packages, finding SPSS the most prevalent across all research studies. Wu et al. (2017) completed a study on landslide susceptibility using logistic regression analytics within the SPSS framework.

Reliability and Validity

Reliability

In the context of qualitative research, reliability implies a consistency and repeatability of the process and the result set within tolerance for a margin of variability

(Leung, 2015). To reduce the potential for variations leading to diverse result sets, a researcher may adapt survey instruments from prior studies, thus increasing the reliability and repeatability (Šumak & Šorgo, 2016). My study employed as foundational constructs the prior work from several prior validated works (Klug & Xue, 2015; Lease, 2005; Rhee et al, 2012). Furthermore, Ali, Rasoolimanesh, Sarstedt, Ringle, and Ryu (2018) in addition to Henseler, Hubona, & Ray (2016) state that any result greater than .7 for Cronbach's alpha and composite reliability confers internal reliability. Using Cronbach's alpha to assess the reliability of the instrument and subsequent measures is appropriate to address any concerns or threats to reliability (Topaloglu, Caldibi, & Oge, 2016).

Validity

Researchers must produce evidence of validity to strengthen their arguments and extricate potential confounding factors through the identification and pronounced mitigation for external and internal validity threats (McKibben & Silvia, 2016). Controlling, minimizing, or eliminating threats to validity for results is one of the most important concepts in research (Haegele & Hodge, 2015; Orquin & Holmqvist, 2018).

External validity threats refer directly to the degree at which results are generalizable and include threats to reactive or interactive effects from testing, selection bias (including experimental treatment), reactive effects, and treatment interference (Haegele & Hodge, 2015). Threats to internal validity correspond to the causation relationship between the dependent and independent variables (Haegele & Hodge, 2015; Orquin & Holmqvist, 2018). The common theme across these types of validity threats is the attachment to experimental (and quasi-experimental) study designs wherein evidence

produces as a result of an experiment or conclusions emanating from the results of an experiment (Marcellesi, 2015; Haegele & Hodge, 2015; McKibben & Silvia, 2016). My study was neither an experimental nor quasi-experimental design, and therefore these specific validity arguments are unnecessary.

Statistical conclusion validity. All quantitative studies, however, require discussion pertaining to threats toward statistical conclusion validity or the use of proper statistical analyses and methods when calculating the relationship strength between variables (Petursdottir & Carr, 2018; Tengstedt, Fagerstrom, & Mobekk, 2018). The covariation between the dependent and independent variables is the concern for statistical conclusion validity when reporting a difference in correlative effects where none exists (Type I or false positive) or the opposite (Type II or false negative), reporting no correlation where one does exist (Millner, Lee, & Nock, 2015; Tengstedt et al., 2018). The threats to statistical conclusion validity include low statistical power, violated assumptions of statistical testing, heterogeneity of the units under study, error rate problem, and a restriction of range (Petursdottir & Carr, 2018; Tengstedt et al., 2018).

Low statistical power. Relates directly to the sample size and could impact if the sample is too small to effectively draw conclusions or if there is too much group variability and apply mainly to inferential statistics and can be mitigated by correctly determining participant requirements and narrowing the variations in participant relationship to the dependent variable (Petursdottir & Carr, 2018). For my participant sizing, I applied G*power to achieve a mathematically significant minimum size requirement (114 at .8 power for a medium effect size) in addition to an a priori sample

size calculation setting the minimum number of required participants at 118. Green (1991) recommends when interested in discerning the beta weights a sample size of $N \geq 104 + k$, where k is the number of predictor variables, equating to 113 in my study. Additionally, the focus participant pool will consist only of those in a position to determine the future of cloud engagement for their respective organizations, thus narrowing the variability of the group. The effect size relates directly to the degree of relationship across the variables. A medium effect size is adequate when performing research focusing on technology acceptance or adoption models (Bosco, Aguinis, Singh, Field, & Pierce, 2015; Eisend, 2015; Šumak, & Šorgo, 2016).

Violated assumptions of statistical testing. Violated assumptions occur when conclusions are drawn incorrectly based on the data collected, perhaps through identification of patterns early in the process and never passed through statistical measure and is also inferential as it involves over or underestimating the significance of an effect (Petursdottir & Carr, 2018). Properly defining the requirements for all applicable testing that are intended for use is a means of prevention and employing non-parametric tests that do not force any distributional assumption (Stroustrup, 2018; Holgado-Tello, Chacon-Moscoso, Sanduvete-Chaves, & Perez-Gil, 2016).

Heterogeneity of units under study. The greater the diversity of individual participants, the more defined an impact to the interpretations of results through obscuring valid relationships and therefore conceals or obfuscates cause-effect paradigms and is most impactful when multiple series of data collection occur with an alteration not the group dynamic (Petursdottir & Carr, 2018; Yanagida, Strohmeier, & Spiel, 2016).

The study did not investigate cause and effect, nor will it iterate over a period using the same or dissimilar groups. Each participant equates to another as decision-makers for their organizations.

Error rate problem. The error rate problem originates from a temptation by researchers to present only that data which is statistically significant, also termed dredging or fishing, that produces omitted variable bias (Gundry & Deterding, 2018). Additionally, following analysis on data sets without an a priori hypothesis or explicit research design, increases the opportunity for dredging, a type I error (Ibiamke & Ajekwe, 2017). Ensuring adequate power and better construction of the survey measurement instruments and increasing the number of questions on a scale (Ibiamke & Ajekwe, 2017). My study, to reduce bias, included multiple questions from reverse perspectives which will also increase the scale set and reduce situational distractions.

Restriction of range. Specifically, with the independent variable, a restriction of range or a reduction in possible values restricts clarity that weakens correlation through reduced variability (Petursdottir & Carr, 2018; Zarit, Bangerter, Liu, & Rovine, 2017). Utilizing questionnaires that previously received validation is a primary means of ensuring appropriate testing, albeit modification may introduce restrictions that must be considered as beyond normal distributions and therefore, appropriately analyzed (Lewis et al., 2017). For my study, I founded my survey on several previously validated designs and ensured maximum variability across the independent variable contexts.

To ensure maximum generalizability across other or larger populations, obtaining a large number of cases or participants is essential (Aurenhammer, 2016). Returning to

power recommendations for minimum samples sizes, establishing a minimum range of 114 for medium effect upwards of 166 for a large effect produces an adequate number of subjects to generalize the results. Additionally, two modifiers were included in the survey instrument as they relate to organizational contexts: FS and SC. The two descriptors provided ample control measures for examining the data from the only variations in perspective as each participant fulfills the same role and responsibility regardless of geographic location. Probabilistic or random sampling ensures generalizability of results via a minimization of bias potential and reduce confounder influence (Haegele & Hodge, 2015; Palinkas et al., 2015). A random sample of the target population to ensure adequate representation across each sector and size reduced any risk to generalization.

Transition and Summary

The intent of my study was to investigate the relationship between specific security threat vectors and the impact on cloud adoption decision-makers within a wide array of business types and sizes. The results provided a hierarchical notation regarding the importance of each to provide a guideline aligned to practitioners for research, development, and mitigation of threats to achieve greater adoption rates. In the previous section, I restated the purpose of the study and discussed my role as the researcher to include detailed information on my involvement with the subject matter and the ethics necessary to engage such a project. I presented the strategies I employed to engage with a distinct participant pool and what will constitute a valid group as it aligns with the research question. I provided the research methodology I chose (quantitative) and briefly

discussed how it compares with the alternatives (qualitative and mixed methods), justifying my methodology decision. In addition, I offered justification on the research design to align with the nature of the study (non-experimental correlation), providing ample validated and peer-reviewed sources to support my decision. Next, I described the participant population and substantiated the alignment with the intent of the research query, as well as the method to derive the appropriate number of participants to validate the results. I discussed the instrumentation, approaches, scale, and the conceptual measurement data, while indicating approval from prior authors of existing instruments to replicate their survey methods. I also noted the techniques for data collection and validated the process, followed by an in-depth discussion on the statistical analysis method including a defense of the chosen option and a means of identifying both assumptions and mitigating potential for errors. Study validity was proposed, wherein I described threats to validity and focused on the means to reduce the possibility of exploitation.

The next section provides the data and derived analysis from this quantitative correlational study. I present the findings and discussed how they apply to professional practice including the implications for social change. The recommended actions for practitioners and further research for scholars will preface any reflections I have looking back on the study and the process.

Section 3: Application to Professional Practice and Implications for Change

I utilized a quantitative correlational method to analyze and determine the existence of relationships between the predictive independent variables ST, AH, DP, MI, DL, SP, RC, and the dependent variable, executive decision-makers' adoption intention. The following is a presentation of the binary logistic regression analysis and descriptive statistics. The data retrieved from the online survey instrument provided the foundation for this analysis.

Overview of Study

The intent of this quantitative correlational study was to discern the existence and depth of relationship between executive decision-makers' intention to adopt cloud computing infrastructure for their organizations and the impact of specific security concerns on that decision. Specifically, I measured the relationship between ST, AH, DP, MI, DL, SP, and RC against the decision to invest in cloud. I utilized two methods to determine participant size requirements. The first was G*Power in which I performed an *F* test with an effect size of .15 and the number of predictors (7), and power ranging between .8 (80%) and .95 (95%). The result was a required pool between 114 and 166. The second was to calculate sample size using the Tabachnick formula; $N \geq 50+8m$, where m is equal to the number of independent variables. The derived result was 122, aligning with the findings in G*Power. I received 290 responses from a requested pool of 2,741 executive decision-makers across the United States over a 9-week period resulting in a 10.6% response rate. After pruning incomplete and incorrect responses, I was able to utilize 261 valid responses for the survey, exceeding my minimum

requirements. I performed binary logistic regression testing on the survey data. The results indicate that while all of the predictors were influential as security concerns impeding adoption, some were significantly more impacting.

Presentation of the Findings

In this section, I describe the statistical tests, variables, intent, and how each relates to the hypotheses utilizing relevant descriptive statistics to ascertain assumptions. Of the 290 responses I received, four were incomplete, thus violating MAR, MCAR, MNAR, and three were completed in less than 30 seconds; the average response time was 4 minutes and 29 seconds. Another 22 were deemed ineligible for completing the survey with the same Likert variable chosen across each of the response categories. I had intentionally created similar queries in reverse for each of the focus areas to capture such. As I was able to achieve a greater response rate than necessary, I opted to eliminate these responses, rather than impute variables for those missing in addition to the incomplete and ineligible responses, resulting in a total of 261 valid responses.

Descriptive statistics indicated that the respondents represent industries across the spectrum, with IT firms representing 23.4%, financial services at 13.4%, manufacturing, and professional services both indicating 8% (see Table 2). Within the scope of firm size, respondents reporting medium were the highest percentage (28%), while large was the least at 11.9% (see Table 3). The technical knowledge of impacting factors indicated a large number of executive decision-makers were at least partially sure what each vector entailed, notably all exceeding 20% for absolutely sure and 40% for relatively sure (see Table 4).

Table 2

Representation of Firm scope Among Respondents

Firm Scope	Frequency	Percent	Cumulative Percent
Construction	19	7.3	7.3
Education	9	3.4	10.7
Energy/Utilities	7	2.7	13.4
Financial services	35	13.4	26.8
Government	3	1.1	28.0
Healthcare	22	8.4	36.4
IT	61	23.4	59.8
Manufacturing	21	8	67.8
Professional services	21	8	75.9
Real estate	11	4.2	80.1
Retail	18	6.9	87.0
Telecommunications	5	1.9	88.9
Travel/Hospitality	5	1.9	90.8
Wholesale distribution	6	2.3	93.1
Other	18	6.9	100.0
Total	261	100.0	

Table 3

Representation of Firm Size Among Respondents

Firm Size	Frequency	Percent	Cumulative Percent
Very small	51	19.5	19.5
Small	36	13.8	33.3
Medium	73	28.0	61.3
Medium-large	70	26.8	88.1
Large	31	11.9	100.0
Total	261	100.0	

Table 4

Percentage of Respondents Understanding the Threat Vectors

Threat vector	Unsure	Relatively Unsure	Relatively Sure	Sure
ST	6.1	16.5	53.6	23.8
AH	4.6	15.7	55.2	24.5
DP	8.0	22.3	48.6	21.1
MI	6.9	13.0	52.1	28.0
DL	5.7	18.0	47.2	29.1
RC	4.6	22.2	46.0	27.2

The individual responses for each functional threat vector (ST, AH, DP, MI, DL, SP, and RC) were recoded to create composite variables by first recoding to align the direction of each question, then computing the mean from each respondent. Similarly, the intention to adopt cloud computing and the security factors involved with such a decision were calculated to form binary indicators of adoption or otherwise.

Data Reliability

The reliability of each composite variable was validated using Cronbach's alpha. As stated by Lechien et al. (2016), Cronbach's alpha values higher than .7 indicate high reliability. Each of my coefficients exceeded this limit when means were tested in SPSS for reliability. Intention to implement cloud presented a Cronbach's alpha score of .782, and the independent variables related to the various security vectors each remained well above .7 (see Table 5).

Table 5

Reliability Statistics Using Cronbach's Alpha

Variables	Cronbach's alpha	Number of queries
Intent to Implement	.782	3
Shared Technology (ST)	.794	4
Account Hijacking (AH)	.768	3
Data Protection (DP)	.806	2
Malicious Insiders (MI)	.766	3
Data Leakage (DL)	.816	3
Service Partner Trust (SP)	.793	4
Regulatory Concerns (RC)	.830	4

Data Analysis Assumptions

In Section 2, I proposed a set of assumptions for binary logistic regression to ensure accurate analysis: normality, multicollinearity, and outliers. These assumptions are presented in this subsection.

Normality. To test for normality, a probability plot or percentage plot, assesses how closely two sets of data agree and provides a basis for understanding outliers, skewness, and kurtosis (Liang, Tang, & Zhao, 2018). Additionally, probability plots provide for standardized residual analysis by observing how closely plot points skew along a 45-degree angle in a straight line and easily indicate the appearance of outliers (Donnelly & Shardt, 2019). I performed P-P plot assessments for each of the variables and determined that in each case, normality is indicated despite slight deviation from the normal distribution (see Figure 3). I also validated multivariate normality following Käärik et al. (2016) who stated that normality exists within the threshold landscape of

between -1 and +1. The results of the skewness test indicate a -.326 (ST), .400 (AH), .221 (DP), .098 (MI), .345 (DL), .678 (SP), and .982 (RC).

