2017

Strategic Cyber-Risk Implications of Cloud Technology Adoption in the U.S. Financial Services Sector

Olatunji Mujib Arowolo
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Olatunji Mujib Arowolo

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. Nikunja Swain, Committee Chairperson, Management Faculty
Dr. Aridaman Jain, Committee Member, Management Faculty
Dr. Branford McAllister, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Strategic Cyber-Risk Implications of Cloud Technology Adoption

in the U.S. Financial Services Sector

by

Olatunji Mujib Arowolo, CISA, CISM, CGIET, PCIP

MS, University of Dallas, Irving, TX, 2007

BS, DeVry University, Irving, TX, 2003

BEng, University of Ado -Ekiti, Nigeria, 1999

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management & Decision Sciences

Walden University

November 2017

Abstract

According to research, the risks of adopting new technology and the technological and organizational factors that influence adopting it are not clear. Thus, many financial institutions have hesitated to adopt cloud-computing. The purpose of this quantitative, cross-sectional study was to evaluate the cyber-risk implications of cloud-computing adoption in the U.S. financial services sector. The study examined 6 technological and organizational factors: organization size, relative advantage, compliance, security, compatibility, and complexity within the context of cyber-risk. Using a combination of diffusion of innovation theory and technology–organization–environment framework as the foundation, a predictive cybersecurity model was developed to determine the factors that influence the intent to adopt cloud-computing in this sector. A random sample of 118 IT and business leaders from the U.S. financial services sector was used. Multiple regression analysis indicated that there were significant relationships between the intent to adopt cloud-computing by the leaders of financial organizations and only 2 of the 6 independent variables: compliance risk and compatibility risk. The predictive cybersecurity model proposed in this study could help close the gaps in understanding the factors that influence decisions to adopt cloud-computing. Once the rate of cloud-computing adoption increases, this study could yield social change in operational efficiency and cost improvement for both U.S. financial organizations and their consumers.

Strategic Cyber-Risk Implications of Cloud Technology Adoption in the U.S. Financial Services Sector

by

Olatunji Mujib Arowolo, CISA, CISM, CGIET, PCIP

MS, University of Dallas, Irving, TX, 2007

BS, DeVry University, Irving, TX, 2003

BEng, University of Ado-Ekiti, Nigeria, 1999

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management & Decision Sciences

Walden University

November 2017

Dedication

I dedicate this paper to my close and extremely supportive parents, who have played a major role in the development of my personality, ambition, and interests. I dedicated this dissertation to the memories of my deceased father, who remained the most self-motivated and ambitious person I know. He instilled in me perseverance, setting an example by his hard work and dedicated persona.

Acknowledgments

I would like to take this opportune moment to extend my heartfelt gratitude and love to my family - To Folasade Arowolo, my wife, thank you for your support and encouragement. To my children, Olamide Toreek Arowolo, Lolade Taofeek Arowolo, and my daughter, Bisola Azizat Arowolo. Thank you for sacrificing much of your play time for your dad's achievement. My appreciation goes to my dissertation chair, Dr. Nikunja Swain, for his guidance and valuable insights starting from the Knowledge Area Modules (KAM) demonstration to completing this project. Special thanks go to Dr. Aridaman Jain, my research methodologist, for his input, constructive feedback and willingness to engage and mentor at all times. I also want to say a big thanks to Dr. Branford McAllister, the university reviewer, and all my other professors who have been part of this journey, and to my friends, coworkers and course mates for their encouragement.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Organization leaders are turning to emerging technologies, such as cloud-computing, to cut down their operational costs, and elastically meet the demands of their customers (Ardjouman, 2014). A recent report by Frost and Sullivan (2015) revealed that approximately 91% of enterprises are either currently using cloud services, or are in the planning or implementation stage. Some of these organizations are adopting cloud-computing to achieve the benefits of reduced head-count—costs associated with maintaining a large IT workforce (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Some are taking advantage of this technology to (a) cut down on their periodic maintenance costs and energy consumption, (b) do away with costly upfront investment in hardware and software, and (c) still enjoy advanced technologies at a fraction of their cost (Aljabre, 2012; Marston et al., 2011).

Cloud-computing has the potential to challenge the status quo in the financial services sector by changing the way customers receive and consume technology services (Aleem & Sprott, 2013). The emergence of this technology model has created significant opportunities and new forms of strategic benefits for both the financial organizations and their customers. While the slide towards cloud-computing has been rapid for many market sectors, cloud-computing adoption in the financial industry has been very slow (Chopra, Mungi, & Chopra, 2013). Chen and Zhao (2012) showed that security and privacy are the foremost reasons.

A 2015 IBM report reflected a serious concern in the increasing level of cyber-attacks directed at the financial industry, making this sector the U.S. industry with the

most cyber incidents in the last 2 years. This increasingly sophisticated cyber threat landscape has made the decision to adopt cloud-computing much more complicated, resulting in a wait-and-see approach (Fernandes, Soares, Gomes, Freire, & Inácio, 2014; Mandhala & Gupta, 2014).

Prior studies have identified information security and regulatory risks as the major concerns that continue to keep many financial firms from implementing the full benefits of cloud-computing (Aleem & Sprott, 2013; Dutta, Peng, & Choudhary, 2013). However, what these studies failed to cover was the degree of influence of the various security and privacy risk factors that shaped decisions to adopt cloud-computing. Security is a vast domain with varied risk attributes and, without a clear understanding of the level of cyber-risks associated with cloud-computing in the financial services sector, it is difficult for leaders in this market sector to navigate past these adoption hurdles. Therefore, scholars need to engage in a concerted effort to better shape the adopter's understanding of the real security and privacy concerns surrounding cloud-computing.

This study evaluated financial leaders' perception of security risks, specifically, those charged with technology adoption and their degree of influence on decisions to adopt cloud-computing. The focus of this study was to critically evaluate the influence of these risks using a cross-sectional approach and thus inform discussion on strategies to lessen their impacts and increase the adoption of cloud-computing in the financial services sector.

In this chapter, I cover the background, purpose statement, research question, key technical terms, theoretical frameworks, and the nature and significance of the study.

Background of the Study

The growing need for a cost-effective and sustainable technology solution to accelerate business agendas has boosted discussions about a clear strategic policy for the use of cloud-computing in financial service organizations (Rani & Gangal, 2012). A study conducted by Crosman (2010) to gauge cloud readiness showed that financial leaders are willing to move their existing technology infrastructures to the cloud and use a combination of public and private cloud-computing innovations to reduce their operational costs and meet their customer needs (Crosman, as cited by Bidgoli, 2011). Despite the benefits of cloud-computing, leaders in these firms are concerned about the potential consequences of putting their data in the cloud (Marston et al., 2011). They are worried about the current security threats landscape, and the increasing level of exposure (Zimmerman, 2014).

Scholars of cloud-computing have identified security and regulatory compliance as the biggest risks impeding the adoption of cloud-computing in the financial services sector (Rani & Gangal, 2012; Sengupta, Kaulgud, & Sharma, 2011). My review of selected cloud-computing publications, however, suggests a lack of a structured cybersecurity framework for analyzing the security risks of the cloud in the current cloud adoption literature. Given the plausible claims on the strategic implication of cybersecurity risks and the consequences of a cyber-attack if such risks were not mitigated (Pfleeger & Caputo, 2012), the need for a structured framework for evaluating cloud-computing adoption in U.S. financial organizations cannot be overemphasized. Therefore, this study could be useful as a model for predicting the influence of

technology risks on the *intent to adopt cloud-computing* in the U.S. financial services sector.

A recent cybersecurity survey conducted by Verizon offered great insights into the disruptive potentials of cybersecurity risks for businesses (Verizon Business, 2015). The study provided a holistic view of the organization's cyber readiness, with its results tailored to reflect each organization's unique risk profiles according to business sectors. The study showed that cyber-attacks against organizations, irrespective of the industry sectors, are becoming more frequent, more sophisticated, and more widespread. Although large-scale credit-card compromises of the likes of Home Depot and Target, just to name two, generated the most news in the United States, many organizations around the world have also experienced actual or attempted breaches in recent years (Verizon Business, 2015). By 2019, criminal cyber-attacks are estimated to cost $2.1 trillion, quadrupling the half a billion dollars that are currently incurred by global cyber-crime and espionage (Dawson, 2016). With public cloud-computing enabling a shared, multitenant environment, and the number of cloud adopters increasing, the threat landscape is bound to become more intensified (Bhadauria, Chaki, Chaki, & Sanyal, 2014).

A recent cybersecurity report published by the State of New York buttressed the sharp increase in cyber-attacks against critical financial infrastructure in the United States (Cuomo & Lawsky, 2014). Cyber gangs continue to aim at compromising critical financial systems to either steal money or perpetrate fraud. Such attacks have the potential to affect how people interact with their financial institutions and, more importantly, affect how they exchange information, from both social and economic

perspectives (Fernandes et al., 2014). Cyber-attacks specifically have created significant costs for the financial services sectors, representing about 76% of their incurred expenses reported in customer reimbursements, 38% due to loss of customer business, and 31% because of damage to the organizations' brands (Cuomo & Lawsky, 2014). Given the impact of a cyber-attack, it is important that business owners who are considering moving their business to the cloud (a) understand the cyber-risk implications of cloud-computing, (b) develop robust cloud security strategies, and (c) use properly structured assessment techniques to manage their cybersecurity risks (Marston et al., 2011).

To avert these risks, it is essential for organizations choosing to adopt cloud-computing to act strategically by evaluating various risk factors with the cloud and their long-term implications, instead of focusing exclusively on costs. A well-designed and well-executed risk assessment can help planners analyze and respond to risks from a complex and sophisticated security standpoint that threaten the long-term viability of their financial institutions.

The Federal Financial Institution Examination Council (FFIEC) acknowledged that new technology platforms, such as cloud-computing, create new opportunities for cyber-criminals to exploit financial services firms and their customers (Gaughan, 2015). Multiple high-profile cases of cyber-attacks have left companies with damages in the range of tens of millions of dollars. The FFIEC recently provided technical documentation (Cope, 2015) that offers guidance on evaluating cybersecurity risks for cloud adopters in the financial services environment. Despite this institutional guidance on cloud-computing and cyber readiness, administrators of many financial firms are still

unclear about which approach is best to sufficiently manage the risks. This unclear discernment of cyber-risks is a key gap that is slowing down cloud adoption (Mandhala & Gupta, 2014). General concerns about the security of customers' data in the cloud and the requirements for safeguarding strategic business information from malicious insiders across multiple cloud domains continue to impede the adoption of cloud-computing in this sector (Fernandes et al., 2014).

The complexity of the financial services regulatory landscape is another inhibitor of cloud-computing adoption that is frequently referenced in the peer-reviewed literature (Sengupta et al., 2011). Compliance measures how well an individual or organization can adopt and implement an innovation within the constraints of existing laws and future regulatory demands. Attempts to understand the regulatory implications of cloud-computing have gone beyond the consequences of tactical risk measurement processes suggested in most cloud-computing publications (Latif, Abbas, Assar, & Ali, 2014). During the last few years, the U.S. financial sector has witnessed increased and more stringent regulatory demands to minimize risks and maximize efficiency (Schwarcz, 2012). These demands have dramatically heightened the need for financial leaders to evaluate regulatory compliance as a serious business risk when confronted with the decision to use the cloud. Unlike operational or financial risks that organizations can absorb or simply transfer, maintaining regulatory compliance affects the full business spectrum. As the trend continues to grow, cloud stakeholders will need to navigate a proliferation of new regulatory requirements and proactively address them to sustain their strategic objectives.

Using cloud-computing for financial products and services requires a surgical approach to understanding its risks and benefits. The need for the financial sector to meet its strategic business objectives, safeguard the brand, and protect its stakeholders against the alarming cost of noncompliance and the potential impacts of a cyber-attack represent a few critical reasons why this study is important.

In summary, there is a gap in the literature on knowledge about the degree to which technology risks—particularly security and compliance risks—influence cloud adoption decisions in the U.S. financial services industry. As a researcher and cybersecurity practitioner with hands-on experience in the financial sector, I am cognizant of the practical cyber-risks and benefits of technology infrastructure and the disruptive potential for business of weak cybersecurity practices. In this research, therefore, I carried out a multiple linear regression analysis to examine the implications of six technological and organizational risk factors in predicting the intent to adopt cloud-computing in the U.S. financial sector. In this study, I evaluated and clarified risks associated with cloud-computing, particularly in the context of practical security and regulatory challenges surrounding the confidentiality and privacy of consumer data in the cloud. The specific problem targeted for this research—lack of knowledge and understanding about the influence of cloud-computing risks—was framed in the context of risk attributes of cybersecurity (Kallberg & Thuraisingham, 2012). The goal was to provide a holistic view of the concepts, technology, action, training, and best practices to facilitate secure adoption of cloud-computing in the U.S. financial services sector (Von Sol & Van Niekerk, 2013).

Problem Statement

Cloud-computing creates a significant opportunity for financial services firms to optimize their existing legacy technology platforms, transition away from traditional procedure-based approaches, and to add competitive dynamics to the way financial products are delivered to consumers (Ahmadalinejad, Hashem, & Branch, 2015; Lee, Trimi, & Kim, 2013). The transformative nature of cloud-computing allows for innovation and experimentation in a variety of ways (Gartner, 2011). Despite the benefits of cloud-computing, there are legitimate business concerns surrounding its adoption in this market sector. The need for financial services firms to safeguard their customer information has forced most organization leaders to delay the adoption of cloud-computing for their core business functions (Rani & Gangal, 2012; Victor & Mircea, 2014). A recent survey by Cloud Security Alliance (CSA) concluded that the preeminent security and compliance risks associated with moving their data to the cloud presented challenges to financial services organizations (CSA, 2015). The financial services leaders' concerns about protecting their customers' nonpublic information (CNPI) in the cloud, and the increased potential to fall prey to a cyber-attack using the new technology platforms, have somewhat impeded their propensity to adopt cloud-computing (Bose, Luo, & Liu, 2013).

The general problem of this study was the slow adoption of cloud innovation by U.S. financial services firms. The specific problem was the lack of knowledge and understanding of cybersecurity risks, specifically, operationalization of the common security and compliance risks that are slowing down cloud-computing adoption in the

U.S. financial sector. This quantitative study was limited to analyzing the effects of key cybersecurity concerns (Gonzalez et al., 2012; Kallberg & Thuraisingham, 2012) as a measure of both the security and compliance risks on cloud-computing adoption in financial services firms.

Purpose of the Study

The purpose of this quantitative cross-sectional study was to evaluate the cyber-risk implications of cloud-computing adoption and to increase understanding of the key cyber-risk management strategies to facilitate the adoption of cloud services in the U.S. financial services sector. To achieve this purpose, it was first necessary to analyze the financial industry's main concerns about cloud services adoption. This analysis focussed on cybersecurity requirements, consisting of the security and regulatory compliance risks, organizational risk appetite, and long-term approaches to protecting key business operations and data in the cloud. I evaluated the cybersecurity risks using a cross-sectional survey of technology leaders to develop an understanding of their strategies and thus to facilitate cloud adoption in this market sector. I examined the degree of influence of six selected risk attributes of innovation (organization size, relative advantage, compliance, security, compatibility, and complexity) based on Rogers's diffusion of innovation (DOI) theory and technology–organization–environment (TOE) framework, to predict this study's dependent variable: the *intent to adopt cloud-computing* in the U.S. financial services sector.

Research Question and Hypotheses

The following research question guided this study: What are the practical cyber-risks of technological and organizational factors that strongly influence the *intent to adopt cloud-computing* in the U.S. financial services sector?

To address the research question, I employed six constructs composing the independent variables—*organization size, relative advantage, compliance, security, compatibility, and complexity*—to measure the degree of perceived innovation risks that influenced the dependent variable: the *intent to adopt cloud-computing* in the U.S. financial services sector. I collected this information via a survey instrument and evaluated the survey questions by calculating the mean rating of the financial leaders' responses to a seven-item Likert-type survey. Each of the independent variables was an average of equally weighted survey responses measuring the benefits and cybersecurity risks associated with cloud-computing, while an interval variable measured the *intent to adopt cloud-computing* for financial services operations (dependent variable). The values ranged from 1 (*strongly disagree*) to 7 (*strongly agree*). I used IBM Statistical Package for the Social Sciences (SPSS) to analyze the relationship between each of the independent variables and the dependent variable.

The research instrument used for this study was an adapted version of the survey instrument originally developed in Tweel's dissertation (2012; see Appendix C), which has since been used in many studies on the adoption of cloud-computing including a recent dissertation study by Lee (2015) focusing on the adoption of cloud-computing in the health care sector. For my study, Tweel's survey instrument was modified to focus on

cybersecurity and innovation risk attributes of cloud-computing (see Appendix B for a copy of the survey instrument used in this study).

Given the tendency for some financial services firms to adopt cloud-computing for noncritical functions, I introduced *core services* as a control variable for the hypotheses. Consistent with a post-positivist, deterministic, research paradigm (Pierce & Sawyer, 2013), I statistically tested the following hypotheses to address this research problem:

$H1_0$: There is no significant relationship between financial institution *size* and the *intent to adopt cloud-computing* for core financial services operations

$H1_a$: There is a significant relationship between financial institution *size* and the *intent to adopt cloud-computing* for core financial services operations.

$H2_0$: There is no significant relationship between the *relative advantage* of cloud-computing technology and the *intent to adopt cloud-computing* for core financial services operations.

$H2_a$: There is a significant relationship between the *relative advantage* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H3_0$: There is no significant relationship between perceived *compliance risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H3_a$: There is a significant relationship between perceived *compliance risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H4_0$: There is no significant relationship between perceived *security risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H4_a$: There is a significant relationship between perceived *security risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H5_0$: There is no significant relationship between *compatibility risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

*H*5a: There is a significant relationship between the *compatibility risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H6_0$: There is no significant relationship between *complexity* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H6_a$: There is a significant relationship between *complexity* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

Theoretical Foundation

This quantitative study used a cross-sectional survey to investigate the cybersecurity risks of cloud-computing adoption in the U.S. financial services sector and their effects on cloud adoption decisions. The theoretical framework for this study included a combination of the TOE framework developed by Tornatzky and Fleischer (1990) and Rogers's DOI theory, because the latter reinforces the attributes of innovation adoption, particularly during the pre-adoption stage (Rogers, 2003). While Rogers's diffusion theory examines five technology characteristics (relative advantage, compatibility, complexity, trialability, and observability) and how each impacts the success of an innovation adoption (see literature review in Chapter 2), I focused on cyber risk as a measure of Rogers's DOI attributes to make them relevant to this study. The use of TOE sought insights into the organizational behavioral context (Baker, 2012; Pfleeger & Caputo, 2012) for cybersecurity processes (McCrohan, Engel & Harvey, 2010; Rabai, Jouini, Aissa, & Mili, 2013) and their influence on the adoption and implementation of a new innovation, such as cloud-computing.