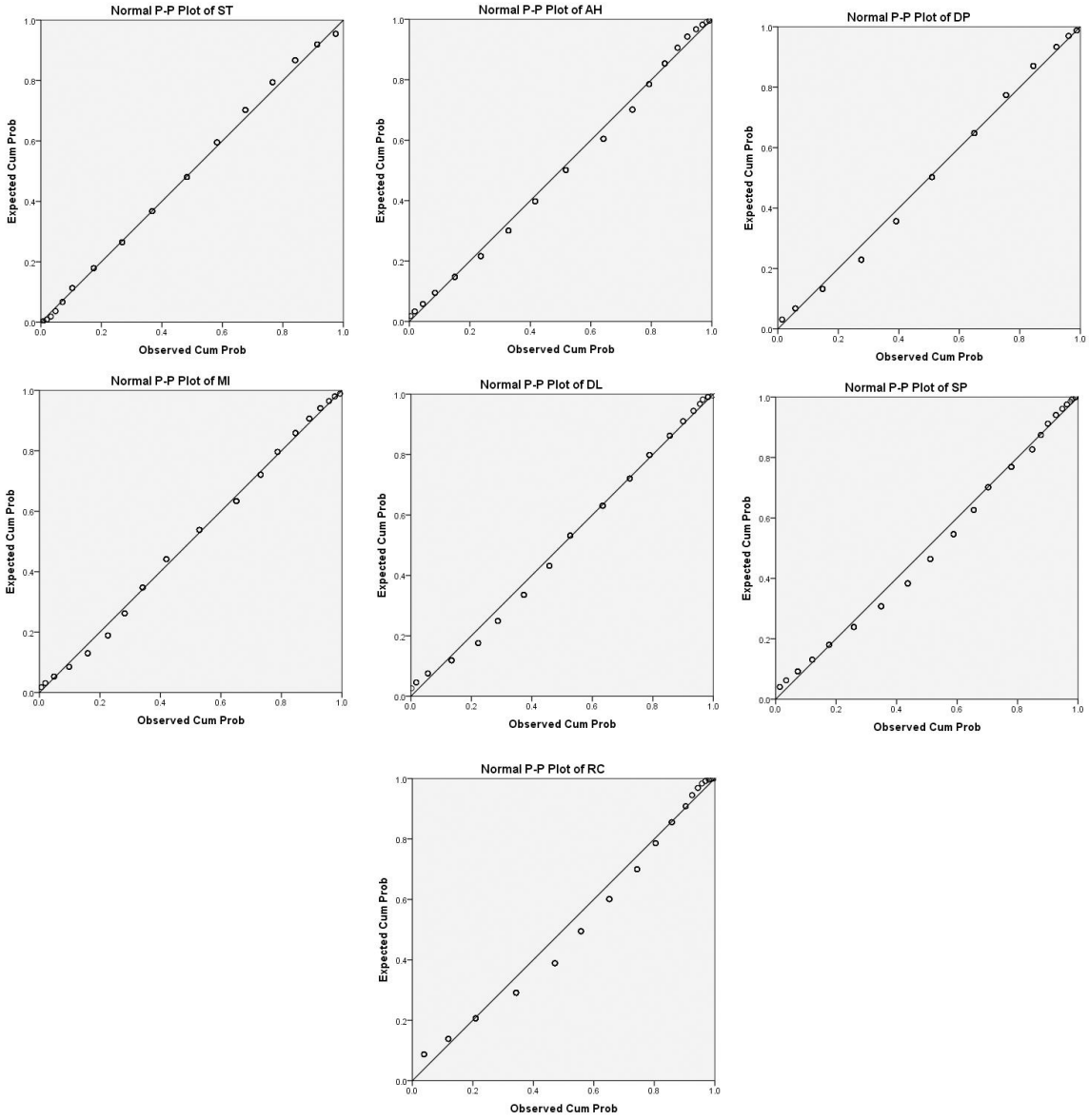

Figure 3. P-P Plots of all variables indicating normality

Multicollinearity. Multicollinearity refers to linear regression analyses; however, it remains a trusted approach for correlative independent variables that could present misleading interpretations should such a correlation exist when performing logistic regression analysis (Vatcheva et al., 2016). Utilizing methods to determine significant interconnection between explanatory variables from a linear approach is appropriate across these variables in a binary logistic regression model to ensure validity (Khikmah et al., 2016). I tested the assumption that no multicollinearity exists across my predictor variables executing a variable inflation factor (VIF) analysis within SPSS, targeting the dependent variable against each of the composite independent variables. Although Daoud (2017) suggested that a VIF above 1 but lower than 5 suggests a moderate degree of multicollinearity, the degree of impact varies by number of predictors and quantity of the data set contents. As O'Brien (2007) stated, taken into context, VIF values may slide upwards on the scale and yet still represent data sets free of multicollinearity. The application of contextual information, such as tolerance to VIF, indicates that with a tolerance level less than .20 or .10 and a VIF greater than 5 or 10 would indicate a multicollinearity issue (O'Brien, 2007). I ran iterative regression testing using my dependent and independent variables and found the closest variable to multicollinearity was SP at a tolerance level of .260 and a VIF of 3.8. The rest of the variables were well below tolerance (see Table 6).

Table 6

Multicollinearity Statistics

Variables	Tolerance	VIF
Shared Technology (ST)	.761	1.314
Account Hijacking (AH)	.525	1.904
Data Protection (DP)	.497	2.010
Malicious Insiders (MI)	.471	2.124
Data Leakage (DL)	.530	1.886
Service Partner Trust (SP)	.260	3.846
Regulatory Concerns (RC)	.380	2.635

Note. N=261, the dependent variable is Intention to Adopt (RO)

Outliers. Prior to the generation of the composite variables, I manually assessed for extreme outliers across the dataset and removed records that failed to meet the reversed query notation (repeated entries regardless of query direction). After manual interpretation, I ran an outlier test in SPSS to identify outliers using a 3.0 inter-quartile range rule multiplier, again, removing any dataset that existed outside this spectrum. According to Hoaglin and Ingewicz (1987), the 1.5 range multiplier was inaccurate approximately 50% of the time. I re-ran the same analysis on the composite sets, and while the boxplots did indicate some outliers at the 1.5 multiplier, none were indicated at 3.0, indicating the absence of outliers.

Inferential Analysis Results

Binary logistic regression offers an objective position for analyzing the impacts of multiple, and perhaps plentiful, covariates on a binary result set (Li, Morgan, & Zaslavsky, 2018). Binary logistic regression is the most applicable method to apply to a

correlation question to determine which variables are most strongly correlated to the dependent variable and has been widely employed in the analysis of influencing factors (Kohn, 2018; Lever, Krzywinski, & Altman, 2016). The use of binary logistic regression is preferred when there are two or more independent variables and the singular dependent (nominal) variable may possess one of two states (Lever et al., 2016; Kohn, 2018). My dependent variable (adoption) is dichotomous, either negative or not, as influenced by the independent variables' attributes. It was therefore necessary to generate a binary result from the captured data set indicating the impact security concerns have upon the decision to adopt cloud computing and those that do not. Rationale for conversion of Likert responses is well-documented and provides a clarity for fuzzy logic inherent in the linguistic terms commonly applied to Likert scales (Sohn, Kim, & Yoon, 2016). Differences of opinion rank highest at the leading and trailing edges of the Likert scale thus requiring a score analysis to make the differences more easily understood, which leads to more in-depth analysis (Mircioiu & Atkinson, 2017). Responses on the Likert scale that indicated systemic hesitation to adopt (3.0 and above across the means profile, derived from the "Strongly Disagree", "Disagree", and "Disagree Somewhat" queries associated with adoption factors and influencers) were placed in the impacted category, those below represented lesser degree of impact. The intent was to discern the probability that the participant displaying abject concern regarding adoption has a relationship to the seven independent variables. Recoding adjusted into a new variable set the binary value of "1" to those indicating concern, and "0" otherwise.

Binary logistic regression results indicated the model was statistically significant as the model summary displays goodness of fit that indicates how well the model predicts the dependent variable. Table 7 displays the goodness of fit statistical analysis for both Pearson and Deviance models. The Pearson goodness of fit test, $x^2(134) = 151.404$, while $p = .144$, and the Deviance goodness of fit test, $x^2(134) = 133.383$, while $p = .499$, both indicate appropriate fit. Additionally, I wanted to verify using a likelihood-ratio test that considers the log likelihood difference of nested models, that while under regularity conditions asymptotically follow a Chi-square distribution between the full regression and a reduced model (Tekle, Gudicha, & Vermunt, 2016). Significance is noted when $p < .05$, and thus, goodness of fit. Table 8 shows the significance of the final model when compared to the intercept only, indicating $x^2(123) = 133.383$, $p < 0.001$, again an indication of fit.

Table 7

Goodness of Fit

	Chi-square	df	Sig.
Pearson	151.404	134	.144
Deviance	133.383	134	.499

Note. Link function: Logit.

Table 8

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	360.438			
Final	133.383	227.055	123	.000

Additionally, I applied Nagelkerke pseudo r-squared testing to validate the fit defined by the correlation of the model's predicted and actual values ranging from 0 to 1 (Walker & Smith, 2016). The resulting value was .776, or 78%, indicating strong potential for fit. The classification table notes an 88.1% correct classification of the cases (see Table 9).

Once goodness of fit was established, the next step was to measure the impact, if any, the independent variables had upon the dependent variable to predict the outcome. I applied multiple binary logistic regression tests, determining that three of the seven independent variables did display impact to varying degrees, while the remaining either did not significantly impact the decision process or were insignificant enough of an outcome to drive decision-making (see Table 10).

Table 9

Classification Table

Observed			Predicted		
			RO		Percentage
			.00	1.00	Correct
Step1	RO	.00	108	13	89.3%
		1.00	18	122	87.1%
	Overall Percentage		48.3%	51.7%	88.1%

Table 10

Statistics for Variables in the Equation

Threat vector	B	SE	Wald	df	Sig.	Exp(B)	95 % CI for Lower	EXP(B) Upper
ST	.467	.154	9.185	1	.002	1.595	1.179	2.157
AH	-0.16	.145	.012	1	.912	.984	.741	1.308
DP	.155	.147	1.115	1	.291	1.167	.876	1.556
MI	.315	.159	3.929	1	.047	.730	.534	.996
DL	.153	.147	1.074	1	.300	1.165	.873	1.555
SP	.545	.244	4.971	1	.026	1.724	1.068	2.783
RC	.215	.201	1.147	1	.284	1.240	.837	1.837
Constant	-3.58	1.09	10.792	1	.001	.028		

Summarization of the Findings

The intent of this study was to answer the research question: What is the relationship between (a) ST, (b) MI, (c) AH, (d) DL, (e) DP, (f) SP, (g) RC, and the propensity by executive decision makers to adopt cloud computing? In response to this question, I performed binary logistic regression analyses. I began by assessing assumptions associated with binary logistic regression, indicating a successful

satisfaction of normality, outlier extraction, and an absence of multicollinearity. I executed the binary logistic regression analysis (a = .05, two-tailed) in SPSS to test against my hypotheses:

H_o: There is no relationship between (a) ST, (b) MI, (c) AH, (d) DL, (e) DP, (f) SP, (g) RC, and the propensity by executive decision makers to adopt cloud computing.

H_a: There is a significant relationship between (a) ST, (b) MI, (c) AH, (d) DL, (e) DP, (f) SP, (g) RC, and the propensity by executive decision makers to adopt cloud computing.

The statistical analysis discerned the theoretical conclusions to be valid and significant, while rejecting the null hypothesis across the spectrum, as three of the seven threat vectors indicated significant correlation (i.e., ST, MI, and SP).

Interpretation of Results

Across the seven independent variables representing various, but distinct threat vectors, only three showed significance for contribution of impact against the decision to adopt cloud computing. I employed a binary logistic regression model to determine significant relationships between the dependent and independent variables. The model as an equation is $p = \frac{\exp(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots \beta_z X_z}{1 + \exp(\beta_0 + b\beta_1 X_1 + \beta_2 X_2 + \cdots \beta_z X_z}$, which resembles bivariate logistic regression, save for the inclusion of multiple covariates and a dependent variable. In this instance, the probability of declining cloud is indicated by p, X_1-X_z are the independent variables, and β_0 - β_z are the regression coefficients. For this study, the final predictive

model was: $p =$

$$\frac{\exp(-3.580+(.467xST)+(-.016xAH)+(.155xDP)+(.315xMI)+(.153xDL)+(.545xSP)+(.215xRC)}{1+\exp(-3.580+(.467xST)+(-.016xAH)+(.155xDP)+(.315xMI)+(.153xDL)+(.545xSP)+(.215xRC)}$$

Impacting. ST was the strongest correlation, $x^2(1) = 9.185$, $p < .01$, followed by SP as the median, $x^2(1) = 4.971$, $p < .05$, and MI remaining, $x^2(1) = 3.929$, $p < .05$. While positive coefficients indicate relationships that are positively sloped, that is, as one increases so does the other, negative relationships are inverse; while one increases the other decreases (Schober et al., 2018). Each of these correlations were indicated by positive coefficients (ST=.47, SP=.55, and MI=.32), indicating that in 47% of the cases, ST represented a degree of impact negating adoption, while SP accounted for 55%. MI represented 32% impact to the decision of adoption.

Non-impacting. AH was the least influential and not a significant impact, $x^2(1) = .012$, $p > .05$. DL was moderately nullified, $x^2(1) = 1.074$, $p > .05$, and almost equivalently so DP was similarly non-impacting, $x^2(1) = 1.115$, $p > .05$. RC was the closest to significance, $x^2(1) = 1.147$, $p > .05$. It is interesting to note that AH produced a negative coefficient, indicating that for each unit of increase of concern over AH, there was a decrease in the impediment for adoption. Which this may seem counterintuitive, consider the business perspective. Approaching this from a business perspective, as again, the participants were all executive decision-makers, the threat of AH from the corporation would decrease if the enterprise migrated to a cloud provider, limiting the degree of impact from its own organization. Perhaps more to the point the legal ramifications fall to the provider, thus relieving the enterprise from legal burden or a result of misunderstanding of the terminology (Bokhari et al., 2016).

I chose to include in this model all variables including those that were deemed non-impacting or possessed no significant correlative effect. I hypothesize that the responses to this are fluid and depend greatly upon geographic boundaries. The inclusion of these variables, while not significant at this juncture, may indeed prove essential artifacts for future studies that exceed the limitations set upon this research. Additionally, the advent of hybrid cloud may involve the expansion of some of the lesser contributing factors and contraction of those considered favorable in this study. For example, an executive decision-maker opting instead for private cloud functions that inhibited their adoption under public consumption would be less inclined to be concerned about ST, but more so toward regulatory concerns. It is important for future work to establish the main contributing threat vectors in this research.