I expressed this cross-sectional study in the form of a dependent variable—IT leaders' interest in cloud-computing adoption —and six independent variables. The independent variables included technological (*relative advantage*, *compatibility, security, complexity*), organizational (organizational *size*), and environmental (regulatory *compliance*) factors. These technology components were mapped to common cloud-computing security and compliance risk attributes, as identified by the Cloud Security Alliance (CSA, 2013) and National Institute of Standards and Technology (NIST) cloud

security framework (Liu et al., 2011). The integration of the TOE, DOI, and CSA/NIST cybersecurity frameworks formed the lens shaping the survey questions and capturing the perceived cybersecurity risks of the cloud in this study. Figure 1 provides an overview of the theoretical framework mapped for this study. I will explain the theoretical framework in depth in Chapter 2.

Nature of the Study

This quantitative study used a cross-sectional survey design to evaluate the relationship between two research constructs: (a) financial services leaders' perception of cyber-risks with cloud-computing, and (b) their *intent to adopt cloud-computing*. I applied the standard requirements and formats of a cross-sectional research design (Leedy & Ormrod, 2013) to assess these relationships between the research constructs in U.S. financial services firms. In the following chapters, I define the research variables, highlight the hypotheses, present the instrument and data-gathering methodology, analyze the data, and assess the findings. This study included a pilot test to ensure that the survey instrument was sound and valid (see Appendix C). I used SurveyMonkey to recruit participants with a specialized background in information technology, information security, and, more importantly, leaders who were familiar with the concepts of cloud-computing in the financial services sector.

I used the SPSS descriptive statistics procedures to analyze the data from the survey instrument. I used key elements of quantitative data analysis, including descriptive statistics and multiple linear regression to explore the relationships between the independent variables (*relative advantage, compatibility, complexity, trialability, and*

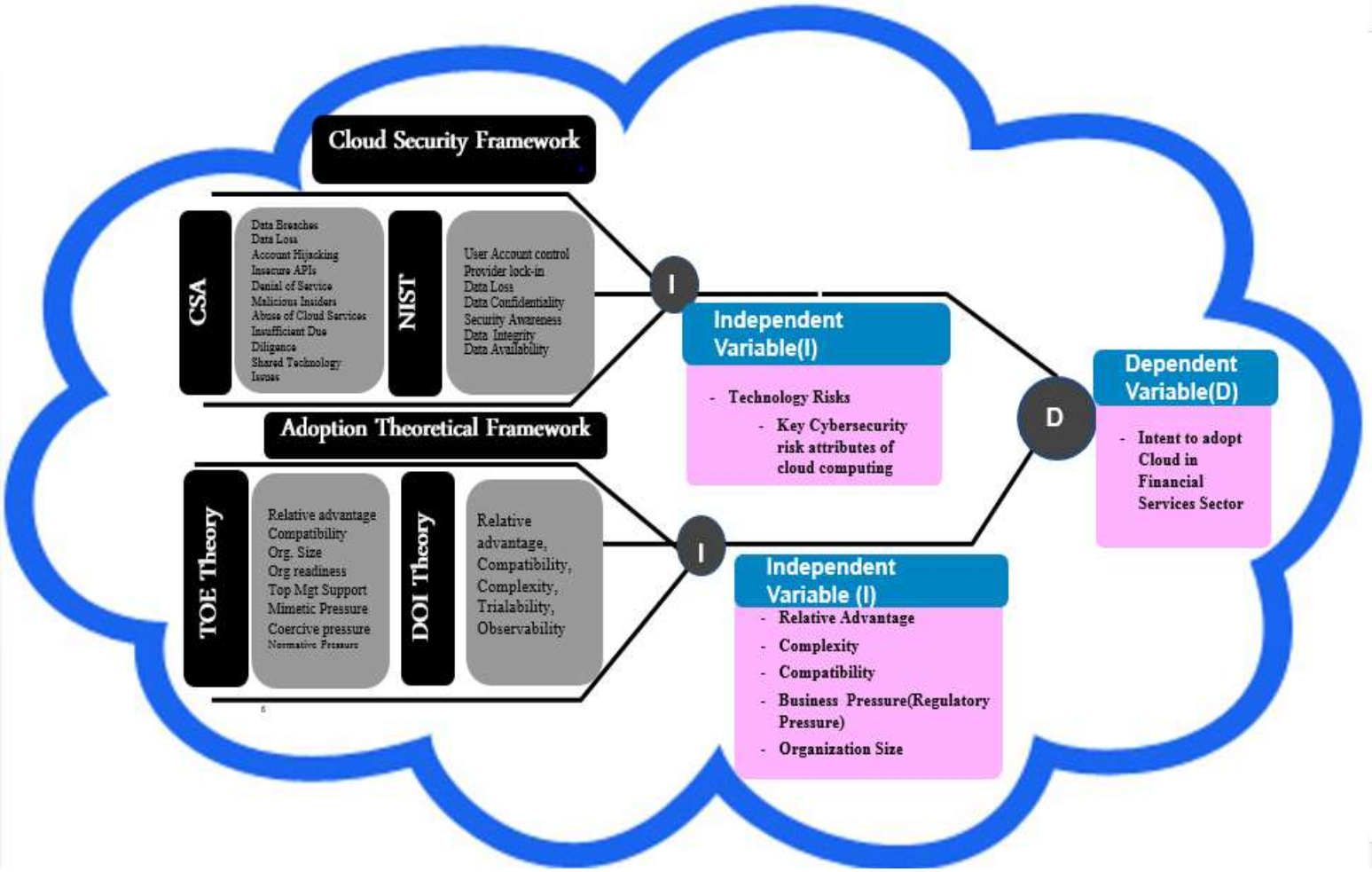

Figure 1. Theoretical foundation for the predictive cloud security framework. Framed in the context of the technology–organization–environment (TOE) framework developed by Tornatzky and Fleischer (1990), and Rogers's Diffusion of Innovation (DOI) theory, by Everet Rogers, as mapped with CSA & NIST frameworks.

observability, security, and compliance) and the dependent variable (the *intent to adopt cloud-computing* for the U.S. financial sector). In other words, using regression, I tested the relationship between (a) the collection of independent variables and each dependent variable and (b) the relationship between the dependent and independent variables individuallyThe results are presented using graphs and visual impressions to represent the respondents' perceptions for this study.

Definitions

The following technical and operational terms may have multiple meanings or may be unfamiliar to the readers of this study on cloud-computing and cybersecurity.

Access control: The established physical or logical rules to ensure a system request is valid (dos Santos, Westphall, & Westphall, 2013).

Authentication: The process of establishing confidence in user identity that the user presents electronically to access an information system (Zissis & Lekkas, 2012).

Cloud-computing: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Xu, 2012, p. 2)

Community cloud: The cloud infrastructure managed by a third-party organization that is shared by several companies to support a specific group of community members with common concerns including the mission, security requirements, policy, or compliance considerations (Zissis & Lekkas, 2012).

Compatibility: A measure of the degree to which an innovation is perceived to be consistent with an organization's needs, ideas and socio-cultural values (Daugherty, Chen, & Ferrin, 2011; Rogers, 2003, p. 15).

Compliance: Obedience to government regulations such as the Graham Leach Bliley Act (GLBA), the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security (PCI-DSS) requirements, which have created laws for auditing and accountability over access to customer non-identifiable data (Fernandes et al., 2014).

Complexity: The degree to which an innovation is perceived as relatively difficult to understand and use (Rogers, 2003). Complexities surrounding the task of managing multiple vendors and cloud providers will be a significant consideration for most cloud adoption decisions (Aleem & Sprott, 2013).

Core platforms: Important subsets of a financial services platform that include deposits, credit, loans, and product configurators, plus related basic client data (Hoppermann, 2011; Tang, Mehrez, & Tuna, 2014).

Cyber-crime: Illegal computer activity or behavior that targets the security of a computer information system and the data processed by it (Olayemi, 2014).

Cyber-criminal: A person who is involved in a crime using a computer and internet network (Lau, Xia, & Ye, 2014).

Cyber-law: The laws of the internet that govern cyberspace interactions and human protections (Droege, 2012).

Cyber-risk: The uncertain consequence of an event or an activity impacting an asset or human value (Aven & Renn, 2009).

Cybersecurity: This term is often used interchangeably with the term *information security*, and involves the collection and administration of technology tools, policies, concepts, and management processes to protect information, including the organization's and users' assets (ITU, as cited by Von Solms & Van Niekerk, 2013).

Diffusion: The process by which "innovation is communicated through certain channels over time among the members of a social system" (Rogers, 2003, p. 177).

Data encryption: The conversion of data into a form from which the original data cannot be restored without knowing the secret key (Brakerski & Vaikuntanathan, 2014).

Financial services organization: An organization or institution that offers financial products and services for consumers at a cost.

Hacking: Use of profound knowledge from computers and technology to gain unauthorized access to others' computer systems (Holt, Strumsky, Smirnova, & Kilger, 2012).

Hybrid cloud: A cloud infrastructure involving two or more clouds (private, community, or public) that is bound together by a proprietary technology that enables data and application portability (Kulkarni, Gambhir, Patil, & Dongare, 2012).

Information security (IT Security): The protection of information assets against common attacks (Whitman, as cited by Von Solms & Van Niekerk, 2013).

Infrastructure as a Service (IaaS): The computing capability provided for storage, network, and other technology services consumers can deploy and use to run their arbitrary software (Mell & Grance, 2011).

Innovation: The personification, combination, or synthesis of an idea related to an object, products, or services that one perceives as something new and potentially valuable to the adopters (Kamalian, Rashki, & Arbabi, 2011; Rogers, 2003).

Platform as a Service (PaaS): A cloud-computing infrastructure consisting of programming environments, virtualization, layered interface, and other development tools to enable consumers use the platform, with possible access to configure its settings for their own environment (Mell & Grance, 2011).

Private cloud: The cloud infrastructure specifically carved out for a private organization's use. The client organization or a third-party vendor manages the infrastructure (Mell & Grance, 2011).

Public cloud: Infrastructure that the cloud-selling organization owns but makes available to the public or a large industry group (Mell & Grance, 2011).

Relative advantage: Expressed as economic profitability, low initial cost, decreased discomfort, social prestige, savings in time, and/or a reward, is instrumental to the rate at which an innovation spreads (Rogers, 2003).

Revenue: The surrogate of the organization size to characterize the need to make quick and decisive adoption decisions to maintain and enhance an organization's competitive standing (Baker, 2012).

Vulnerability: A weakness in an information system or a poor characteristic of the system establishing conditions which a threat actor can exploit to compromise the system (Paulauskas & Garsva, 2015).

Assumptions

I made the following assumptions in this study:

- Leaders of financial services firms I surveyed for this study have similar cybersecurity and privacy requirements for managing their business data or other critical information assets that are regarded as highly sensitive to their operations, or essential to meeting their strategic business goals.
- Economic benefits such as reduced operational cost from economies of scale that are attributed to common rationales for an enterprise adoption of cloud-computing will also be relevant to firms in the U.S. financial services sector.
- Financial services leaders I surveyed for this study had decision-making capabilities, or at a minimum, were capable of influencing adoption decisions.
- Because of my professional background, recent security leadership experiences in the financial sector did not negatively influence this study.
- All the research participants had sufficient understanding of cloud-computing to provide relevant answers to the research questions as framed in the context of this cross-sectional study.

Scope and Delimitations

This study was limited to investigating the cyber-risks influencing the *intent to adopt cloud-computing* in the U.S. financial services sector. Using the lens of Rogers's

(2003) DOI theory and the TOE framework developed by Tornatzky and Fleischer (1990) as guidance, I selected six constructs (*relative advantage, compatibility, complexity, organization size, security, and compliance*) as key influencing predictors of the *intent to adopt cloud-computing* in the U.S. financial firms. The use of these factors was supported by recent studies on cloud-computing (Powelson, 2012; Son & Lee, 2011; Wu, Cegielski, Hazen, & Hall 2013).

I evaluated revenue as a surrogate of organization factor (organization size) and focused on the cyber-risk implications of all the selected constructs to empirically measure the cybersecurity risks influencing cloud-computing adoption decisions. While Rogers's (2003) DOI theory originally identified five technology factors (relative advantage, compatibility, complexity, trialability, and observability) as critical to the success of an innovation adoption, I decided to exclude trialability and observability because they show insignificant correlation for cloud adoption decisions (Powelson, 2012). I left out environmental factors from TOE, because they are beyond the scope of this study.

The scope was limited to business and technology leaders in active U.S. financial services firms. To objectively answer the survey questions and test the hypotheses, I used SurveyMonkey audience recruiting services, also known as the SurveyMonkey audience pool, to recruit participants with a specialized background in information technology, information security, and—more importantly—leaders who were familiar with the concepts of cloud-computing in the financial services sector. I used a random sampling

method with a sample framework set as the list of participants validated by SurveyMonkey and members of the SurveyMonkey audience pool.

Limitations

My choice of the six variables for this study was limited to an in-depth examination of core innovation attributes and cybersecurity variables supported by the current literature (Tweel, 2012; Lee,2015). Although I selected the variables primarily using the theoretical lens of innovation theories (Rogers, 2003; Tornatzky & Fleischer, 1990), they may not be representative of all the factors associated with cloud-computing innovation. A key limitation of many innovation studies using Rogers's DOI theory is that they are often limited in substance when it comes to the adoption implementation, provide an inexplicit generalization of conceptual constructs (Doyle, Garrett & Currie, 2014; Fichman, 1992; Klein & Sorra, 1996), and exhibit a stance on the innovation adoption process that is not sufficient or specific enough to guide organizations considering technology adoption today. With a bit of abstraction mostly from synthesizing Rogers's DOI theory with the TOE framework (Tweel, 2012), I defined the six independent variables and finally mapped the theoretical constructs with NIST standards on cloud security. I expected this study to provide evidence-based strategies that could benefit organizations facing a wave of critical decisions on whether or not to adopt cloud-computing for their core financial processes. By mapping out the theoretical components, this study could help extend the theoretical constructs of innovation adoption and research instruments to explicitly measure the perceived cybersecurity risks surrounding cloud-computing adoption.

Another limitation of this study was that, like any cross-sectional study, it was prone to sampling biases like length-biased sampling or recall bias (Mandel & Rinott, 2014). The people completing the survey can be exposed to such bias, for example, through poorly worded research questions, thus creating unintentional influence on how the survey questions are answered (Fowler, 2013). To mitigate this risk, I used an existing survey instrument that scholars conducting research in this area have previously validated, and revised it to fit this study's purpose. Given that I adapted the research instrument, I subjected my slightly modified questions to the proper cognitive and pretest processes (Fowler, 2013) in order to identify and correct all questions that could lead to any form of bias.

I interviewed subject-matter experts, queried IT leaders with decision-making responsibilities for cloud-computing adoption, and used a previously validated questionnaire with straightforward survey questions. This approach was intended to control for effects of common research bias and ensure the validity and reliability of this study.

While this cross-sectional study has the potential to extend the theoretical applicability of the cybersecurity factors underpinning the adoption of cloud-computing for the financial services sector, it was limited to the use of key respondents from that sector. Nonetheless, by ensuring that the survey participants I chose were well-grounded in this market sector and familiar with the concepts of cloud-computing, findings from this study are expected to provide useful insights into the practical and most probable cyber-risks causing the slow adoption of cloud-computing in this sector. The framework

and research instrument used in this study will therefore serve as an exploration vehicle to further examine the cyber-risk implications of cloud-computing in the U.S. financial services sector (Talib, Atan, Abdullah, & Murad, 2012).

Significance of the Study

Significance to Theory

The unclear perception of cyber-risks and its influence on the adoption of cloud-computing in the financial services sector represents a key gap in technology research that requires concerted scholarly effort (Mandhala & Gupta, 2014). While scholars have traditionally used the DOI theory and TOE framework to study innovation adoption in organizations (Fernandes et al., 2014; Talib et al., 2012), this study extends the theoretical bases by focusing on cybersecurity risk attributes of cloud-computing. I expected lessons learned from this study would help fill the knowledge gap in this area and enhance the predictive model suggested for determining *intent to adopt cloud-computing* in U.S. organizations (Lee, 2015; Tweel, 2012).

Significance to Practice

I expected this study to be useful to financial services leaders and policymakers in their effort to mitigate the effects of cybersecurity risks and to facilitate the adoption of cloud-computing in this market sector. I also anticipated that this study's findings would represent an opportunity for cloud and technology providers to strengthen their offerings. A clear understanding of cyber-risk attributes of cloud-computing could attract more contributions from both academics' and technology services providers' spheres on ways

financial services organizations can use the cloud's benefits to position themselves for economic competitiveness.

Significance to Social Change

The implications of this study for social change can be expressed in terms of operational efficiency for organizations, and cost improvements for consumers. I anticipated that a clearer understanding of the cyber-risks associated with cloud-computing would reduce financial administrators' security and compliance concerns, leading to the emergence of successful cloud business delivery models for organizations in this sector. The new cloud business model might be expected to help financial services firms expand their products and services. Also, by understanding the true cyber-risks of cloud-computing and ways to mitigate them, financial services firms' administrators would be more likely to adopt cost-effective cloud-computing to process their core business functions. Cost savings from this adoption might make financial products and services potentially more affordable to consumers.

Increasing cloud-computing adoption in the financial services sector is expected to help combat global warming. Plausible scholarly evidence shows that carbon emissions in the environment are becoming a crucial issue and have a wide range of consequences for both society and the climate (Singh, Mishra, Ali, Shukla, & Shankar, 2015). Cloud-computing has been appraised as the IT solution with the most potential to reduce paper consumption and provide energy savings and high efficiency for organizations (Liang, Liang, & Chang, 2012). Financial services firms using cloud-computing can significantly reduce the environmental pollution resulting from paper

disposal. And, increasing cloud-computing adoption in the financial services sector is likely to help reduce the disposal of large computing resources from data centers that often contributes to climate change and seriously threatens the quality of human life (Gattulli, Tornatore, Fiandra, & Pattavina, 2012; Liang et al., 2012).

Summary and Transition

Cloud-computing heralds an evolution of technology innovation with strong potential to shape how consumers gain access to financial products and services. It has the capability to revolutionize customers' experience and interaction with financial products and services. Despite the tangible benefits identified with the cloud, leaders in the financial services sector have legitimate business concerns about the cyber-risks posed by cloud-computing and the controls that facilitate a secure and compliant cloud-computing adoption in this market sector. This chapter provided background on the cybersecurity and privacy risk concerns associated with cloud-computing adoption processes and their influence on the slow adoption of cloud-computing in the U.S. financial sector.

To examine the possible ways of facilitating the adoption of cloud-computing innovation, I proposed a quantitative, cross-sectional study drawing on the theoretical frameworks of Rogers's (2003) DOI theory along with the TOE framework (Tornatzky & Fleischer, 1990). While Rogers's diffusion theory examined five technology characteristics (relative advantage, compatibility, complexity, trialability, and observability) and their implications for innovation adoption, I focused on cyber-risk to

empirically measure the theoretical factors influencing cloud-computing adoption to make them relevant to this study.

I conducted this quantitative cross-sectional study to examine the relationship between financial leaders' *intent to adopt cloud-computing* and independent variables that make up the benefits and cybersecurity risks of this technology. I expect this study's findings to reveal practical ways to securely achieve a higher rate of cloud adoption in the financial sector.