The findings suggest that executive decision-makers are inherently impacted by their concerns governing security, specifically the three vectors recognized, and that impact influences their decisions regarding the adoption of cloud computing. The results align with prior literature, noting that more than 70% of participants on a cloud adoption survey forego adoption of cloud related directly to security concerns (Balasooriya et al., 2017). Similarly, Rao and Selvamani (2015) related security factors as impediments to adoption of cloud as critical to the decision-making process for more than 70% of their survey participants. Phaphoom et al. (2015) identified the significance of structure breakdown for identifying specific security concerns based on perceptions. The origin of these perceptions is perhaps well-documented; as the perception of cloud by decision-makers is one of immature standards and procedures, with little protection mechanisms

(Kalaiprasath et al., 2017). Binary logistic regression tests executed to significantly predict the individual impact of each security-related variable on the perception by decision-makers regarding the overall security of the architectural model. That is, the tests elucidated a response to detect the propensity of executive decision-makers to adopt cloud computing architecture in relation to specific security concerns. Specifically, that we reject the null hypothesis for ST, MI, SP, AH, DL, DP, and RC.

Theoretical Framework Discussion

I opted to perform a quantitative study, performed using a survey instrument and a target population of U.S.-based executive IT decision-makers to garner insight as to their perspectives on security as it relates to their adoption practices for cloud. To accomplish this, I applied the TOE framework, applying the various security-focused threat vectors within the three contexts of technological, organizational, and environmental characteristics. Martins et al. (2016) utilized the TOE to determine that the application of the variables into the three contexts allows for the varied perspectives upon which they draw conclusions regarding adoption practices based on perceptions. The TOE presents advantages over alternate theories because of the contexts from which the variables emanate, providing a more holistic view, both for perceptions of challenges and on implementation operation (Gangwar et al., 2015).

The implication that security is directly related to the impediments on cloud computing adoption are well-documented in a study performed to examine cloud influencers that focused on the TOE as a framework for dissecting the various contextual information (Hsu & Lin, 2016). Lippert and Govindarajulu (2006) explain for their work

on examining the correlative relationships of adoption for innovative technologies that the three contexts represent constraints and opportunities. As an example, the inclusion of organization factors, such as firm size and scope, provided of little consequence in the perceived security risks inherent in the architectural model. The only exception came from those executive decision-makers who reported IT as their firm's business focus (see Table 11). While the over-arching statistics did indicate some impact from the security vectors, a significance was present (p <.05) in analysis related to intention to adopt and that business category that did not exist in the others (Scope7). FS has no impact on analysis across the various SC and threat variables.

Table 11

Statistics for Variables in the Equation (RO – SC)

Firm Scope				95 % Conf Int.	
	Wald	df	Sig.	Lower	Upper
Scope1	1.481	1	.224	-.519	2.219
Scope2	.089	1	.766	-1.465	1.990
Scope3	.518	1	.472	-1.150	2.486
Scope4	2.062	1	.151	-.328	2.124
Scope5	.039	1	.844	-2.350	2.875
Scope6	.743	1	.389	-.749	1.924
Scope7	6.079	1	.010	.372	2.684
Scope8	3.279	1	.070	-.102	2.589
Scope9	2.360	1	.124	-.290	2.391
Scope10	.234	1	.629	-1.208	2.000
Scope11	.131	1	.718	-1.160	1.685
Scope12	.122	1	.727	-2.953	1.991
Scope13	.122	1	.727	-2.853	1.991
Scope14	.452	1	.397	-.822	1927
Scope15	.138	1	.764	-1.298	1.964

Without the ability to focus on SC and FS as ancillary correlative information, such as inherent in the TOE, that slight indication may have been missed or

misinterpreted. As Alkhalil et al. (2017) stated, the ability to provide analysis at any size or scope as juxtaposition when discussing demand or appetite for innovation more clearly defines the relationship. Provided the focus on IT firms indicates a higher degree of comfort with security-related concerns, one might assume communication and training that exist within that paradigm should be the focus for customers of cloud. In this study, the appearance of minute concern within the context of organizational scope for IT firms suggests, as Ray (2018) notes, a specifier in determining the degree of risk acceptance within an organization based on practice.

Numerous papers note the value expressed in dissecting the factors under study into the three contexts. The technological context focuses entirely on technologies and their impacting characteristics (Chiu, et al., 2017; Tornatzky & Fleischer, 1990). For the purpose of this paper, I followed the example from Klug and Xue (2015) that applied compatibility and complexity as over-arching themes. Access controls are considered akin to the technological stack when considering cross-platform capabilities (Alassafi et al., 2017). Fraudulent techniques and malicious encryption denote both AH and data protect mechanisms as technological constructs as well (Albadrany et al., 2018; Gangwar et al., 2016; Kazim et al., 2015). The sole technological influencer in my study was ST or multitenancy, which can also be attributed to virtual machine management, arguably a potential future inclusion into the environmental context. Raj, et al. (2017) found that virtual machine management was a common ingress mechanism, while Islam et al. (2016) found that virtual machine mismanagement constitutes a cross-platform security

concern. Regardless, my study confirms that this is a notable context of concern for decision-makers.

Following the explanation of the technological construct and the possibility of inclusion for future studies of ST into environmental context, we find the majority of these patterns contained within the environmental context proved significantly impactful. The environmental impact focuses on dimensions of influence outside the scope of technological consideration dealing with the complexity of operations and consumption of services (Hoti, 2015). Influencers such as MI and SP conform to the environmental aspect via the focus on the operational aspects that include wider participation in management and service landscape (Jegadeeswari et al., 2016; Sohal et al., 2018). Similarly, RC and DL focus on network pathways and reporting structures of the cloud architecture, to include the business operations frameworks (Cayirci et al., 2016; Ray, 2016). Alassafi et al. (2017) specify the inclusion of these attributes in the environmental context of the TOE. For this study, the two influencing factors, SP and MI relate to the environmental structures inherent in a provider-customer relationship.

Current literature. The following section provides updated information from relevant and current literature published subsequent the literature review in Section 2. In each case, the studies remained consistent with prior literature, each indicating security as a significant contributor to the rejection of cloud computing, and several noting the lack of impact related to FS or SC. Each employed the TOE as a framework for conducting the research, albeit some extending the TOE into newly classified branches of methodologies.

A recent publication by Matias and Hernandez (2019) employed the TOE framework in their study on the adoption of cloud computing and found technological and environmental issues were equally impactful on key decision-makers' intention. Similarly, they found that firm size and scope were not significant contributors to intention, and perceived benefits were well-known across the participant pool (Matias & Hernandez, 2019). The authors did not dissect security, but as in previous works, coalesced all the factors (albeit well-defined in their paper across the same aspects in this study) into a single attribute within the technological context (Matias & Hernandez, 2019). A key differentiator was their discovery that RC were a significant contributor to the decision process, and one can hypothesize that the dissimilarity is geographical as their study includes foreign business entities where privacy laws protecting individuals are more stringent. The authors found that engaging with the TOE construct enabled them to assess, explore, and understand the factors related to adoption of cloud computing (Matias & Hernandez, 2019).

Data security and risk were the significant contributors in another recent study as to the lack of adoption for cloud computing, albeit again, security converged all security and data risk attributes that also employed the TOE (Juma & Tjayanto, 2019). The TOE in this study was extended to include aspects of the TAM and the I-E (Internal and External model) called the ITOTAM that utilizes the contexts inherent in the TOE with the additional facets of the TAM and the I-E as extensions (Juma & Tjayanto, 2019). Half of the factors presented in the environmental context were significantly impactful to the outcome of adoption intention amongst the participants. SC and FS were not included in

this study, as the participant pool was limited to universities, although RC were also found to be significant, though less so than security. As this study emanates from Zanzibar, it too found RC as a significant contributor to the delay in adoption of cloud computing; lending credence to the supposition that foreign enterprises are more focused on such considerations because of the stringent policies native to global considerations.

A significant barrier to the broad adoption of cloud computing involve security concerns, as noted by researchers examining business enterprise in Lebanon, garnering the largest noted barrier to adoption (Sabbah, Trabulsi, Chbib, & Sabbah, 2019). The authors also included within the environmental context, the service partner aspect, which they labeled as 'contract', noting the outsourcing nature of the paradigm, noting the second-largest barrier to adoption in their study (Sabbah et al., 2019). RC were insignificant contributors, though that may have more to do with the notably weaker data privacy laws within Lebanon only recently enacted in 2018 (Privacy International, 2019). The study, like the majority of others within my literature review and this subsequent addendum, noted that SC and FS have little significance on the adoption of cloud computing, while all perceive the value from a cost and ease of use perspective as beneficial (Sabbah et al., 2019). The contextual organization varies slightly from prior models, or perhaps it is a language difference, as the term 'characteristics' seem to apply to perceived inherent attributes of cloud, while 'advantages and disadvantages' often refer to the perceived security concerns, which can be interpreted as a technological construct. The conclusion drawn in this study indicate a need for SMEs (practitioners) to

help minimize the perceived challenges to cloud computing adoption and thereby eliminate the barriers (Sabbah et al., 2019).

Aligning well with my study is one that focuses on the healthcare industry within the United States and the lackadaisical approach to cloud computing adoption. Gao and Sunyaev (2019) extracted various aspects of security from the technological aspect to instead focus on these derivatives independently and therefore, assign security and privacy into a new context; data/information. These considerations proved that the security-focused aspects were contributing factors to the dearth of cloud computing adoption, in addition to an equivalent of SP, which they deemed as outsourcing of IT within the environmental context (Gao & Sunyaev, 2019). The research found that security and privacy issues, within the healthcare industry pose a specific and substantial impact and mention within the dataset the concern over misuse of data by personnel, or MI action (Gao & Sunyaev, 2019). Their conceptual framework that incorporates the TOE with these new categories, while not in extant literature, does showcase the value of the TOE standard as the intent is to align the variables in a contextual manner.

Applications to Professional Practice

The intent of this quantitative correlational study was to indicate the presence of a relationship between executive decision-makers intent to adopt cloud computing and several key threat vectors related specifically to security; ST, AH, MI, DL, DP, RC, SP, with additional conditionals, SC and FS. The executive decision-maker's intent to adopt cloud represented the dependent variable, while each of the security vectors indicated an aspect of security for the independent variables. The purpose was to prove the

relationship existed and then to signify to what extent each was impactful, thus providing practitioners with a roadmap to increase awareness and to mitigate concerns thus enabling greater acceptance. It is widely accepted, based on the extant literature, that conditions such as ease of use and lower cost for operation are well-understood among this demographic. Instead, the focus was on the barriers to greater adoption, which again, from extant literature were well within the realm of security and security-related controls.

I utilized a survey instrument to collect data from only those in an executive position wherein the responsibility lay to decide upon the future technological direction. These roles included CIOs and executive IT director positions across a distributed field of corporate, government, and NPOs. One of the key data points form this study was the lack of significance the SC had upon any of the factors, with the sole exception of firms whose business focus is IT. The fact that overall, IT firms were more inclined to adopt and less concerned about security implications may promote the concept that communication and education are important for wider adoption.

Multitenancy, or ST were indicated as the largest contributor to perceived vulnerability, and thus the greatest detractor to adoption. The indication that the sanctity of one's platform is only as strong as its weakest link is prevalent and one that practitioners should consider prior to engaging with executive leadership. Service providers should focus their attention to resolving the perception of vulnerability, either via a training program targeting executive leadership, or mitigation of actual cross-platform exposure. Enhancing the virtualization framework using containers, for example, is a means of extricating segments of workloads within a common

organizational paradigm and include such enhancements as containerized networking to reduce cross-contamination from a flow perspective (Kim, et al., 2016).

SP as the second significant factor as an impediment to adoption involves the maturity of the platform and provider. The concept of migrating services to a provided cloud operation is a form of outsourcing, even considering IaaS as a token delivery paradigm, wherein most of the services are still maintained by the business, the foundational aspects are hosted elsewhere. Despite the continuous availability nature of cloud, there remains doubt on the part of executives to entrust their critical operations to any platform outside their span of control.

As Nayar and Kumar (2018) noted, increasing efficiencies at scale while decreasing costs of architectural considerations is a challenge to IT enterprises. Cloud computing offers business opportunities to improve services and service offerings equal to large enterprises with greater scalability, ease of use, and reduced cost (Alkhalil et al., 2017; Balasooriya et al., 2017). These perceived benefits are well known and well documented means to break the status quo paradigm, namely the necessity to increase the footprint of infrastructure to accommodate extended services (Fan, et al., 2017; Rathi & Given, 2017). Conjoined with the reduction in cost for infrastructure is the associated costs of labor, such as specialized support staff (to varying degrees based on level of cloud ingress) in addition to the cost of hardware refresh over time (Senyo et al., 2016; Lo, et al., 2015). Al-Badi et al. (2017) found that nonprofits, to include educational enterprises, especially benefit from these advancements to offer greater scope of services to their respective consumers. Quantifiably, the tangible benefits are clearly understood

at the executive tier, to include continuously available operations (Akkaya et al., 2016). However, there is a measure of annotated risk uncertainty that creates a degree of bias and defers the adoption of new technology (Antons & Piller, 2015).

As noted by Rao et al. (2015) and Senyao et al. (2016) in two disparate studies, perceived security risk accounted for 70% of critical factors when executives consider the viability of cloud computing adoption. Wu (2016) extended this research to prove that biases reflecting these security concerns exacerbated the lackadaisical response to adoption. Phaphoom et al. (2015) found that a degree of ambiguity or lack of transparency regarding control procedures accounted for much of the negative implications. Kreslins et al. (2018) derived that perceptions of security, including a lack of confidentiality controls and regulatory or policy considerations were significant drawbacks. It is vital that providers offer a means to deflate negative perceptions to specific areas of concern to promote a greater adoption rate (Arpaci et al., 2015).

The data reflected in this study promote the attention to detailed dissection of specific perceived risks, even if those risks may not truly exist but require, instead, education and communication to relieve those perceived concerns. The difference between IT firms and non-IT firms in this study provide a basis for enhancing the understanding of perceived threats as a mediator between adoption or lack thereof. Those that were impacted offer insight to the most highlighted vectors of concern for executive IT decision-makers; a roadmap for practitioners to follow, mitigate, and achieve greater adoption rates.

Implications for Social Change

The implications for positive social change include enabling NPOs and not-for-profit organizations access to the same enterprise-class architectures currently in use by only those entities large enough to afford on-premises workloads. Decreased costs and required specialists allow such cost-focused operations to focus on development as opposed to management of resources. A reduction in the IT budget allows for the more effective use of such funds toward the goals and intentions of the organization, thus offering two prime benefits: increased reach and capability as well as reduced costs for overhead.

Another benefit to social change, specifically with nonprofit and not-for-profit organizations, is the cloud enablement of cognitive analytics and big data. Analytics provides organizations with the capability to understand and respond to consumer needs, garnering market share, or engaging more meaningfully with patrons (Tan, Zhan, Ji, Ye, & Chang, 2015). Analysis of structured and unstructured data from social media outlets provide businesses with essential data used to navigate customer needs and maximize efficiencies; the same would be available for NPOs (Feng, Du, & Ling, 2017).