In Chapter 2, I provide a detailed literature review of cloud-computing and the theoretical foundation for this study. In Chapter 3, I go over the research design and methodology. In Chapter 4, I present the results of the study, and in Chapter 5 I provide a discussion, conclusion, and recommendations for future research.

Chapter 2: Literature Review

The adoption of cloud-computing in the financial services sector has been a contentious topic among business leaders and specialists in the field of social sciences (Apostu, Rednic, & Puican, 2012). On the one hand, some experts have argued that cloud-computing could improve competitiveness and cost benefits among businesses (Dhar, 2012; Obeidat & Turgay, 2013); on the other hand, some experts have raised concerns about the all-too-prevalent security and privacy challenges of cloud-computing adoption and the consequences for organization brands (Fernandes et al., 2014). The purpose of this quantitative, cross-sectional study was to evaluate the cyber-risk implications of cloud-computing adoption and to increase understanding of key cyber risk management strategies in order to facilitate the adoption of cloud services in the U.S. financial services sector.

This chapter provides the theoretical foundation for technology adoption, and informs the discussion of factors surrounding the slow adoption of cloud-computing in the financial services sector. The chapter begins with the search strategy, followed by an historical review of Rogers's (2003) concept of innovation adoption; it examines the foundation and development of innovation theory from its earliest form in the 1960s through the present. The next section explores Tornatzky and Fleisher's (1990) TOE framework—the primary technological and organizational factors used as foundational constructs for this study. Next, I compare the recent views of other scholars on the concepts of technology adoption, its trends, and benefits. Finally, I summarize the strategic implications of such claims.

Literature Search Strategy

In this search, I used the following online databases to obtain peer-reviewed articles and industry research articles published within the last 5 years: Google Scholar, Google, ProQuest Central, Business Source Premier/Complete, Science Direct, and IEEE Xplore Digital Library. The following search terms were used: *cyber-risk, cybersecurity, cyber-crimes, IT security, cyber-attacks, cloud-computing, , cloud agenda setting, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), strategy, Innovation theory, Diffusion of Innovation (DOI), Technology-Organization-Environment (TOE), cloud service provider (CSP), cloud banking, financial firms, financial institution, cloud, financial laws, regulation, internet banking, electronic banking, online banking,* and *mobile banking.*

Theoretical Foundation

Scholars have widely accepted the use of innovation theories as foundations for innovation adoption spanning multiple fields in the last decades (Fichman, 1992; Lin & Chen, 2012; Rogers, 2003). More specifically, scholars have used innovation theories to describe innovation adoption from multiple levels, both from social and organizational contexts (Wisdom, Chor, Hoagwood, & Horwitz, 2014). In recent years, experts have made several efforts to extend these theoretical concepts further into understanding and predicting the true premises behind technology adoption in the financial services sector (Al-Jabri & Sohail, 2012). My study reflects the growing need to use cloud-computing solutions to innovate business functions in this sector. Insights from innovation adoption processes and their inhibitors and stimulators can potentially help cloud innovation

adopters in financial organizations (Howell-Barber, Lawler, Desai, & Joseph, 2013) understand and predict the cloud's strategic implications for their business and ways to manage them effectively.

I will describe two major propositions of innovation theories—Rogers's (2003) DOI and Tornatzky and Fleischer's (1990) TOE—and contrast the theorists' viewpoints on innovation. To critically examine the extent to which knowledge gained from this relationship predicts the *intent to adopt cloud-computing* in financial organizations' settings, I will compare and contrast the theorists' explanation of the relationship between innovation characteristics, management perceptions, and organizations' risk landscape using current publications on cloud adoption processes.

Diffusion of Innovation (DOI) Theory

Rogers (1962) undertook a comprehensive empirical study in the realm of innovation and posited that the following three major factors tend to influence adoption of innovation:

- The actor's identity and perception of the innovation
- The process
- The result, the decision about whether or not to adopt an innovation

Rogers summed up these views in his description of innovation diffusion theory as an "integrated body of concepts and generalizations on diffusion; with hands-on exploration and examples that provide powerful observational evidence and reasoning on technology adoption" (Rogers, 1969, pp. 10-11). In his complementary work, Rogers (2003) defined *innovation* as a new concept or process viewed as being new, and described *adoption* as

complete endorsement of an innovation. Central to this theory was that innovation adoption follows a sequence of processes through which an adopter passes before making a decision on whether or not to accept an innovation. Thus, Rogers (2003) defined *diffusion* as the means by which an innovation is passed on to members of a group. The diffusion process progresses from the first conception of a new idea, through development of an attitude toward it, then to an intent to follow or abandon the concept, and finally to endorsement of this decision. Rogers's theoretical stance provides critical insights into the innovative behavior of individuals in a social system, creating a considerable body of research on innovation diffusion theory.

Tornatzky and Klein (1982) sparked interest in the exploration of innovation theory. Their general notion of innovation diffusion underlies, at least implicitly, much prior work on innovation research. They defined innovation as a commodity or operation that is new to its creators and/or to its possible consumers. They likened their views of innovation adoption to the decision to use an innovation, and described innovation implementation as the transformation during which adopters of an innovation become more competent and invested in using it. They viewed implementation as the critical gateway between the decision to adopt the innovation and the routine use of the innovation. The fundamental distinction between these theorists' viewpoints with respect to Rogers's definition is the extension of adoption to include the actual implementation of technology within and across organizations. By expanding the focus beyond individual adoption processes to include teams, Tornatzky and Klein created a unique opportunity to fully extend Rogers's work into organizations and communities by exploring additional

diffusion research studies by other scholars that focused on existing organizational-based innovation (Klein & Knight, 2005).

Fichman is another theorist credited with advancing innovation theory in its present form. Fichman's (1992) theoretical perspectives were similar to Tornatzky and Klein in that Fichman outlined the potential relevance of innovation adoptions to organizational settings. Fichman endorsed the need to broaden the scope of classical diffusion into organizations and decried the implicit notion that individuals only adopt innovations for their own independent use, given that they are part of a larger community of interdependent users. Fichman asserted that research studies on innovation adoption should examine large organizations (Fichman, 2004). While much of Fichman's conceptual definition of innovation diffusion theory appears to provide a useful summary, to set the stage for critical analysis of various strands of inquiry on technology adoption decisions we must understand the process that resulted in prior generalizations of innovation concepts.

Rogers (2003) proposed that DOI often unfolds as a series of processes from knowledge of the innovation through persuasion, decision, implementation, and—finally—confirmation. The knowledge phase starts with identifying information related to the innovation. Rogers submitted that during this stage, the individual has not been inspired to find more information about the innovation. The individual is exposed first to an innovation but lacks sufficient information about it.

Fichman (1977) supported Rogers's assertion that knowledge accelerates the diffusion of innovations. Fichman proposed that "organizations with greater learning-

related scale, related knowledge, and diversity are more likely to initiate and sustain the assimilation of complex technologies" (p. 5). Fichman proclaimed that the adopters' knowledge of innovation is very important because some technologies cannot be directly adopted as a "black-box" without further "tweaking" and/or "customization" to align with the adopters' needs, a characteristic Fichman evidently believed to impose a substantial burden on adopters (Fichman, 1992). As Fichman claimed, innovations that impose a substantial knowledge burden on the would-be adopters is likely to inhibit diffusion and thus requires a comparatively strong push or "babysitting" to lower the barrier and speed up the adoption.

While Fichman agreed with Rogers on the significance of knowledge, his criticism of the classical diffusion process is that it focused more on the determinants of a would-be adopter's willingness to adopt, rather than providing a holistic view of the adopter's skills and cumulative history of innovation activities as important knowledge-measuring criteria for the adopter's innovativeness. For complex technology adoption to be successful in the organizational setting, Fichman recommended that organization stakeholders take appropriate steps to overcome the knowledge barrier by investing in organization learning and working closely with the supply-side and mediating institutions to ensure that knowledge barriers are lowered over time (Fichman & Kemerer, 1997).

Tornatzsky and Klein's (1982) studies also showed that relative advantage of a particular technology innovation has a significant relationship to adoption. They believed that users are more likely to adopt an innovation if they find the innovation to be relatively easy to use. In this regard, the relative ease of use opens up opportunity for

adopters of innovation. It is important for the adopter of cloud-computing solutions to use appropriate measures to capture questions and explore possible responses to any unexpected results relating to the focal innovation (Habib, Hauke, Ries, & Mühlhäuser, 2012). Also, getting proper insights into such technologies and developing assessment criteria relevant to the organization prior to entanglement with unnecessary vendor promises is a great strategy to objectively evaluate a cloud innovation (Carcary, Doherty, & Conway, 2013). Without a clearly defined assessment, adopters are more likely to be predisposed towards different kinds of influence often staged by vendors when trying to persuade a customer to adopt an innovation (Son & Lee, 2011).

Rogers (2003) described the persuasion stage as a phase of the diffusion process where an individual takes interest in the innovation and actively seeks more information to form either a favorable or unfavorable attitude towards it. Rogers underscored the possibility that when some people have experiences with an innovation, this encourages other potential users to try it out (Rogers, 2003). As Rogers explained, use of interpersonal channels and/or internal sources to reach out to the adopters is more important during this stage in shaping the adopters' decision. As Rogers emphasized, the decision stage often represents the most difficult stage of the adoption process (Rogers, 1962, 2003). In this stage, adopters need to develop sustainable decisions regarding the adoption. Rogers asserted that they obtain critical insight through exposure to key aspects of the innovation to enable a formal decision on whether to adopt or reject the innovation. Possible actions following the decision stage include implementing the recommended innovation.

Fichman's take on the adoption decision is that an individual's or organization's decision to adopt an innovation often depends on the dynamics of community-wide levels of adoption. As Fichman claimed, factors such as "network externalities" (e.g., internet, webinars, e-mail, etc.) and "critical mass" (e.g., community of users) streamline the adoption process by utilizing instant information sharing among the adopters and thus allow the individual or organization to assert a prominent presence in a community of individuals or organizations with adoption interests (Fichman, 1992). In summary, Fichman proclaimed that organizational innovation adoption will depend on the outcomes of decisions taken at both the organization and individual levels, as opposed to adoption decisions in the classical diffusion context that were predominantly made on the individual level. Fichman argued that while the aforementioned factors are quite common in the context of IT adoption, they can limit the opportunities to apply Rogers's classical diffusion theory "as is" (Fichman, 1992, p. 1). On the other hand, Fichman subscribed to Rogers's early research on organizational diffusion (1983). Rogers's (2003) DOI theory implies that it is best that scholars examine characteristics of the individual adopter, the organizational setting, and the technology in question (p. 11). Fichman also supported the potential relevance of Rogers's claim that factors such as individual leader characteristics (e.g., attitude towards change) and organizational structure (e.g., centralization, formalization, organizational slack) are part of an important list of criteria that influence decisions to adopt an innovation and often represent factors that set the stage for innovation implementation.

Rogers believed that much of the insight developed in the implementation stage results from exploring the consequences of the decision made during the previous stage. In this stage, the individual explores the innovation to a certain degree and evaluates the reasoning behind the formulation of adoption decisions (Rogers, 2003). Rogers noted that exploring the consequences may create some degree of uncertainty in this stage, but the result will overshadow such ambiguity as the idea gains more support (Rogers, 2003). Following the implementation stage is the decision confirmation. The confirmation stage, according to Rogers, comes with reassurance of the decision made to adopt an innovation. In this stage, the individual has made a decision, but confirms the decision in order to stop or continue using the innovation to its fullest potential. As Rogers proclaims, the individual can still reverse this decision and discontinue the adoption if the individual is confronted with negative messages about decisions concerning the adoption or if there is a perceived dissatisfaction with the innovation. Possible courses of action include revising the decision and reevaluating it, or abandoning the innovation altogether and doing something else. Rogers submitted that while the aforementioned stages are important to alleviating the uncertainty surrounding the innovation adoption process, it is also important to examine certain characteristics that stimulate the rate of diffusion.

Characteristics of Innovation Diffusion

Rogers's (2003) diffusion theory included five technology innovation characteristics—relative advantage, compatibility, complexity, trialability, and observability—and the effects of each attribute on the success of an innovation adoption. Rogers noted that successful efforts to diffuse an innovation depend partly on these

aforementioned five characteristics of innovation diffusion, how innovative an individual is, and the leadership role played by such an individual during the adoption-decision process. Innovations offering more of these attributes are likely to spread exponentially in a social system and are much more likely to be adopted faster than innovations that are less framed by such characteristics. Rogers defined relative advantage as the extent to which people view an innovation as better than the process or object it replaces. Rogers argued that relative advantage, often expressed as economic profitability, low initial cost, decreased discomfort, social prestige, savings in time, and/or a reward, is instrumental to the rate at which an innovation spreads (Rogers, 2003). Rogers introduced another characteristic described as *compatibility* as an important criterion for successful adoption. The fact that some innovations offer compelling, fundamental relative advantages regarding scalability and lower running cost does not overshadow an important factor such as system compatibility, as an example, for experienced technology adopters because innovation may sometimes become incompatible with certain perceived needs or interoperability with existing products or services (Rogers, 1995). Rogers (2003) argued that the most effective mechanism for determining how well an innovation meets the adopter's needs, social values, and the opportunities envisioned for the product is a measure of the innovation's *compatibility*. Rogers defined compatibility as the extent to which users consider an innovation complementary with their standards and requirements. As Daugherty et al. (2011) aptly noted, the more an innovation aligns with users' standards and requirements, the more likely it is to be adopted. The next important attribute is complexity of the innovations. Regarding cloud solutions, Fernandes et al.

(2013) warn about the issue of compatibility with the current cloud-computing solutions. This issue, these authors say, is primarily due to the proprietary formats with current solutions. To encourage wide adoption of cloud solutions across organizations, they therefore call for cloud providers to support and adhere to open cloud standards by making sure their solutions are compatible with each other.

Rogers (2003) defined complexity as the extent to which an innovation is considered hard to comprehend and utilize. As Rogers argued, too much complexity of an innovation can be detrimental to its adoption. Regarding Rogers's (2003) applicability with cloud-computing, Obeidet and Turgay (2013) predict that as an innovation continues to diffuse throughout the industry, the ease of making transitions from traditional infrastructures to cloud-computing will appease adopters. Also, the complexities surrounding the task of managing multiple vendors and cloud providers will be a significant consideration for most cloud adoption decisions (Aleem & Sprott, 2013). Some experienced vendors often exhort their clients to try the product prior to making any final financial commitment to it.

Trialability, stated Rogers (2003), is the level one may experiment with an innovation in a restrained way. As Rogers suggests, some innovations typically involve a radical new way of doing things. Therefore, it is important to ensure that the innovation is properly experimented with or tried, especially because such innovations may supersede the things that the adopters use all day, every day. To be successful, it is essential that the innovation (like cloud-computing) is properly tried and the adopter applies the results from such trial efforts to provide a reasonable assurance of the opportunities envisioned

for the solution (Victor & Mircea, 2014). The more an innovation is tried, the more the adopter becomes confident of its favorable results. The last important characteristic is the *observability* of innovation.

Rogers (2003) defined observability as the level to which an innovation's outcomes are confirmable to others. In the context of cloud-computing, good, observable results will likely lower uncertainty about selecting the trustworthy cloud provider and speed up the rate of adoption (Habib et al., 2012; Qi & Chau, 2013). If an innovation produces no observable results, it is likely that the adopter will disregard the value of its potential benefits. That is, its value will be unknown to the adopter and, consequently, create uncertainty, an estimator behavior that slows down the rate of innovation adoptions (Cegielski, Jones-Farmer, Wu, & Hazen, 2012). In summary, Rogers argued that the availability of all five of these characteristics represents between 49% and 87% of the variation in new product adoption (Rogers, 2003, p. 221).

Tornatzsky and Klein (1982, 1999) challenged the corollary that Rogers's innovation characteristics or attributes are *sine qua non* for a successful innovation adoption, and criticized this notion on pragmatic grounds. Using meta-analytical techniques, Tornatzsky and Klein (1982) identified some classical issues with Rogers's theory of innovation diffusion model. While they found that a significant relationship emerged between Rogers's adopter categories and their views on innovations, they gave a frank negation of his description of innovation characteristics. They analyzed Rogers's view and posited that his description of innovation characteristics merely follows a retrospective approach. As they succinctly stated, "innovation characteristics research

studies should predict, rather than simply explain in a post-hoc fashion, the critical events of the phenomenon" (Tornatzky & Klein, 1982, p. 29). One interpretation of these unsatisfactory results is that innovation characteristics by themselves are unlikely to be strong predictors of adoption. Another part of Tornatzsky and Klein's criticism is that innovation should focus on both adoption and implementation. The rationale behind their argument was that the organization actor—that is, the person (executive, top management or the opinion leader) responsible for an adoption decision is likely to differ in his or her opinions when compared to the implementers (Klein & Ralls, 1995). Tornatzsky and Klein (1982) strongly posited that, irrespective of the characteristic under consideration, adoption decisions are subject to social influences and can be different across a broad range of organizations. Cegielski et al. (2012) supported the views about the organizational influence on a firm's adoption intention, particularly in the context of cloud-computing innovation. Despite Tornatzsky and Klein (1982), the results of their study showed some consistency with Rogers's view on the characteristics of innovation and their potential for a successful implementation of adoption.

Rogers's (2003) view was that successful innovation is dependent on the *innovativeness* of the individuals in a social system. Rogers described innovativeness as the "degree to which an individual or other unit of adoption is relatively earlier in adopting new ideas than other members of a system" (Rogers, 2003, p. 22). Rogers described people who are capable of influencing adoption decisions as the opinion leaders, change agents, and champions. Rogers argued that, based on the individual's

innovativeness, these adopters will fall into one of the following categories: innovators, early adopters, early majority, late majority, or laggards, as depicted in Figure 2.

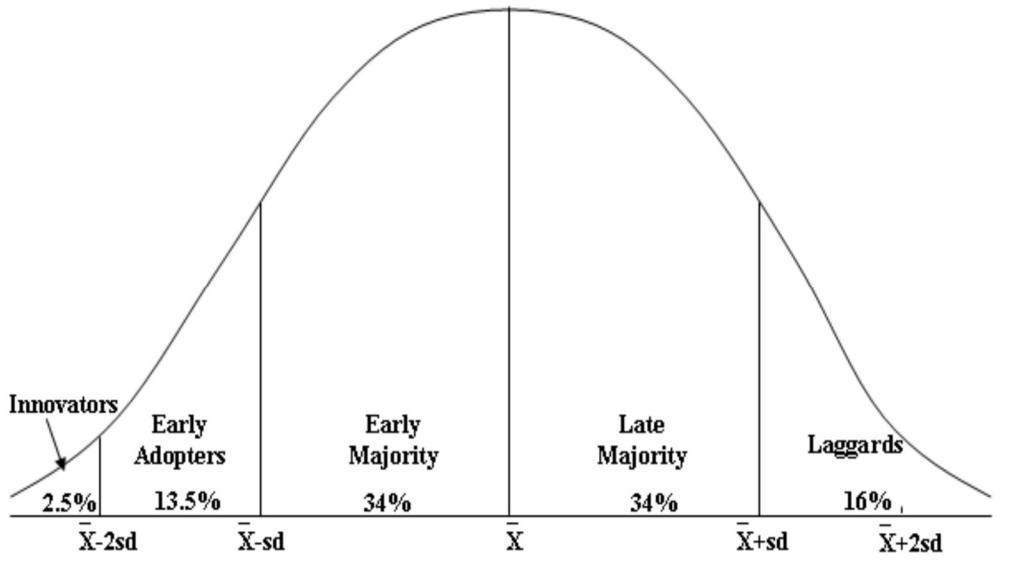

Figure 2. Adopter categorization based on innovativeness level. (From *Diffusion of Innovations,* 5E by Everett M. Rogers. Copyright © 1995, 2003 by Everett M. Rogers. Copyright © 1962, 1971, 1983 by Free Press, a Division of Simon & Schuster, Inc. Reprinted with the permission of Free Press, a Division of Simon & Schuster, Inc. All rights reserved.)