Investment and enablement of cloud operations also reduce the carbon footprint an entity produces for similar or extended operational capabilities (Singh, Mishra, Ali, Shukla, & Shankar, 2015). Singh et al. (2015) found that cloud enablement reduced generated carbon emissions by virtualizing their entire supply chain while lowering their TCO.

Recommendations for Action

Gangwar and Date (2016) indicate that it is the perceived difficulties related to security concerns are the largest impediment to adoption and without procedural mitigations or standardization in the form of researched means to alleviate those concerns, all relative advantages are moot. The findings in this study, that specifically target security vectors and place no emphasis on the already well-known advantages, indicate that three risk areas require the greatest attention: ST, MI, and SP. Development of research paradigms that focus on these critical areas will lead to either mitigations or enhance transparency thus enabling greater adoption. IT practitioners, for both providers and enterprise consumers, should drive these considerations and enhance the ensuing communication.

The first recommendation is to address concerns regarding the security ramifications of ST. The lack of isolation between consumers operating within the confines of the same resource, thus creating a dependency across multiple enterprises in the form of virtual machines originating within the same platform space, is a cause for concern (Hussain et al., 2017; Indu et al., 2018). Showcasing a means of driving protection in these shared platform experiences could provide consumers with greater confidence in cross-tenancy vulnerabilities. An example may be to introduce container mechanisms with software-defined networking stacks to further isolate not merely the operations stack but also the ingress/egress flow. The goal of practitioners is to place emphasis on defining mechanisms through considerable documentation based on individual operations research to alleviate these concerns by potential consumers. A

primary means of communication of these findings will be to draft an architectural platform white paper within the Open Group framework (TOGAF) to address such operational considerations from a technical perspective and educate architects on executive-level perceptions.

Regarding MI, the impetus is placed both upon providers and IT staff within the consumers organization to draft user-level isolation requirements. Whereas MI reflect high priority within the CSA, the perception of risk is exponentially increased across virtualized entities (Kalaiprasath et al., 2017). The model inherently increases the number of active participants within the context of a service operation when an unknown number of provider assets maintain access to an enterprise's platform space (Aldossary & Allen, 2016). It is therefore the responsibility of practitioners within the provider complex to formulate a means of limiting access and demonstrate these protection mechanisms to potential customers. Accordingly, this is not precisely a business model, but rather a technical one, as the system will need modifications to allow more granular access controls above and beyond standard access control lists. A means to combat this is a requirement to always force escalation of privilege access. Ensuring operations are self-documenting on disparate systems for which the architects and SMEs have no access create log data for a mechanism such as a file analysis device to alert when changes occur. Similarly, the consumer's IT staff should require of the provider a means to configure via specification a means to limit consumer activity within the day-to-day operations platform. Using a tool such that provides finite control sets based on externalized parameters to individuals from the client is a means to combat this effort.

Trust implies more than transparency regarding the acquisition of, and access to data streams. SP also includes hiring practices and governance, all of which is modified by the reputation of the provider (Sidhu & Singh, 2017). Factors such as longevity of service and future architectural decisions by the provider promote or degrade such trust by a consumer (Alassafi et al., 2017). The implication that a provider must have been in operation for an extended period of time does not confer maturity of services, rather that the provider displays a maturity in the means of promoting said service and the platform upon which the service operates (Ali et al., 2015). The best platform for dissemination of this information is communication, represented by various means of delivery. Keynote addresses within the Open Group Architecture board specializing in cloud operations to devise standards of best practice design for over-arching template creation, and the modification of these standards at each provider organization that meets or exceeds these fundamental foundations. Furthermore, each provider should enable an architectural review board to promote compliance and a transparent means of executing actions in a repeatable and agile manner on the part of senior SMEs and engineers for the organization to adopt and then communicate. Such items should include visible roadmaps for architectural decisions, narrow in scope for the immediate future to include mature methods of delivery and execution and extending to broad design directions that could then narrow to specify conditionals.

Recommendations for Further Study

As detailed in Section 1, limitations may impact validity and therefore decrease generalization across the entire industry for the reported result set (Greener, 2018).

Using nonprobability sampling, while necessary to achieve the specific demographic, lacks contextual data (Quick & Hall, 2015). These limitations, however, provide a foundation for further study, as a qualitative interview process to further expand the nature of the individual security focal points from a direct conversation with executive decision-makers. I do not believe a future study that focuses on the interpretation and perceptions of a specific role within an organization can reduce the limitation of nonprobability sampling to zero. Randomized sampling is simply unattainable when one specifies a particular subset. Nor can one reduce the impact of dishonest responses in a future quantitative study. Therefore, a qualitative study, wherein the context of responses is inclusive toward the finalization of data would provide useful insight that this study could not. Additionally, I found that firm scope was only relevant for IT firms, who may have access to a greater degree of information that enterprises whose operations do not drive IT would not. Therefore, a separate study eliminating IT firms, or comparing IT firms against others would confirm or deny that hypothesis.

I discovered another variance between extant literature and my study; the difference between domestic (United States) and foreign operations regarding regulatory concerns. The discovery evokes a noted delimitation from section 1, wherein a note the geographic boundaries of the United States and the potential for variance outside this scope. My study did not show regulatory concerns as a prime demotivator for adoption of cloud computing initiatives, but literature derived from external studies proves otherwise. It would be valuable to drive information across different geographical boundaries to determine if tighter restraints placed upon enterprises in other countries

proves a differentiator among the hierarchy of concerns by executive decision-makers. For example, the General Data Protection Regulation (GDPR) is far more stringent than current regulatory measures in the United States and could provide greater insight toward these concerns for European operations.

Reflections

At the risk of sounding cliché or banal, I found the entire doctoral process to be an enlightening experience. As in life or business, once is faced with seemingly insurmountable odds and yet, when executed methodically and with perseverance, one can accomplish this daunting task. While the hurdles never seem to cease, neither should the drive to vault over them. The more time I spent in academia, the more I realized it was analogous to life, and business, and everything else we face in our lives. No problem is too large if one is relentless and focused, not to mention garners invaluable aid and mentorship along the way, which is often the hardest part of any exercise, asking for it.

I began this expedition with wide-eyed hope and excitement, and while I refuse to say I became more cynical, I do think I tempered that exuberance with wisdom, wrought from places I did not expect. Having spent more than 20 years in the field as an engineer and executive architect and having arguably designed some of the first workload-based operations emulating what would become IaaS and PaaS, I still found plenty to learn. It is truly about the journey and not the destination. I have built some of the first continuously available systems and defined security operating standards across a diverse spectrum, but the doctoral processes is less about what you think you know and forces you to examine what it is you do not.

It is because of this experience I now realize that my biases toward cloud and security were evident, and subsequently extracted during the entire doctoral process. If there is one lesson to be learned, it is to embrace one's own predilections toward bias and having acknowledged them, move on. While I understood, from personal experience having sold the idea of cloud even before we called it cloud, the many issues surrounding a consumer's unwillingness to invest in this new paradigm, it is a different thing to prove it in a repeatable way. Ironic, given that repeatable processes are the very foundational aspects of architectural and security design specifications, that I would assume otherwise for academia.

While I can unequivocally state that my involvement in this study did not produce any effect on the participants, as I have no way of correlating the completed surveys with who executed them, I do think that the results of the study will have an impact on them professionally and perhaps personally. Throughout my literature review, I found no evidence to support that any prior work had specifically targeted those in an executive role who decide on future direction for their enterprises. Perhaps several took the initiative subsequent to the completion to assess their knowledge of these artifacts and the impact their own biases may have on their decisions. Certainly, if practitioners heed the data found within, the road to cloud adoption will become easier to accomplish.

Summary and Study Conclusions

Security-related concerns are the single most prevalent cause of cloud computing rejection across a diverse enterprise landscape (Balasooriya et al., 2017; Khan & Al-Yasiri, 2016; Selvamani, 2015; Senyo et al., 2016). Despite the acknowledgement of the

relative advantages of migration to cloud, such as ease of use and cost reduction, more than 70% of enterprises forego adoption based on the perception of insecure operations (Alkhalil et al., 2017; Balasooriya et al., 2017; Gangwar & Date, 2016; Gao & Sunyaev, 2019). There is an inclination to follow the "herd mentality" based entirely on perceived realities, especially where risk is concerned, to drive decisions (Botzen et al., 2015; Sand & Nilsson, 2017). Perceptions can bias decisions, formulating from inaccurate or easily manipulated data, manifesting as real threat vectors (Haghani & Sarvi, 2017; Liu et al., 2015). Therefore, the problem is not a question of what is, but what is perceived and who is perceiving it. Executive decision-makers are the roles responsible for directing the architectural course for their enterprises and yet, I was unable to locate a previous study that interpreted their perceptions regarding the negatively impacting criteria for adoption.

My analysis was conducted by obtaining 261 responses, all from executive decision-makers, and uploaded into SPSS to determine the frequency and descriptive statistics related to singular tiers of threat vectors as they relate to the intention on adoption of cloud computing. A rejection of the null hypothesis was found for three of the seven vectors: ST, MI, and SP. I find it an imperative that we, as practitioners listen to this often-neglected segment to discern what artifacts impede progress on the adoption of cloud, or any new technological effort that requires executive coordination. The intent of this study is to prove a direction for practitioners to research and, if necessary, mitigate or communicate their findings to prospective consumers to alleviate these concerns and thereby extend cloud adoption. When cloud becomes ubiquitous, the capabilities will expand exponentially.

References

Abutabenjeh, S., & Jaradat, R. (2018). Clarification of research design, research methods, and research methodology: A guide for public administration researchers and practitioners. *Teaching Public Administration,* 36(3), 237-258. doi: 10.1177/0144739418775787

Adams, P., Prakobtham, S., Limpattaracharoen, C., Suebtrakul, S., Vutikes, P., Khusmith, S., … Kaewkungwal, J. (2017). Ethical issues of informed consent in malaria research proposals submitted to a research ethics committee in Thailand: a retrospective document review. *BMC medical ethics, 18*(1), 50. doi: 10.1186/s12910-017-0210-0

Afendulis, C. C., Caudry, D. J., O'Malley, A. J., Kemper, P., & Grabowski, D. C. (2016). Green house adoption and nursing home quality. *Health Services Research*, *51* (Suppl 1), 454–474. doi:10.1111/1475-6773.12436

Agarwal, A., Siddharth, S., & Bansal, P. (2016, March). Evolution of cloud computing and related security concerns. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-9). IEEE. doi: 10.1109/cdan.2016.7570920

Ain, N., Kaur, K., & Waheed, M. (2015). The influence of learning value on learning management system use: An extension of UTAUT2. Information Development, 32(5), 1306-13216. doi:10.1177/0266666915597546

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, N.J: Prentice Hall

Akkaya, M., Sari, A., & Al-Radaideh, A. T. (2016). Factors affecting the adoption of

cloud computing based-medical imaging by healthcare professionals. *American Academic & Scholarly Research Journal*, *8*(1), 13-22. Retrieved from http://www/aasrc.org/aasrj/

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics*, *34*(7), 996-1010, doi: 10.1016/j.tele.2017.04.010

Al-Badi, A., Tarhini, A., & Al-Kaaf, W. (2017). Financial incentives for adopting cloud computing in higher educational institutions. *Asian Social Science*, *13*(4), 162-174. doi: 10.5539/ass.v13n4p162

Albadrany, A. O., & Saif, M. Y. (2018). Review on security challenge faced organization based on-cloud computing. *International Journal*, *7*(6). doi: 10.30534/ijns/2018/01762018

Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*, *7*(4), 485-498. doi: 10.14569/ijacsa.2016.070464

Al-Hujran, O., Al-Lozi, E. M., Al-Debei, M. M., & Maqableh, M. (2018). Challenges of cloud computing adoption from the TOE framework perspective. *International Journal of E-Business Research (IJEBR)*, *14*(3), 77-94. doi: 10.4018/IJEBR.2018070105

Ali, F., Rasoolimanesh, S. M., Sarstedt, M., Ringle, C. M., & Ryu, K. (2018). An

assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. *International Journal of Contemporary Hospitality Management*, *30*(1), 514-538. doi: 10.1108/IJCHM-10-2016-0568

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

Alkhalil, A., Sahandi, R., & John, D. (2017). An exploration of the determinants for the decision to migrate existing resources to cloud computing using an integrated TOE-DOI model. *Journal of Cloud Computing*, *6*(1), 1-20. doi: 10.1186/s13677-016-0072-x

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics*, *35*(1), 38-54. doi: 10.1016/j.tele.2017.09.017

Amron, M. T., Ibrahim, R., & Chuprat, S. (2017). A Review on Cloud Computing Acceptance Factors. *Procedia Computer Science*, *124*, 639-646. doi: 10.1016/j.procs.2017.12.200

Anderson, B. S., Wennberg, K., & McMullen, J. S. (2019). Editorial: Enhancing quantitative theory-testing entrepreneurship research. *Journal of Business Venturing*, *34*(5). doi: 10.1016/j.jbusvent.2019.02.001

Antons, D., & Piller, F. T. (2015). Opening the black box of "Not Invented Here": Attitudes, decision biases, and behavioral consequences. *Academy of Management Perspectives*, 29(2), 193-217. doi: 10.5465/amp.2013.0091

Antwi, S. K., & Hamza, K. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management*, *7*(3), 217-225. Retrieved from https://iiste.org/Journals/index.php/EJBM

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). 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

Astroth, K. S., & Chung, S. Y. (2018). Focusing on the fundamentals: Reading quantitative research with a critical eye. *Nephrology Nursing Journal*, *45*(3), 283-287.

Aurenhammer, P. K. (2016). Network analysis and actor-centred approach—a critical review. *Forest policy and economics*, *68*, 30-38. doi: 10.1016/j.forpol.2014.12.010

Awa, H. O., Ukoha, O., & Emecheta, B. C. (2016). Using TOE theoretical framework to study the adoption of ERP solution. *Cogent Business & Management*, *3*(1), 1196571. doi: 10.1080/23311975.2016.1196571

Aziz, N. A. A., Ali, Z., Nor, N. M., Baharum, A., & Omar, M. (2016, June). Modeling multinomial logistic regression on characteristics of smokers after the smoke-free campaign in the area of Melaka. In *AIP Conference Proceedings* (Vol. 1750, No. 1, p. 060020). AIP Publishing. doi: 10.1063/1.4954625 1

Balasooriya, P., Wibowo, S., Grandhi, S., & Wells, M. (2017). The impact of security concerns on personal innovativeness, behavioural and adoption intentions of

cloud technology. *Software Networking*, *2017*(1), 265-290. doi: 10.13052/jsn2445-9739.2017.013

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations*, *61*(8), 1139-1160. doi: 10.1177/0018726708094863

Basias, N., & Pollalis, Y. (2018). Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. *Review of Integrative Business and Economics Research, 7*, 91-105. Retrieved from http://sibresearch.org/uploads/3/4/0/9/34097180/riber_7-s1_sp_h17-083_91-105.pdf

Boies, K., Fiset, J., & Gill, H. (2015). Communication and trust are key: Unlocking the relationship between leadership and team performance and creativity. *The Leadership Quarterly*, *26*(6), 1080-1094. doi: 10.1016/j.leaqua.2015.07.007

Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2016). Security and privacy issues in cloud computing. *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 896–900.

Bosco, F. A., Aguinis, H., Singh, K., Field, J. G., & Pierce, C. A. (2015). Correlational effect size benchmarks. *Journal of Applied Psychology*,*100*(2), 431. doi: 10.1037/a0038047

Botzen, W. W., Kunreuther, H., & Michel-Kerjan, E. (2015). Divergence between individual perceptions and objective indicators of tail risks: Evidence from floodplain residents in New York City. *Judgment and Decision Making*, *10*(4),

365-385. Retrieved from http://journal.sjdm.org/

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

Busse, C., Kach, A. P., & Wagner, S. M. (2017). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, *20*(4), 574-609. doi: 10.1177/1094428116641191

Caruana, E. J., Roman, M., Hernandez-Sanchez, J., & Solli, P. (2015). Longitudinal studies. *Journal of Thoracic Disease*, *7*(11), E537–E540. doi:10.3978/j.issn.2072-1439.2015.10.63

Cayirci, E., Garaga, A., De Oliveira, A. S., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing*, *5*(1), 14. doi: 10.1186/s13677-016-0064-x

Changchit, C., & Chuchuen, C. (2018). Cloud computing: An examination of factors impacting users' adoption. *Journal of Computer Information Systems*, *58*(1), 1-9. doi: 10.1080/08874417.2016.1180651

Chauhan, S., & Jaiswal, M. (2016). Determinants of acceptance of ERP software training in business schools: Empirical investigation using UTAUT model. *The International Journal of Management Education*, *14*, 248-262. doi:10.1016/j.ijme.2016.05.005

Chen, T., Chuang, T. T., & Nakatani, K. (2016). The perceived business benefit of cloud

computing: An exploratory study. *Journal of International Technology and Information Management, 25*(4), doi: 7.9/ICCPCT.2017.8074287.

Chiu, C. Y., Chen, S., & Chen, C. L. (2017). An integrated perspective of TOE framework and innovation diffusion in broadband mobile applications adoption by enterprises. *International Journal of Management, Economics and Social Sciences (IJMESS), 6*(1), 14-39. Retrieved from http://hdl.handle.net/

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2016). Managing ethical challenges to mental health research in post-conflict settings. *Developing World Bioethics, 16*(1), 15-28. doi:10.1111/dewb.12076

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65,* 334-345. doi: 10.1016/j.chb.2016.08.034

Cobb, J. A. (2016). How firms shape income inequality: Stakeholder power, executive decision making, and the structuring of employment relationships. *Academy of Management Review, 41*(2), 324-348. doi: 10.5465/amr.2013.0451

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering, 59,* 126-140. doi: 10.1016/j.compeleceng.2016.03.004

Cramer, A. O., van Ravenzwaaij, D., Matzke, D., Steingroever, H., Wetzels, R., Grasman, R. P., ... Wagenmakers, E. J. (2016). Hidden multiplicity in exploratory multiway ANOVA: Prevalence and remedies. *Psychonomic Bulletin & Review, 23*(2), 640-647. doi: 10.3758/s1342

Cruz-Jesus, F., Pinheiro, A., & Oliveira, T. (2019). Understanding CRM adoption stages: Empirical analysis building on the TOE framework. *Computers in Industry*, *109*, 1-13. doi: 10.1016/j.compind.2019.03.007

Curtis, E. A., Comiskey, C., & Dempsey, O. (2016). Importance and use of correlational research. *Nurse Researcher (2014+)*, *23*(6), 20. doi: 10.7748/nr.2016.e1382

Cycyota, C. S., & Harrison, D. A. (2002). Enhancing survey response rates at the executive level: Are employee-or consumer-level techniques effective?. *Journal of Management*, *28*(2), 151-176. doi: 10.1177/014920630202800202

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing*, *36*(4), 253-263. doi: 10.1097/DCC.0000000000000253

Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. (2015). Toward energy-efficient cloud computing: Prediction, consolidation, and overcommitment. *IEEE Network*, *29*(2), 56-61. doi: 10.1109/mnet.2015.7064904

Dang, C., Li, Z. F., & Yang, C. (2018). Measuring firm size in empirical corporate finance. *Journal of Banking & Finance*, *86*, 159-176. doi: 10.1016/j.jbankfin.2017.09.006

Daoud, J. I. (2017, December). Multicollinearity and regression analysis. In *Journal of Physics: Conference Series (Vol. 949, No. 1, p. 012009)*. IOP Publishing. doi: 10.1088/1742-6596/949/1/012009

Davies, C., & Fisher, M. (2018). Understanding research paradigms. *Journal of the Australasian Rehabilitation Nurses' Association (JARNA), 21*(3), 21–25. Retrieved from http://www.arna.com.au/

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. doi: 10.2307/249008

Dekel, E., Friedenberg, A., & Siniscalchi, M. (2016). Lexicographic beliefs and assumption. *Journal of Economic Theory*, *163*, 955-985. doi: 10.1016/j.jet.2016.03.003

DeSimone, J. A., Harms, P. D., & DeSimone, A. J. (2015). Best practice recommendations for data screening. *Journal of Organizational Behavior*, *36*(2), 171-181. doi: 10.1002/job.1962

Donnelly, T., & Shardt, Y. A. (2019). Using normal probability plots to determine parameters for higher-level factorial experiments with orthogonal and orthonormal bases. *The Canadian Journal of Chemical Engineering*, *97*(1), 152-164. doi: 10.1002/cjce.23296

Dulmer, H. (2016). The factorial survey: design selection and its impact on reliability and internal validity. *Sociological Methods & Research*, *45*(2), 304-347. doi: 10.1177/0049124115582269

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers*, *1-16*. doi: 10.1007/s10796-017-9774-y

Eisend, M. (2015). Have we progressed marketing knowledge? A meta-meta-analysis of effect sizes in marketing research. *Journal of Marketing, 79*(3), 23-40. doi:10.1509/jm.14.0288

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

Emani, S., Peters, E., Desai, S., Karson, A. S., Lipsitz, S. R., LaRocca, R., ... Williams, D. H. (2018). Perceptions of adopters versus non-adopters of a patient portal: an application of diffusion of innovation theory. *BMJ Health & Care Informatics*, *25*(3), 149-157. doi: 10.14236/jhi.v25i3.991

Euchner, J., & Ganguly, A. (2014). Business model innovation in practice. *Research-Technology Management*, *57*(6), 33-39. doi: 10.5437/08956308X5706013

Fadzil, A. S. A., Nasir Syed Mohamad, S. J. A., Hassan, R., Hamid, N. A., & Zainudin, M. I. (2019). Change management designed for schools: Expanding the continuum of UTAUT on education reform. *Global Business & Management Research*, *11*(2), 340–350. Retrieved from http://www.gbmrjournal.com/

Fan, Y., Wu, C., Chen, C., & Fang, Y. (2015). The effect of status quo bias on cloud system adoption. *Journal of Computer Information Systems*, *55*(3), 55-64. doi: 10.1080/08874417.2015.11645772

Farahmandian, S., & Hoang, D. B. (2016, December). Security for software-defined (cloud, SDN and NFV) infrastructures–issues and challenges. *Computer Science and Information Technology*. doi: 10.5121/csit.2016.61502

Fareen, N., Alam, M. K., Khamis, M. F., & Mokhtar, N. (2019). Treatment effects of two different appliances on pharyngeal airway space in mixed dentition Malay children. *International Journal of Pediatric Otorhinolaryngology*, *125*, 159-163. doi: 10.1016/j.ijporl.2019.07.008

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149-1160. doi:10.3758/brm.41.4.1149

Feng, Y., Du, L., & Ling, Q. (2017). How social media strategies of nonprofit organizations affect consumer donation intention and word-of-mouth. *Social Behavior and Personality: an international journal, 45*(11), 1775-1786. doi: 10.2224/sbp.4412

Fitzgerald, D., Hockey, R., Jones, M., Mishra, G., Waller, M., & Dobson, A. (2019). Use of online or paper surveys by Australian women: Longitudinal study of users, devices, and cohort retention. *Journal of Medical Internet Research, 21*(3), e10672. doi: 10.2196/10672

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. doi: 10.1016/j.cose.2016.01.004

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont report?. *The American Journal of Bioethics, 17*(7), 15-21. doi: 10.1080/15265161.2017.1329482

Fu, H. P., Chang, T. H., Chang, T. S., & Liu, L. C. (2016, September). Factor Analysis on Enterprises Adopting Cloud Computing. In *2016 International Conference on Communications, Information Management and Network Security*. Atlantis Press. doi: 10.2991/cimns-16.2016.84

Gangwar, H., & Date, H. (2016). Critical factors of cloud computing adoption in organizations: An empirical study. *Global Business Review*, *17*(4), 886–904. doi: 10.1177/0972150916645692

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, *28*(1), 107-130. doi: 10.1108/JEIM-08-2013-0065

Gao, F., & Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. *International Journal of Information Management*, *48,* 120-138. doi: 10.1016/j.ijinfomgt.2019.02.002

Gholami, A., & Laure, E. (2016). Security and privacy of sensitive data in cloud computing: a survey of recent developments. *Computer Science and Information Technology*, Conference paper. doi:10.5121/csit.2015.51611

Gogtay, N. J., & Thatte, U. M. (2017). Principles of correlation analysis. *Journal of the association of physicians of India*, *65*, 78-81. Retrieved from http://japi.org/

Green, S. B. (1991). How many subjects does it take to do a regression analysis? *Multivariate behavioral research*, *26*(3), 499-510. doi: 10.1207/s15327906mbr2603_7

Greener, S. (2018). Research limitations: the need for honesty and common

sense. *Interactive Learning Environments*, *26*(5), 567-568. doi: 10.1080/10494820.2018.1486785

Groeneveld, S., Tummers, L., Bronkhorst, B., Ashikali, T., & Van Thiel, S. (2015). Quantitative methods in public administration: Their use and development through time. *International Public Management Journal*, *18*(1), 61-86. doi: 10.1080/10967494.2014.972484

Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed methods research through joint displays. *The Annals of Family Medicine*, *13*(6), 554-561. doi: 10.1370/afm.1865

Guillemin, M., Barnard, E., Allen, A., Stewart, P., Walker, H., Rosenthal, D., & Gillam, L. (2018). Do research participants trust researchers or their institution? *Journal of Empirical Research on Human Research Ethics*, *13*(3), 285-294. doi: 10.1177/1556264618763253

Gundry, D., & Deterding, S. (2018). Validity threats in quantitative data collection with games: A narrative survey. *Simulation & Gaming*, 1046878118805515. doi: 10.1177/1046878118805515

Habjan, K. B., & Pucihar, A. (2017). The importance of business model factors for cloud computing adoption: role of previous experiences. *Organizacija*, *50*(3), 255-272. doi: 10.1515/orga-2017-0013

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *Physical*

Educator, *72*(5). doi: 10.18666/tpe-2015-v72-i5-6133

Haghani, M., & Sarvi, M. (2017). How perception of peer behaviour influences escape decision making: The role of individual differences. *Journal of Environmental Psychology*, *51*, 141-157. doi: 10.1016/j.jenvp.2017.03.013

Hales, S., Lesher-Trevino, A., Ford, N., Maher, D., Ramsay, A., & Tran, N. (2016). Reporting guidelines for implementation and operational research. *Bulletin of the World Health Organization*, *94*(1), 58. doi: 10.2471/BLT.15.167585

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

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

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-based nursing*, *18*(3), 66-67. doi: 10.1136/eb-2015-102129

Health and Human Services. (2016). The Belmont Report. Retrieved from https://www.hhs.gov/

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial management & data systems*, *116*(1), 2-20. doi: 10.1108/IMDS-09-2015-0382

Hickey, G. L., Kontopantelis, E., Takkenberg, J. J., & Beyersdorf, F. (2018). Statistical primer: checking model assumptions with regression diagnostics. *Interactive*

Cardiovascular and Thoracic Surgery, *28*(1), 1-8. doi: 10.1093/icvts/ivy207

Hoaglin, D. C., & Iglewicz, B. (1987). Fine-tuning some resistant rules for outlier labeling. *Journal of the American statistical Association*, *82*(400), 1147-1149. doi: 10.1080/01621459.1987.10478551

Holgado-Tello, F., Chacon-Moscoso, S., Sanduvete-Chaves, S., & Perez-Gil, J. A. (2016). A simulation study of threats to validity in quasi-experimental designs: Interrelationship between design, measurement, and analysis. *Frontiers in psychology*, *7*, 897. doi: 10.3389/fpsyg.2016.00897

Hoque, R., & Sorwar, G. (2017). Understanding factors influencing the adoption of mHealth by the elderly: An extension of the UTAUT model. *International Journal of Medical Informatics*, *101*, 75-84. doi: 10.1016/j.ijmedinf.2017.02.002

Hoti, E. (2015). The technological, organizational and environmental framework of IS innovation adaption in small and medium enterprises. Evidence from research over the last 10 years. *International Journal of Business and Management*, *3*(4), 1-14. doi: 10.20472/bm.2015.3.4.001

Hsu, C., & Lin, J. C. (2016). Factors affecting the adoption of cloud services in enterprises. *Information Systems and eBusiness Management*, *14*(4), 791-822. doi: 10.1007/s10257-015-0300-9

Huang, S. M., Chang, I. C., Li, S. H., & Lin, M. T. (2004). Assessing risk in ERP projects: identify and prioritize the factors. *Industrial Management & Data Systems*, *104*(8), 681-688. doi: 10.1108/02635570410561672

Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel

classification of security concerns in cloud computing. *Applied Computing and Informatics*, *13*(1), 57-65. doi: 10.1016/j.aci.2016.03.001

Hwang, Y., Chung, J. Y., & Shin, D. H. (2018). Investigating the post-adoption attitude of the web based content management system within organization. *Journal of Theoretical and Applied Electronic Commerce Research*, *13*(2), 29-42. doi: 10.4067/S0718-18762018000200104

Ibiamke, A., & Ajekwe, C. C. (2017). On ensuring rigour in accounting research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *7*(3), 157-170. doi: 10.6007/IJARAFMS/v7-i3/3284

Inal, H., Yilmaz Kogar, E., Demirduzen, E., & Gelbal, S. (2017). Cronbach's coefficient alpha: A meta-analysis study. *Hacettepe Egitim Dergisi*, *32*(1), 18–32. doi: 10.16986/HUJE.2016017219

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *International Journal of Engineering, Science, and Technology*, *21*(4), 574-588. doi: 10.1016/j.jestch.2018.05.010

Islam, T., Manivannan, D., & Zeadally, S. (2016). A classification and characterization of security threats in cloud computing. *Int. J. Next-Gener. Comput*, *7*(1).