Rogers (2003) described the innovators as a group of adopters who are willing to experience innovations despite the risk of any uncertainty surrounding the adoption. The boundaries of the social system present more limitations to early adopters. Rogers (2003) argued that since early adopters are more likely to hold leadership roles in the social system, other members come to them to get advice or information about the innovation.

The early majority deliberate about adopting an innovation and they are neither the first nor the last to adopt it. The late majority is skeptical about the innovation and its outcomes; economic necessity and peer pressure may lead them to the innovation

adoption. To reduce uncertainty of the innovation, interpersonal networks of close peers should persuade the late majority to adopt it; the laggards tend to decide after considering whether other members of the social system have successfully adopted the innovation in the past. Due to all these characteristics, laggards' innovation-decision period is relatively long. Rogers (2003) argued that the availability of these five characteristics represents between 49% and 87% of the variation in the adoption of new products.

According to Rogers, successful efforts to diffuse an innovation depend partly on the aforementioned five characteristics of innovation diffusion, how innovative an individual is, and the leadership role played by such an individual during the adoption decision process. Innovations offering more of these attributes are likely to spread exponentially in a social system and are much more likely to be adopted faster than those innovations that are less framed by the aforementioned characteristics. Tornatzky and Klein (1982) seemed to believe that Rogers's and other theorists' attempt to generalize the innovation adoption process for both individuals and organizations remains unsettled because they leave no way to conceptualize innovation characteristics at the organizational level separately from individuals operating alone. As Tornatzky and Klein implied, a more useful approach would be to focus on measuring adoption characteristics in relation to specific organizational contexts.

Critics appear to be right in some sense about the limitations of Rogers's theory, especially when it comes to adoption implementation, inexplicit generalization of conceptual constructs (Fichman, 1992; Klein & Sorra, 1996; Thong & Yap, 2011), and insufficient stance on innovation adoption process that is specific enough to guide

organizations, considering technology adoption today (Son & Lee, 2011). Despite such criticisms, Fichman (1992) supported Rogers's view on innovation characteristics and acknowledged the potential relevance of his description of factors such as "individual leader characteristics (e.g., attitude towards change) and organizational structure (e.g., centralization, formalization, organizational slack)" to innovation diffusion research (p. 4). Fichman argued that the extent of divergence from classical diffusion assumptions still provides the basis for classifying IT diffusion research framework. While much of classical diffusion theory is still applicable at the individual adoption level, recent studies have shown that with a few modifications, Rogers's theory can be extended into organizational settings (Tajeddini & Tajeddini, 2012; Wu et al., 2013).

Technology–organization–environment (TOE) Framework

Tornatzky and Fleischer (1990) believed that three main themes drive top organizational innovation characteristics: technology, organization, and environment. These innovation characteristics contribute to organizational innovation dimensions: the migration of innovation from classical innovation theory to a theory that is applicable to organizations. These theorists posited that the technology factor includes a focus on key technology characteristics, including system availability. Organization factors include size, complexity, managerial structure, resource availability, and organizational communication processes. Finally, the environment factor includes certain theoretical dimensions including market sector, market structure, and government regulatory landscape.

The DOI theory and TOE framework seem to be useful in evaluating factors surrounding technology adoptions-diffusions and assessing how technology adoption can be coordinated and managed most efficiently (Borgman, Bahli, Heier, & Schewski, 2013; Chang, Hai, Seo, Lee, & Yoon, 2013). A review of the selected adoption theorists' publications shows that none of the theorists' ideas were developed in a vacuum or offer an absolute explanation of all the characteristics of diffusion; rather, their works were facilitated by the main characteristic of the diffusion process. Among the publications reviewed, Rogers's innovation diffusion theory appears to enjoy much popularity among a wide variety of academic disciplines, public entities, and private organizations; it provides insight into innovation adoption characteristics and management perception and decision processes, as well as strategies for gaining consensus on innovation adoption. His theoretical construct seems to work in many disciplines, and has been shown to hold true over the last decades through empirical evidence referenced in theorists' publications. Furthermore, scholars have argued that Rogers's approach to innovation diffusion is highly effective in explaining adoption of many types of innovations across a wide variety of settings (Fichman, 1992). Research on the diffusion of innovations centers not only on awareness—knowledge—but also on attitude change, decision-making, and implementation of the innovation (Rogers, 2003).

Recent Use of the DOI Theory and TOE Framework in Cloud-computing Adoption Research

Wu et al. (2013) applied Roger's DOI theory to critically evaluate the impact of the cloud-computing model on organizations' supply chain. The authors targeted a

sample of 1232 individuals, primarily managers, from three U.S. firms operating within manufacturing, logistics, and retail organizations. Individual members of these organizations who had expressed their willingness to participate in this study provided the basis of this sample frame. Of the individuals surveyed, about 350 completed the survey and the authors only retained about 289 surveys, resulting in about 61 unusable responses. The results of this survey suggest that despite the financial benefits of cloud-computing, business process complexity, entrepreneurial culture, and the degree to which existing information system complexities affect the innovation tend to affect an organization's propensity to adopt cloud innovation. This study supports the theoretical view of innovation diffusion, and establishes strong theoretical relevance for cloud-computing studies.

TOE also has a strong theoretical base on examining the critical factors for innovation adoption at the organizational level (Son & Lee, 2011). Previous studies have empirically supported the use of TOE for academic research in cloud-computing. Son and Lee (2011) undertook a study to examine the plausible benefits of cloud-computing investment. Using TOE as guidance, the authors used field surveys to capture data from academic and industry professionals on the organizational use of cloud-computing and to determine its economic payoffs. They carried out this scholarly investigation following careful consideration of the key tenets of Roger's classical diffusion theory as framed within the context-of-information view.

Alshamaila, Papagiannidis, and Li (2013) undertook a study to investigate the key determinants of cloud-computing adoption among small to medium sized enterprises

(SMEs). Using the TOE framework, the scholars explored the theoretical constructs underpinning the premise of adoption processes among business leaders in about 15 different SMEs in northeastern England. The use of this theoretical construct helps unveil practical recommendations to remove misconceptions about cloud-computing and factors to increase the rate of cloud adoption among these SMEs.

Son and Lee (2011) argued that the TOE framework is consistent with Rogers's innovation diffusion theory on the technological characteristics of innovation. TOE examines the internal and external organizational characteristics of innovation for the potential adopters. With TOE, researchers can address the adoption at the organizational level instead of examining it solely at the individual level (Oliveira & Martins, 2011).

I combined TOE and DOI as the foundational theoretical framework for this research. By synthesizing the TOE framework and DOI theory, I could apply both theoretical constructs to technology innovations such as cloud-computing. Mapping the key theoretical constructs from the DOI, TOE, and CSA framework for this study was potentially useful for providing a strong cybersecurity model capable of predicting the key cyber-risks that influence the adoption of cloud-computing in the U.S. financial services sector.

Literature Review

Cloud-computing

Cloud-computing heralds an evolution of technology innovation with strong potential to challenge how a marketplace receives technology products and services (Marrero-Almonte et al., 2014). Despite its hype, many organization strategists poorly

understand this concept. According to the U.S. National Institute of Standards and Technology (NIST), cloud-computing is a means of providing widespread, rapid, and easy access to the internet to a large group of users with minimal oversight or repairs (Mell & Grance, 2011). This innovation involves the provision to many customers of computing capabilities unencumbered by equipment or maintenance costs.

Cloud-computing is a relatively inexpensive and feasible platform capable of supporting dedicated computers. Its services span from networks and storage *infrastructure as a service* (IaaS) to renting computing *software as a service* (SaaS) over the internet (Mell & Grance, 2011). Since most people are already using some sort of cloud-computing services, it is relatively easy for a business strategist to use other software applications that the cloud already contains. To enable a well-rounded understanding of cloud-computing, it is helpful to take an in-depth look at the different cloud options and ways the marketplace receives these services.

Among the notable cloud-computing services are *software as a service*, or *SaaS*. SaaS offers the capability for organization users to use applications running on a cloud infrastructure via a web browser from the users' machines (that is, a laptop, personal computer, tablet, etc.) without having to manage the underlying cloud infrastructure supporting the applications (Mell & Grance, 2011). The ease with which consumers can purchase cloud applications has made the SaaS model the most widely adopted form of cloud services (Aleem & Sprott, 2013). A recent Cisco report stated that SaaS represents the highest growing cloud delivery model, and is estimated to represent about 59% of total data center workload by the year 2019 (Cisco, 2015).

Some cloud services are directly available as application infrastructure services. These services are also known as *platform as a service* (PaaS). Like SaaS, PaaS customers are able to run their application packages on the PaaS platform without having to manage the underlying infrastructure. Thus, this model is relatively cheaper for companies because the users do not need to maintain the software or hardware that are required to run the applications. A key business advantage the PaaS has over the SaaS model, however, is that it is more extensible than SaaS, and offers a number of customer-ready features, allowing PaaS customers to enjoy much greater flexibility (Fernandes et al., 2014).