Jager, J., Putnick, D. L., & Bornstein, M. H. (2017). II. More than just convenient: The scientific merits of homogeneous convenience samples. *Society for Research in Child Development. Monographs*, *82*(2), 13-30. doi: 10.1111/mono.12296

Jamal, N. F., Ghafar, N. M. A., Ismail, I. L., & Chek, M. Z. A. (2018). Comparative study on the complex samples design features using SPSS complex samples, SAS

complex samples and WesVarPc. *International Journal of Academic Research in Business and Social Sciences*, *8*(4), 1282-1292. doi: 10.6007/IJARBSS/v8-i4/4238

Jegadeeswari, S., Dinadayalan, P., & Gnanambigai, N. (2016). Enhanced data security using neural network in cloud environment. *International Journal of Applied Engineering Research*, *11*(1), 278-285. Retrieved from https://pdfs.semanticscholar.org/5c01/7b3539979eb5f093c1bfe890f28887e6cf4b.pdf

Jia, Q., Guo, Y., & Barnes, S. J. (2017). Enterprise 2.0 post-adoption: Extending the information system continuance model based on the technology-organization-environment framework. *Computers in Human Behavior*, *67*, 95-105. doi: 10.1016/j.chb.2016.10.022

Jones, M. S., House, L. A., & Gao, Z. (2015). Respondent screening and revealed preference axioms: Testing quarantining methods for enhanced data quality in web panel surveys. *Public Opinion Quarterly*, *79*(3), 687-709. doi:10.1093/poq/nfv015

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, *7*(4), 396. doi: 10.9734/BJAST/2015/14975

Juma, M. K., & Tjahyanto, A. (2019). Challenges of Cloud Computing Adoption Model for Higher Education Level in Zanzibar (the Case Study of SUZA and ZU). *Procedia Computer Science*, *161*, 1046-1054. doi: 10.1016/j.procs.2019.11.215

Käärik, E., Käärik, M., & Maadik, I. H. (2016). On the correlation structures of multivariate skew-normal distribution. *Acta et Commentationes Universitatis Tartuensis de Mathematica*, *20*(1), 83-100. Doi:10.12697/ACUTM.2016.20.07

Kalaiprasath, R., Elankavi, R., & Udayakumar, D. R. (2017). Cloud. Security and compliance-A semantic approach in end to end security. *International Journal on Smart Sensing and Intelligent Systems Special Issue*, *10*(4), 482-494. doi: 10.21307/ijssis-2017-265

Karkonasasi, K., Baharudin, A. S., Esparham, B., Mousavi, S. A., & Suhaimi Baharudin, A. (2016). Adoption of cloud computing among enterprises in Malaysia. *Indian Journal of Science and Technology*, *9*(48). doi: 10.17485/ijst/2016/v9i48/88128

Katunzi, T. M., & Ndekwa, A. G. (2016). Small and medium tourist enterprises and social Media adoption: Empirical evidence from Tanzanian tourism sector. *International Journal of Business and Management*, *11*(4), 71-80. doi: 10.5539/ijbm.v11n4p71

Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. *International Journal of Advances in Engineering & Technology*, *8*(3), 397. doi: 10.14257/ijgdc.2015.8.5.21

Kautonen, T., van Gelderen, M., & Fink, M. (2015). Robustness of the theory of planned behavior in predicting entrepreneurial intentions and actions. *Entrepreneurship Theory and Practice*, *39*(3), 655-674. doi: 10.1111/etap.12056

Kazim, M., & Zhu, S. Y. (2015). A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications (IJACSA)*.

6(3), 109-113. doi: 10.14569/IJACSA.2015.060316

Keeble, C., Baxter, P. D., Barber, S., & Law, G. R. (2015). Participation Rates In Epidemiology Studies And Surveys: A ReVievy 2007–2015. *The Internet Journal of Epidemiology*, *14*(1). doi: 10.5580/IJE.34897

Khan, G. F., Sarstedt, M., Shiau, W. L., Hair, J. F., Ringle, C. M., & Fritze, M. P. (2019). Methodological research on partial least squares structural equation modeling (PLS-SEM) An analysis based on social network approaches. *Internet Research*. doi: 10.1108/intr-12-2017-0509

Khan, N., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, *94*, 485-490. doi: 10.1016/j.procs.2016.08.075

Khanal, N., Parsons, G., Mantz, T., & Mendelson, R. (2016). Critical factors influencing the adoption of cloud computing. *European Journal of Business Research*, *16*(1), 73-96. doi: 10.18374/EJBR-16-1.6

Khikmah, L., Wijayanto, H., & Syafitri, U. D. (2017). Modeling Governance KB with CATPCA to Overcome Multicollinearity in the Logistic Regression. In *Journal of Physics: Conference Series* (*Vol. 824, No. 1*, p. 012027). IOP Publishing. doi:10.1088/1742-6596/824/1/012027

Kim, M., Mohindra, A., Muthusamy, V., Ranchal, R., Salapura, V., Slominski, A., & Khalaf, R. (2016). Building scalable, secure, multi-tenant cloud services on IBM Bluemix. *IBM Journal of Research and Development*, *60*(2-3), 8-1. doi: 10.1147/JRD.2016.2516942

Kim, S., Lee, J., & Yoon, D. (2015). Norms in social media: The application of theory of reasoned action and personal norms in predicting interactions with Facebook page like ads. *Communication Research Reports*, *32*(4), 322-331. Doi: 10.1080/08824096.2015.1089851

Kinchin, G., Ismail, N., & Edwards, J. A. (2018). Pilot study, does it really matter? Learning lessons from conducting a pilot study for a qualitative PhD thesis. *International Journal of Social Science Research*, *6*(1). doi: 10.5296/ijssr.v6i1.11720

Kinuthia, N., & Chung, S. (2017). An empirical study of technological factors affecting cloud enterprise resource planning systems adoption. *Information Resources Management Journal (IRMJ), 30*(2), 1-22. doi:10.4018/IRMJ.2017040101

Kiwanuka, A. (2015). Acceptance process: The missing link between UTAUT and diffusion of innovation theory. *American Journal of Information Systems, 3*(2), 40-44. doi: 10.12691/ajis-3-2-3

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *Journal of Information Systems and Technology Management*, *13*(3), 479–496. doi: 10.4301/S1807-17752016000300007

Klug, W., & Xue, B. (2015). Factors affecting cloud computing adoption among universities and colleges in the United States and Canada. *Issues in Information Systems*, *16*(3), 1.

Kohn, K. (2018). Using logistic regression to examine multiple factors related to e-book use. *Library Resources & Technical Services*, *62*(2), 54. doi: 10.5860/lrts.62n2.54

Kontopantelis, E., White, I. R., Sperrin, M., & Buchan, I. (2017). Outcome-sensitive multiple imputation: a simulation study. *BMC medical research methodology*, *17*(1), 2. doi: 10.1186/s12874-016-0281-5

Kovach, J. J., Hora, M., Manikas, A., & Patel, P. C. (2015). Firm performance in dynamic environments: The role of operational slack and operational scope. *Journal of Operations Management*, *37*, 1-12. doi: 10.1016/j.jom.2015.04.002

Koyfman, S. A., Reddy, C. A., Hizlan, S., Leek, A. C., & Kodish, A. E. D. (2016). Informed consent conversations and documents: a quantitative comparison. *Cancer*, *122*(3), 464-469. doi: 10.1002/cncr.29759

Kreslins, K., Novik, D., & Vasiljeva, T. (2018). Challenge of Cloud Computing for SMEs: A Case of Baltic Countries. *Journal of Innovation Management in Small and Medium Enterprise.* 2018, 1-10. doi: 10.5171/2018.238581

Kucukaltan, B., Irani, Z., & Aktas, E. (2016). A decision support model for identification and prioritization of key performance indicators in the logistics industry. *Computers in Human Behavior*, *65*, 346-358. Doi: 10.1016/j.chb.2016.08.045

Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *JISTEM - Journal of Information Systems and Technology Management*, *14*(1), 21-38. doi: 10.4301/s1807-17752017000100002

Lal, P., & Bharadwaj, S. S. (2016). Understanding the impact of cloud-based services adoption on organizational flexibility: An exploratory study. *Journal of*

Enterprise Information Management, *29*(4), 566-588. doi: 10.1108/jeim-04-2015-0028

Lam, W. M. W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy*, *37*, 42-51. doi: 10.1016/j.infoecopol.2016.10.003

Landers, R. N., & Behrend, T. S. (2015). An inconvenient truth: Arbitrary distinctions between organizational, Mechanical Turk, and other convenience samples. *Industrial and Organizational Psychology*, *8(March)*, 1–23. doi: 10.1017/iop.2015.13

Landrum, B., & Garza, G. (2015). Mending fences: Defining the domains and approaches of quantitative and qualitative research. *Qualitative Psychology*, *2*(2), 199–209. doi: 10.1037/qup0000030

Larosiliere, G. D., Carter, L. D., & Meske, C. (2017). How does the world connect? Exploring the global diffusion of social network sites. *Journal of the Association for Information Science and Technology*, *68*(8), 1875-1885. doi: 10.1002/asi.23804

Lease, D. R. (2005). *Factors influencing the adoption of biometric security technologies by decision-making information technology and security managers* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (UMI No. 305359883).

Lechien, J. R., Huet, K., Finck, C., Khalife, M., Fourneau, A. F., Delvaux, V., Piccaluga, M., Harmegnies, B., & Saussez, S. (2017). Validity and reliability of a French

version of reflux symptom index. *The Journal of Voice, 31*(4), 512-e1. doi: 10.1016/j.jvoice.2016.11.020

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

Lever, J., Krzywinski, M., & Altman, N. (2016). Points of significance: Logistic regression. *Nature Methods, 13*(7), 541-542. doi: 10.1038/nmeth.3904

Lewis, K. M., DuBois, D. L., Ji, P., Day, J., Silverthorn, N., Bavarian, N., ... Flay, B. R. (2017). Meeting the challenges of longitudinal cluster-based trials in schools: Lessons from the Chicago trial of Positive Action. *Evaluation & the health professions*, *40*(4), 450-482. doi: 10.1177/0163278716673688

Li, F., Morgan, K. L., & Zaslavsky, A. M. (2018). Balancing covariates via propensity score weighting. *Journal of the American Statistical Association, 113*(521), 390-400. doi: 10.1080/01621459.2016.1260466

Liang, J., Tang, M. L., & Zhao, X. (2019). Testing high-dimensional normality based on classical skewness and Kurtosis with a possible small sample size. *Communications in Statistics: Theory and Methods, 48*(23), 5719-5732. doi:10.1080/03610926.2018.1520882

Lim, W. M. (2018). Dialectic Antidotes to Critics of the Technology Acceptance Model: Conceptual, Methodological, and Replication Treatments for Behavioural Modelling in Technology-Mediated Environments. *Australasian Journal of Information Systems, 22*. doi: 10.3127/ajis.v22i0.1651

Lippert, S. K., & Govindarajulu, C. (2006). Technological, organizational, and environmental antecedents to web services adoption. *Communications of the IIMA*, *6*(1), 14. Retrieved from http://scholarworks.lib.csusb.edu/ciima/vol6/iss1/14

Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: solutions and future directions. *Journal of Computing Science and Engineering*, *9*(3), 119-133. doi: 10.5626/jcse.2015.9.3.119

Lo, N. W., Yang, T. C., & Guo, M. H. (2015). An attribute-role based access control mechanism for multi-tenancy cloud environment. *Wireless Personal Communications*, *84*(3), 2119-2134. doi: 10.1007/s11277-015-2515-y

Mahajan, A., & Sharma, S. (2015). The malicious insiders threat in the cloud. *International Journal of Engineering Research and General Science*, *3*(2), 245-256.

Marcellesi, A. (2015). External validity: is there still a problem? *Philosophy of Science*, *82*(5), 1308-1317. doi: 10.1086/684084

Maresova, P., Sobeslav, V., & Krejcar, O. (2017). Cost–benefit analysis – evaluation model of cloud computing deployment for use in companies. *Applied Economics*, *49*(6), 521–533. doi: 10.1080/00036846.2016.1200188

Martin, A. J., Collie, R. J., Durksen, T. L., Burns, E. C., Bostwick, K. C., & Tarbetsky, A. L. (2019). Growth goals and growth mindset from a methodological-synergistic perspective: lessons learned from a quantitative correlational research

program. *International Journal of Research & Method in Education*, *42*(2), 204-219. doi: 10.1080/1743727X.2018.1481938

Martin, J., Mortimer, G., & Andrews, L. (2015). Re-examining online customer experience to include purchase frequency and perceived risk. *Journal of retailing and consumer services, 25*, 81-95. doi: 10.1016/j.jretconser.2015.03.008

Martinez-Mesa, J., Gonzalez-Chica, D. A., Duquia, R. P., Bonamigo, R. R., & Bastos, J. L. (2016). Sampling: how to select participants in my research study?. *Anais brasileiros de dermatologia*, *91*(3), 326-330. doi: 10.1590/abd1806-4841.20165254

Martins, R., Oliveira, T., & Thomas, M. A. (2016). An empirical analysis to assess the determinants of SaaS diffusion in firms. *Computers in Human Behavior, 62*, 19-33. doi: 10.1016/j.chb.2016.03.049

Matias, J. B., & Hernandez, A. A. (2019). Cloud Computing Adoption Intention by MSMEs in the Philippines. *Global Business Review*, doi: 10.1177/0972150918818262

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537-542. doi: 10.1177/0267659114559116

McKibben, W. B., & Silvia, P. J. (2016). Inattentive and socially desirable responding: Addressing subtle threats to validity in quantitative counseling research. *Counseling Outcome Research and Evaluation*, *7*(1), 53-64. doi: 10.1177/2150137815613135

Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). New York, NY: Routledge.

Millner, A. J., Lee, M. D., & Nock, M. K. (2015). Single-item measurement of suicidal behaviors: Validity and consequences of misclassification. *PLoS One*, *10*(10), e0141606. doi: 10.1371/journal.pone.0141606

Min, S., So, K. K. F., & Jeong, M. (2018). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology acceptance model. *Journal of Travel & Tourism Marketing*, *1-14*. doi: 10.1080/10548408.2018.1507866

Mircioiu, C., & Atkinson, J. (2017). A comparison of parametric and non-parametric methods applied to a Likert scale. *Pharmacy*, *5*(2), 26. doi: 10.3390/pharmacy5020026

Mlikotic, R., Parker, B., & Rajapakshe, R. (2016). Assessing the effects of participant preference and demographics in the usage of web-based survey questionnaires by women attending screening mammography in British Columbia. *Journal of Medical Internet Research*, *18*(3), e70. doi: 10.2196/jmir.5068

Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior: Theory, Research and Practice*, *95*(124).

Munn, J. C. (2016). Teaching qualitative methods to social workers: Four approaches. *Qualitative Social Work*, *15*, 322-330. doi: 10.1177/1473325015617008

Nayar, K. B., & Kumar, V. (2018). Cost-benefit analysis of cloud computing in

education. *International Journal of Business Information Systems*, *27*(2), 205-221. doi: 10.1504/ijbis.2018.10009814

Njenga, K., Garg, L., Bhardwaj, A. K., Prakash, V., & Bawa, S. (2019). The cloud computing adoption in higher learning institutions in Kenya: Hindering factors and recommendations for the way forward. *Telematics and Informatics*, *38*, 225-246. doi: 10.1016/j.tele.2018.10.007

Noonan, C. F. (2018). Spy the Lie: Detecting Malicious Insiders (No. PNNL-SA-122655). *Pacific Northwest National Lab. (PNNL)*, Richland, WA (United States).

O'Brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. *Quality & Quantity*. *41* (5): 673–690. doi:10.1007/s11135-006-9018-6

O'Grady, E. (2016). Research as a respectful practice: An exploration of the practice of respect in qualitative research. *Qualitative Research in Education*, *5*(3). 229-254. doi: 10.17583/qre.2016.2018

Ohyver, M., Moniaga, J. V., Yunidwi, K. R., & Setiawan, M. I. (2017). Logistic Regression and Growth Charts to Determine Children Nutritional and Stunting Status: A Review. *Procedia Computer Science*, *116*, 232-241. doi: 10.1016/j.procs.2017.10.045

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, *51*(5), 497-510. doi: 10.1016/j.im.2014.03.006

Orquin, J. L., & Holmqvist, K. (2018). Threats to the validity of eye-movement research in psychology. *Behavior Research Methods, 50*(4), 1645-1656. doi: 10.3758/s13428-017-0998-z

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and policy in mental health and Mental Health Services Research, 42*(5), 533–544. doi:10.1007/s10488-013-0528-y

Paul, J., Modi, A., & Patel, J. (2016). Predicting green product consumption using theory of planned behavior and reasoned action. *Journal of Retailing and Consumer Services, 29*, 123-134. Doi: 10.1016/j.jretconser.2015.11.006

Pedersen, A. B., Mikkelsen, E. M., Cronin-Fenton, D., Kristensen, N. R., Pham, T. M., Pedersen, L., & Petersen, I. (2017). Missing data and multiple imputation in clinical epidemiological research. *Clinical Epidemiology, 9*, 157. doi: 10.2147/CLEP.S129785

Perrault, E. K., & Keating, D. M. (2018). Seeking ways to inform the uninformed: Improving the informed consent process in online social science research. *Journal of Empirical Research on Human Research Ethics, 13*(1), 50-60. doi: 10.1177/1556264617738846

Petursdottir, A. I., & Carr, J. E. (2018). Applying the taxonomy of validity threats from mainstream research design to single-case experiments in applied behavior analysis. *Behavior Analysis in Practice, 11*(3), 228-240. doi: 10.1007/s40617-

018-00294-6

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software*, *103*, 167-181. doi: 10.1016/j.jss.2015.02.002

Privacy International. (2019). State of privacy in Lebanon. Retrieved from https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

Quick, J., & Hall, S. (2015). Part three: The quantitative approach. *Journal of Perioperative Practice*, *25*(10), 192-196. doi: 10.1177/175045891502501002

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. *SpringerPlus*, *4*(1), 197. doi: 10.1186/s40064-015-0962-2

Raj, A., & Dharanipragada, J. (2017). Keep the PokerFace on! Thwarting cache side channel attacks by memory bus monitoring and cache obfuscation. *Journal of Cloud Computing*, *6*(1), 28. doi: 10.1186/s13677-017-0101-4

Rakic, S., Novakovic, B., Stevic, S., & Niskanovic, J. (2018). Introduction of safety and quality standards for private health care providers: a case-study from the Republic of Srpska, Bosnia and Herzegovina. *International Journal for Equity in Health*, *17*(1), 92. doi: 10.1186/s12939-018-0806-0

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia Computer Science*, *110*, 465-472. doi: 10.1016/j.procs.2017.06.124

Ranganathan, P., Pramesh, C. S., & Aggarwal, R. (2017). Common pitfalls in statistical

analysis: Logistic regression. *Perspectives in Clinical Research, 8*(3), 148. doi: 10.4103/picr.PICR_87_17

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

Rasyid, A. R., Bhandary, N. P., & Yatabe, R. (2016). Performance of frequency ratio and logistic regression model in creating GIS based landslides susceptibility map at Lompobattang Mountain, Indonesia. *Geoenvironmental Disasters, 3*(1), 19. doi: 10.1186/s40677-016-0053-x

Rathi, D., & Given, L. M. (2017). Non-profit organizations' use of tools and technologies for knowledge management: a comparative study. *Journal of Knowledge Management, 21*(4), 718-740. doi: 10.1108/jkm-06-2016-0229

Raths, D. (2015). 5 Tech tools that help personalize PD: as more districts take advantage of social media, online surveys and more, the days of one-size-fits-all professional development are over. *T H E Journal (Technological Horizons in Education)*, (*1*), 22. Retrieved from http://thejournal.com/

Ray, D. (2016). Cloud adoption decisions: Benefitting from an integrated perspective. *Electronic Journal of Information Systems Evaluation, 19*(1). Retrieved from http://www.ejise.com/

Raza, M. H., Adenola, A. F., Nafarieh, A., & Robertson, W. (2015). The slow adoption of cloud computing and IT workforce. *Procedia Computer Science, 52,* 1114-1119. doi: 10.1016/j.procs.2015.05.128

Resnik, D. B., Miller, A. K., Kwok, R. K., Engel, L. S., & Sandler, D. P. (2015). Ethical issues in environmental health research related to public health emergencies: Reflections on the Gulf study. *Environmental Health Perspectives*, *123*(9), A227-A231. doi: 10.1289/ehp.1509889

Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. *Omega*, *64*, 126-130. Doi: 10.1016/j.omega.2015.12.001

Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221-232. doi: 10.1016/j.cose.2011.12.001

Rice, S., Winter, S. R., Doherty, S., & Milner, M. (2017). Advantages and disadvantages of using internet-based survey methods in aviation-related research. *Journal of Aviation Technology and Engineering*, *7*(1), 5. doi: 10.7771/2159-6670.1160

Rich, A., Brandes, K., Mullan, B. A., & Hagger, M. S. (2015). Theory of planned behavior and adherence in chronic illness: A meta-analysis. *Journal of Behavioral Medicine*, *38*(4), 673-688. doi: 10.1007/s10865-015-9644-3

Robertson, R. A. (2008). *Critical success factors for service-oriented small businesses in the e-commerce environment. (Doctoral dissertation).* Retrieved from ProQuest Dissertations & Theses Global. (UMI No. 304830836).

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York, NY: Free Press.

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the Fundamentals: A Simplistic Differentiation Between Qualitative and Quantitative Research. *Nephrology Nursing Journal*, *45*(2), 209–213. Retrieve from http://www.annanurse.org/

Rutkowski, L., Rutkowski, D., & Zhou, Y. (2016). Item calibration samples and the stability of achievement estimates and system rankings: Another look at the PISA model. *International Journal of Testing*, *16*(1), 1-20. doi: 10.1080/15305058.2015.1036163

Sabbah, H., Trabulsi, H., Chbib, R., & Sabbah, I. (2019). Cloud Computing in Lebanese Enterprises: Applying the Technology, Organization, and Environment (TOE) Framework. *Journal of Computer and Communications*, *7*(10), 21-35. doi: 10.4236/jcc.2019.710003

Saleh, A., & Bista, K. (2017). Examining factors impacting online survey response rates in educational research: Perceptions of graduate students. *Journal of MultiDisciplinary Evaluation*, *13*(29), 63-74. Retrieved from http://journals.sfu.ca/jmde/

Sand, A., & Nilsson, M. E. (2017). When Perception Trumps Reality: Perceived, Not Objective, Meaning of Primes Drives Stroop Priming. *Psychological Science*, *28*(3), 346-355. doi: 10.1177/0956797616684681

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers & Education, 128*, 13-35. doi: 10.1016/j.compedu.2018.09.009

Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: Appropriate use and interpretation. *Anesthesia and Analgesia*, *126*(5), 1763–1768. doi: 10.1213/ANE.0000000000002864

Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., & Salzman, S. (2018). Factors That Influence Adoption of Cloud Computing: An Empirical Study of Australian SMEs. *Australasian Journal of Information Systems, 22*. doi: 10.4018/IJEBR.2018070105

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

Setia, M. S. (2016). Methodology series module 5: Sampling strategies. *Indian Journal of Dermatology, 61*(5), 505. doi: 10.4103/0019-5154.190118

Sharifzadeh, M. S., Damalas, C. A., Abdollahzadeh, G., & Ahmadi-Gorgi, H. (2017). Predicting adoption of biological control among Iranian rice farmers: An application of the extended technology acceptance model (TAM2). *Crop Protection, 96,* 88-96. doi: 10.1016/j.cropro.2017.01.014

Sharma, S. K. (2017). Integrating cognitive antecedents into TAM to explain mobile banking behavioral intention: A SEM-neural network modeling. *Information Systems Frontiers, 1-13*. doi: 10.1007/s10796-017-9775-x

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. *Computers in Human Behavior, 62*, 61-69. doi: 10.1016/j.chb.2016.03.073

Sharpo, G. C., Lawlor, D. A., & Richardson, S. S. (2018). It's the mother!: How assumptions about the causal primacy of maternal effects influence research on

the developmental origins of health and disease. *Social Science and Medicine, 213*, 20-27. doi: 10.1016/j.socscimed.2018.07.035

Sheldon, P. (2016). Facebook friend request: Applying the theory of reasoned action to student-teacher relationships on Facebook. *Journal of Broadcasting & Electronic Media, 60*(2), 269-285. Doi: 10.1080/08838151.2016.1164167

Shrivas, A., Singh, O., & Dubey, M. (2016). Security concerns and remedies in Cloud Computing in Electrical, Electronics and Computer Science (SCEECS), *2016 IEEE Students' Conference on, 1-6*. doi: 10.1109/SCEECS.2016.7509356

Sidhu, J., & Singh, S. (2017). Improved topsis method based trust evaluation framework for determining trustworthiness of cloud service providers. *Journal of Grid Computing, 15*(1), 81-105. doi: 10.1007/s10723-016-9363-1

Singh, A., Mishra, N., Ali, S. I., Shukla, N., & Shankar, R. (2015). Cloud computing technology: Reducing carbon footprint in beef supply chain. *International Journal of Production Economics, 164*, 462-471. doi: 10.1016/j.ijpe.2014.09.019

Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications, 75*, 200-222. doi: 10.1016/j.jnca.2016.09.002

Sohaib, O., Naderpour, M., Hussain, W., & Martinez, L. (2019). Cloud computing model selection for e-commerce enterprises using a new 2-tuple fuzzy linguistic decision-making method. *Computers & Industrial Engineering, 132*, 47-58. doi: 10.1016/j.cie.2019.04.020

Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to

identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security, 74*, 340-354. doi: 10.1016/j.cose.2017.08.016

Sohn, S. Y., Kim, D. H., & Yoon, J. H. (2016). Technology credit scoring model with fuzzy logistic regression. *Applied Soft Computing, 43,* 150-158. doi: 10.1016/j.asoc.2016.02.025

Solares, J. R. A., Wei, H. L., & Billings, S. A. (2019). A novel logistic-NARX model as a classifier for dynamic binary classification. *Neural Computing and Applications*, *31*(1), 11-25. doi: 10.1007/s00521-017-2976-x

Sparkes, A. C. (2015). Developing mixed methods research in sport and exercise psychology: Critical reflections on five points of controversy. *Psychology of Sport and Exercise*, *16,* 49-59. doi: 10.1016/j.psychsport.2014.08.014

Steinmetz, H., Knappstein, M., Ajzen, I., Schmidt, P., & Kabst, R. (2016). How effective are behavior change interventions based on the theory of planned behavior?. *Zeitschrift fuer Psychologie - Journal of Psychology.* Doi: 10.1027/2151-2604/a000255:

Stivala, A. D., Koskinen, J. H., Rolls, D. A., Wang, P., & Robins, G. L. (2016). Snowball sampling for estimating exponential random graph models for large networks. *Social Networks*, *47*, 167-188. doi: 10.1016/j.socnet.2015.11.003

Stroustrup, N. (2018). Measuring and modeling interventions in aging. *Current opinion in cell biology*, *55*, 129-138. doi: 10.1016/j.ceb.2018.07.004

Šumak, B., & Šorgo, A. (2016). The acceptance and use of interactive whiteboards

among teachers: Differences in UTAUT determinants between pre- and post-adopters.

Computers in Human Behavior, *64*, 602-620. doi: 10.1016/j.chb.2016.07.037

Suryateja, P. S. (2018). Threats and Vulnerabilities of Cloud Computing: A Review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297-302. doi: 10.26438/ijcse/v6i3.297302

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, *48*(6), 1273-1296. doi: 10.1007/s11165-016-9602-2

Tan, K. H., Zhan, Y., Ji, G., Ye, F., & Chang, C. (2015). Harvesting big data to enhance supply chain innovation capabilities: An analytic infrastructure based on deduction graph. *International Journal of Production Economics*, *165*, 223-233. doi: 10.1016/j.ijpe.2014.12.034

Tarhini, A., Arachchilage, N. A. G., & Abbasi, M. S. (2015). A critical review of theories and models of technology adoption and acceptance in information system research. *International Journal of Technology Diffusion (IJTD)*, *6*(4), 58-77. Doi: 10.4018/IJTD.2015100104

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, *29*(4), 830-849. doi: 10.1108/ITP-02-2014-0034

Tengstedt, M. A., Fagerstrom, A., & Mobekk, H. (2018). Health interventions and validity on social media: A literature review. *Procedia Computer Science, 138*, 169-176. doi: 10.1016/j.procs.2018.10.024

Thokala, P., Devlin, N., Marsh, K., Baltussen, R., Boysen, M., Kalo, Z., ... & Ijzerman, M. (2016). Multiple criteria decision analysis for health care decision making—an introduction: report 1 of the ISPOR MCDA Emerging Good Practices Task Force. *Value in Health*, *19*(1), 1-13. doi: 10.1016/j.jval.2015.12.003

Toledo, D., Aerny, N., Soldevila, N., Baricot, M., Godoy, P., Castilla, J., ... & Tamames, S. (2015). Managing an online survey about influenza vaccination in primary healthcare workers. *International Journal of Environmental Research and Public Health*, *12*(1), 541-553. doi: 10.3390/ijerph120100541

Topaloglu, M., Caldibi, E., & Oge, G. (2016). The scale for the individual and social impact of students' social network use: The validity and reliability studies. *Computers in Human Behavior*, *61*, 350-356. doi: 10.1016/j.chb.2016.03.036

Tornatzky, L. G., & Fleischer, M. (1990). *Processes of technological innovation*. Lexington, MA: Lexington Books

Tricco, A. C., Antony, J., Soobiah, C., Kastner, M., MacDonald, H., Cogo, E., … & Straus, S. E. (2016). Knowledge synthesis methods for integrating qualitative and quantitative data: a scoping review reveals poor operationalization of the methodological steps. *Journal of Clinical Epidemiology*, *73*, 29-35. doi: 10.1016/j.jclinepi.2015.12.011

Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to government cloud adoption. *International Journal of Managing Information Technology*, *6*(3), 1-16. doi: 10.5121/ijmit.2014.6301

Upham, P., Oltra, C., & Boso, À. (2015). Towards a cross-paradigmatic framework of the social acceptance of energy systems. *Energy Research & Social Science*, *8*, 100-112. doi: 10.1016/j.erss.2015.05.003

Van der Stede, W. A. (2014). A manipulationist view of causality in cross-sectional survey research. *Accounting, Organizations and Society*, *39*(7), 567-574. doi: 10.1016/j.aos.2013.12.001

Vaske, J. J., Beaman, J., & Sponarski, C. C. (2017). Rethinking internal consistency in Cronbach's Alpha. *Leisure Sciences*, *39*(2), 163-173. doi: 10.1080/01490400.2015.1127189

Vatcheva, K. P., Lee, M., McCormick, J. B., & Rahbar, M. H. (2016). Multicollinearity in regression analyses conducted in epidemiologic studies. *Epidemiology (Sunnyvale, Calif.)*, *6*(2). doi: 10.4172/2161-1165.1000227

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. doi: 10.2307/30036540

Wahsh, M. A., & Dhillon, J. S. (2016). An investigation of factors affecting the adoption of cloud computing for E-government implementation. In *Research and Development (SCOReD), 2015 IEEE Student Conference on, 323-338* IEEE. doi: 10.1109/SCORED.2015.7449349

Walker, D. A., & Smith, T. J. (2016). Nine pseudo R2 indices for binary logistic regression models. *Journal of Modern Applied Statistical Methods*, *15*(1), 848-854. doi: 10.22237/jmasm/1462078200

Warth, B., Levin, N., Rinehart, D., Teijaro, J., Benton, H. P., & Siuzdak, G. (2017). Metabolizing data in the cloud. *Trends in biotechnology*, *35*(6), 481-483. doi: 10.1016/j.tibtech.2016.12.010

Whicher, D., Kass, N., Saghai, Y., Faden, R., Tunis, S., & Pronovost, P. (2015). The views of quality improvement professionals and comparative effectiveness researchers on, ethics, IRBs, and oversight. *Journal of Empirical Research on Human Research Ethics, 10*(2), 132–144. http://doi.org/10.1177/1556264615571558

Wiesmann, B., Snoei, J. R., Hilletofth, P., & Eriksson, D. (2017) Drivers and barriers to reshoring: A literature review on offshoring in reverse. *European Business Review*, *29*(1): 15-42 doi: 10.1108/EBR-03-2016-0050

Williams, M. D., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): a literature review. *Journal of Enterprise Information Management*, *28*(3), 443-488. Doi: 10.1108/JEIM-09-2014-0088

Willits, F. K., Theodori, G. L., & Luloff, A. E. (2016). Another look at Likert scales. *Journal of Rural Social Sciences*, *31*(3), 126. Retrieved from http://journalofruralsocialsciences.org/

Wolgemuth, J. R., Hicks, T., & Agosto, V. (2017). Unpacking assumptions in research synthesis: A critical construct synthesis approach. *Educational Researcher*, *46*(3),

131-139. doi: 10.3102/0013189X17703946

Wu, C. (2016). Status quo bias in information system adoption: A meta-analytic review. *Online Information Review*, *40*(7), 998-1017. doi: 10.1108/OIR-09-2015-0311

Wu, Z., Wu, Y., Yang, Y., Chen, F., Zhang, N., Ke, Y., & Li, W. (2017). A comparative study on the landslide susceptibility mapping using logistic regression and statistical index models. *Arabian Journal of Geosciences*, *10*(8), 187. doi: 10.1007/s12517-017-2961-9

Yanagida, T., Strohmeier, D., & Spiel, C. (2016). Dynamic change of aggressive behavior and victimization among adolescents: Effectiveness of the ViSC program. *Journal of Clinical Child & Adolescent Psychology, 1-15*. doi: 10.1080/15374416.2016.1233498

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53. doi: 10.1080/17538947.2016.1239771

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior, 45*, 254-264. doi: 10.1016/j.chb.2014.12.022

Yeou, M. (2016). An investigation of students' acceptance of moodle in a blended learning setting using technology acceptance model. *Journal of Educational Technology Systems*, *44*, 300–318. doi:10.1177/004723951561846

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, *7*(1), 5. doi:

10.1186/s13174-016-0046-8

Yin, R. K. (2014). Case study research: Design and methods, (5th ed.). Thousand Oaks, CA: Sage

Yoon, H. Y. (2016). User acceptance of mobile library applications in academic libraries: an application of the technology acceptance model. *The Journal of Academic Librarianship*, *42*(6), 687-693. doi: 10.1016/j.acalib.2016.08.003

Zanello, G., Fu, X., Mohnen, P., & Ventresca, M. (2016). The creation and diffusion of innovation in developing countries: a systematic literature review. *Journal of Economic Surveys*, *30*(5), 884-912. doi: 10.1111/joes.12126

Zarit, S. H., Bangerter, L. R., Liu, Y., & Rovine, M. J. (2017). Exploring the benefits of respite services to family caregivers: methodological issues and current findings. *Aging & Mental Health*, *21*(3), 224–231. doi:10.1080/13607863.2015.1128881

Zhang, X., Yu, P., Yan, J., & Spil, I. T. A. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer e-health innovations: a case study in a primary care clinic. *BMC health services research, 15*(1), 71. doi: 10.1186/s12913-015-0726-2

Appendix A: NIH Training Certificate

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Johnathan Van Houten** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 11/05/2017.

Certification Number: 2552070.

Appendix B: Email Invitation to Participate in Research

Date: <Date>
Subject: Invitation to participate in research study

Recipient:

My name is Johnathan Van Houten and I am currently a doctoral student at Walden University pursuing a Doctorate in Information Technology degree. I am conducting a research study to validate the impact and determine a hierarchical threat index for security concerns as impediments to adoption of cloud services, titled "Relationship Between Specific Security Concerns and Intention to Adopt Cloud Computing". I have sent this to you as a request to participate in my study. Participation requires a minimal degree of time completing a brief online survey; perhaps five minutes.

The intent is to establish the relationship between security concerns held by key decision-makers as impediments to the adoption process and to hierarchically prioritize them such that practitioners may understand and address them. While participation will not provide compensation to you specifically, the benefits to practitioners for obtaining focus on specific concerns you, as decision-makers possess is relevant.

If you are in a role wherein you represent the gating factor to adopt cloud or not, regardless of the size or scope of your business, your input will be valuable to my research and ultimately, to the field.

By accessing and participating in the survey, you agree to the established parameters and provide informed consent regarding any personal information retrieved by the instrument. However, the study is not guided by parameters concerning the sex of the individual nor will any names be requested. The only material of a specific nature will concern the size and scope of the organization you represent. All data will be protected, and no association to participants will relate directly to said data.

You can participate by completing the survey at www.surveymonkey.com/<link to survey>.

If you wish to decline or cancel participation at any time, merely close the browser without submitting.

Thank you for your time and consideration.

Sincerely,
Johnathan Van Houten
Doctoral Candidate, Walden University

Appendix C: Approvals for Use of Survey Instruments

YR

Young Ryu <ryoung@utdallas.edu>
Mon 2/11/2019 1:48 PM
Johnathan Vanhouten

Dear Jonathan,

You may use the survey instrument for your dissertation work.

Good luck.

Young Ryu

...

On 2/8/2019 9:56 AM, Johnathan Vanhouten wrote:

> Dr. Young Ryu
>
> I am a doctoral student from Walden University working on a doctoral research study tentatively titled "Relationship Between Specific Security Concerns and CIO Intention to Adopt Cloud" under the direction of my doctoral study committee chaired by Dr. Constance Blanson.
> I would like your permission to obtain, use, and print the survey instrument presented in your work titled "Unrealistic optimism on information security management" (2012).
>
> I will use this survey only for my research study and not in any other manner.
>
> If this request is acceptable and you approve, please indicate so via an email response.
>
> Sincerely,
>
> Johnathan Van Houten
> Doctoral Candidate

D

Dr. David R. Lease <dlease@verizon.net>
Sat 2/9/2019 9:39 AM
Johnathan Vanhouten

Hi Jonathan:

Permission to use my data collection instrument is approved. Please let me know if you or Dr. Blanson have any questions or wish to add me to your committee.

Best wishes on your doctoral journey!

Regards,

David Lease

-----Original Message-----
From: Johnathan Vanhouten <johnathan.vanhouten@waldenu.edu>
To: dlease@verizon.net <dlease@verizon.net>
Sent: Fri, Feb 8, 2019 10:52 am
Subject: Request to utilize survey instrument

Dr. David R. Lease

I am a doctoral student from Walden University working on a doctoral research study tentatively titled "Relationship Between Specific Security Concerns and CIO Intention to Adopt Cloud" under the direction of my doctoral study committee chaired by Dr. Constance Blanson.
I would like your permission to obtain, use, and print the survey instrument presented in your work titled "Factors Influencing The Adoption Of Biometric Security Technologies By Decision Making Information Technology And Security Managers" (2005).

I will use this survey only for my research study and not in any other manner.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,

Johnathan Van Houten
Doctoral Candidate

BK

Bill Klug <Bill_Klug@bcit.ca>
Thu 5/23/2019 2:54 PM
Johnathan Vanhouten

Hi Johnathan,

Yes, you can use my survey instrument.

Would you like a copy of the survey instrument in a Word document so it is easier to copy and paste the questions?

Good luck you in your research!

Bill Klug, Ph.D.
Cloud Computing Option Head & Instructor
School of Computing & Academic Studies
British Columbia Institute of Technology
Office: SE09-100
Phone: 604-451-7148
Twitter: @BCITcloud

...

From: Johnathan Vanhouten <johnathan.vanhouten@waldenu.edu>
Sent: May 23, 2019 11:49 AM
To: Bill Klug <Bill_Klug@bcit.ca>
Subject: Request to use survey instrument

Dr. William Klug,

I am a doctoral student from Walden University working on a doctoral research study tentatively titled "Relationship Between Specific Security Concerns and CIO Intention to Adopt Cloud" under the direction of my doctoral study committee chaired by Dr. Gary Griffith. I would like your permission to obtain, use, and print the survey instrument presented in your work titled "The Determinants of Cloud Computing Adoption by Colleges and Universities" (2014).

Appendix D: Survey Instrument

Item	Question	Strongly Disagree	Disagree	Disagree Som	Neither Ag	Agree Sor	Agree	Strongly Agree								
O1	I feel that cloud computing is secure.															
O2	I feel I have a grasp on the security landscape.															
O3	The concerns I have about cloud-based security are not an impediment to adoption															
T-ST1	Shared technology is reliable.															
T-ST2	I am concerned with sharing systems across various enterprises.															
T-ST3	I am aware what constitutes shared technology or multi-tenancy.															
T-ST4	I feel as though authorization and access methods within cloud do not adequately prevent cross contamination.															
T-ST5	I would pay more for private cloud because of my security concerns regarding isolation															
T-AH1	I believe the complexity of authentication and access methods are sufficient to prevent account hijacking.															
T-AH2	I am not concerned that an unknown number of cloud provider employees will possess access to my data and services.															
T-AH3	I believe the cloud provider defends unauthorized accesses to our service machines both programmatically and through education of its employees.															
T-AH4	I understand the concept of account hijacking.															
T-AH5																
T-DP1	I am not concerned with the threat of external manipulation of my cloud data.															
T-DP2	I feel as though protection mechanisms in cloud are capable of protecting my data from modification.															
T-DP3	I am aware of the means to protect data at rest and in flight from manipulation.															
O-SC1	What is the primary business or industry of your organizati	Construction		Educatio	Energy/Utilitie	Financial S	Governm	Health	IT	Manufacturir	Professional Se	Real Estate	Retail	Telecommu	Travel/Ho	Wholesale distri	Other
	The firm size refers to the magnitude of the enterprise and reflects the market size, capital investment capability, or employee count.															
O-FS1	What would you consider the size of your organization?	Very Small	Small	Medium	Medium La	Large										
E-MI1	I am not concerned with malicious insiders (from my organization).															
E-MI2	I am not concerned with malicious insiders (from the cloud provider's organization).															
E-MI3	I believe that access methodologies employed by the cloud provider are sufficient to protect my services from malicious insiders.															
E-MI4	I am aware what a malicious insider is.															
E-DL1	The risk to leaking data is low in cloud computing.															
E-DL2	The risk to losing data is low in cloud computing.															
E-DL3	I feel that the data protections in place mirror those of the traditional datacenter.															
E-DL4	I am aware what constitutes both data leakage and loss.															
	I believe there are cloud providers that deserve our enterprise's absolute trust.															
	I trust that our cloud provider will stay abreast of security vulnerabilities and protect the hypervisors against intrusion.															
	I believe cloud providers have the trust of our customer base.															
	I am not concerned about cloud provider employees and access to our data															
E-RC1	I believe that cloud providers understand the laws and regulations for any geography in which my business would operate.															
E-RC2	I believe that cloud providers ensure their services meet the requirements across various legal entities.															
E-RC3	I believe that cloud providers can prove alignment with global regulatory requirements and maintain adequate records.															
E-RC4	I am aware of the regulatory requirements for my business sector across all the geographies we operate.															