Cloud-computing Deployment Models

Given the diversity of cloud services, it is essential for cloud adopters to understand how one deploys different cloud services to identify their benefits and risks. One can deploy cloud services via four different models: public, private, community, and hybrid clouds. The primary distinction among these models lies in the strategy used for housing different layers of the technology and the underlying infrastructure that different customers (also known as tenants) employ to access it, as described below.

Public. A public cloud is a deployment model whereby the cloud service provider (CSP) owns and operates the cloud infrastructure with plans to make it available for public use (Ren, Wang, & Wang, 2012). Different tenants from multiple locations via the internet (Aleem & Sprott, 2013) can access technology services housed on this infrastructure. A key advantage of this model is that it is scalable and less costly than

other cloud models. A disadvantage is that it is less secure than other deployment models (Bhaduaria et al., 2013).

Private. A private cloud consists of private infrastructure that is available to a specific customer and may reside in the internal data center of the organization, usually behind a firewall (Bhadauara et al., 2014; Fernandes et al., 2014). In this model, the customer is either responsible for the security of the infrastructure or may have the CSP take such responsibility. In comparison with other models, private clouds are more secure but require the support of highly knowledgeable IT professionals to meet organizational security requirements (Bhaduaria et al., 2013).

Community. The community cloud is a deployment model in which multiple organizations with shared business needs come together to use a cloud infrastructure (Zissis & Lekkas, 2012). Usually, this model is set up to support a group of organizations with a common business interest, security or regulatory requirements (Mell, & Grance, 2011). Cloud services are limited to members of the business sector and members of the community can access the cloud services via web browser (Aleem & Sprott, 2013). The community cloud eliminates the common security risks of public clouds and is less costly when compared with private clouds (Zissis & Lekkas, 2012).

Hybrid. A hybrid cloud model consists of a combination of private, public, or community clouds with the purpose of serving well-defined business needs (Fernandes et al., 2014). A key benefit of this model is that it provides the platform for an organization to classify which of its technology assets can reside in either the private, public, or

community cloud (Kulkarni et al., 2012). Both the adopting organization and the cloud service provider (CSP) manage this model.

With the various deployment models described above, users can now have the flexibility to subscribe to SaaS, IaaS or PaaS services or build a cloud service of their own for private or public consumption. A common feature set of these cloud options is that they involve a diffuse, distributed computing infrastructure that the web services provides (Zhou et al., 2013). This distributed approach, especially for those in the private cloud environment, uses the traditional data-center practices of isolating the server architecture to avoid heterogeneity in the server firm and thus ensures greater efficiencies in computer processing power (Zhou et al., 2013). This in turn benefits both the CSPs and the organizations adopting these services by reducing complexity and maintenance costs associated with running the cloud infrastructure. This approach thus creates a high potential for organizations to cut their expenditures and maximize their time without forgoing the benefits of IT (Moreno-Vozmediano, Montero, & Llorente, 2013).

Benefits of Cloud-computing Services

Cloud-computing reduces the potential for companies to overspend on technology, and provides other benefits needed to ensure organizational sustainability (Alzahrani, Alalwan, & Sarrab, 2014; Garg & Buyya, 2012). The convergence of multiple trends in information technology has largely made possible the emergence of cloud services. The flexibility to use utility computing, or virtualize different IT service management models, has essentially led to the increasing trend of external deployment of IT services (Zissis & Lekkas, 2012). This new capability allows organizations to pay just

for the computing services they need. A chief benefit to this approach is that it helps organization stakeholders stop worrying about unplanned costs of IT (Martens & Teuteberg, 2012). As Dhar (2012) aptly puts it, cloud-computing lowers costs in two basic ways: first, by employing preexisting information technology software and hardware, and second, by simplifying information technology operations. The new shift from being capital-expense-centric to paying only for services used creates scale economies (Wang, Zhan, Shi, & Liang, 2012) and offers a unique opportunity for these organizational stakeholders to trim down their expenses and properly budget for what is needed to run their IT shops (Whaiduzzaman, Sookhak, Gani, & Buyya, 2014). Marston et al. (2011) also provide specific evidence to substantiate the benefits of cloud-computing services. According to these authors, organizations adopting cloud-computing can reduce costs associated with maintaining a large IT workforce, periodic maintenance costs, energy consumption, and costly upfront investment in hardware and software, as well as the hidden costs of unplanned system outages or natural disasters.

Another important profit aspect of cloud-based technology is the great deal of flexibility it offers (Zissis & Lekkas, 2012). Cloud-computing allows companies to focus on their core competencies rather than being preoccupied with developing and managing technology infrastructure (Dhar, 2012). Given the flexibility with cloud-computing, companies can rent pieces of underlying computer infrastructure or a development platform that is already running the required applications and technology resources without having to purchase extensive cost-intensive hardware and software to build the infrastructure from scratch (Xu, 2012). This, in turn, makes it efficient for organizations

to provision and deliver their technology products and services, an accelerating trend that helps businesses gain a competitive edge (Mell & Grance, 2011). Given this new capability, organizations can therefore benefit from the accelerated time to market through reduced technology costs, increased capacity, reliability, elastic IT services, and improved performance requirements associated with the automation of their business process activities to provide scalable solutions (Jadeja & Modi, 2012).

The scalable use of cloud-based technologies and the increased speed of deployment they offer can be helpful for organizations that need to expand their IT provision to meet increased operational demands. In other words, with cloud-based technologies, organizations can promptly react to changing business demands without incurring unnecessary costs that have historically been associated with the traditional IT delivery model. Cloud-based technologies also reduce unnecessary costs such as those associated with delays (both in the time spent and the use of resource efforts for provisioning in-house systems), allowing IT stakeholders to provide more efficient IT solutions on demand. The ability to rent IT infrastructure as needed allows IT services to scale up smoothly, lowering common barriers for startup companies and promoting innovation as well as a level ground for competition (Victor & Mircea, 2014).

Use of Cloud-computing in the Financial Services Sector

The financial industry has faced many challenges in the last few years. First, there is pressure to streamline financial operations and enable contemporary products and services that reflect today's consumers—convenient, mobile driven, and socially engaged customers (Saarijärvi, Grönroos, & Kuusela, 2014). Second, there is a regulatory need to

adapt to the low interest rates strategy posited by the Federal Reserve in reaction to the recent economic downturn, which has created very low margins and profitability for organizations in this sector (Bassett, Lee, & Spiller, 2015). The combination of these strategic needs, when combined with the costs associated with meeting the industry's stiff regulatory and compliance requirements, creates tremendous challenges for organizations in this market sector. Despite these challenges, discussion about transforming financial services platforms using cloud-computing continues to gain a high importance in the boardrooms (Zimmerman, 2014). One reason why cloud-computing has become a perennial topic in this discussion is that for many financial organizations, cloud-computing represents a huge mechanism for reducing their reliance on expensive, branch-focused distribution core platforms and opens unbounded possibilities to shift their approach to a customer-centric model to achieve sustainable growth (Valentine, 2013). This debate over superseding the traditional core platforms with cloud services, in a way, has become a crucial strategic discussion for business competitiveness (Victor & Mircea, 2014).

Cloud-computing strategically positions financial organizations for unfolding business possibilities and serves as a speedy platform to get there (Demirkan & Delen, 2013). It allows financial firms to innovate quickly by using new capabilities: for example, organizations adopting cloud-computing can deliver new cloud services quickly and easily in a range of forms, from online banking, to mobile banking, ATMs, dialers, and relationship management, among others that offer significant benefits at a fraction of their cost. Specifically, cloud-computing can help financial services firms shift their IT

spending from capital expenditure (Capex) to operational expenditure (Opex) and therefore reduce costs associated with running traditional technology platforms via the economies of scale built into the cloud-computing platforms (Wang et al., 2012). Adopting cloud-computing platforms can increase the industry's flexibility and—if they are well designed—enhance the capabilities of the industry's existing products and services landscape. In more particular terms, cloud-computing can:

Reduce service costs to financial firms. Use of cloud-computing reduces capital investments in large technology hardware, software, storage and expensive data centers to a model where a firm only pays for the capacity needed for a service. Put differently, cloud-computing changes the expensive traditional technology delivery model to an affordable pay-per-use model (Frăţilă, Zota, & Constantinescu, 2013). Thus, organizations in this sector will be able to offer cost-effective services to their consumers.

Enable contemporary product and service offerings for consumers. An important trend in the financial industry is the ability to eliminate the commercial and technical fragmentation that has become a serious barrier to successful introduction of contemporary products and services for consumers. Cloud-computing bridges the gap between the financial applications providers, operators (Prasad, Gyani, & Murti, 2012), and consumers, and makes it possible to meet the trends consumers have come to expect in today's services. For example:

- **Mobile cloud-computing.** Mobile cloud-computing is one of the mobile technology trends capable of shaping the future of the financial services sector. It combines the advantages of both mobile computing and cloud-

computing, thereby providing optimal services for the consumer on the go. Common applications consumers can use with cloud-computing platforms include mobile commerce, mobile learning, and social networking, among others (Alzahrani et al., 2014).

- **Cloud-based dialer.** The advent of cloud-computing has allowed the possibility of moving basic financial services functions such as lending, deposits, insurance, mortgage processing, payments, and claims, to mention a few, to the cloud. With software such as the claim processing application in the cloud, for example, several financial services firms can take the advantage of this innovation to reduce costs associated with using traditional dialers. A report published by Accenture shows how a financial firm, SunTrust, was able to use cloud dialers to efficiently reduce its inbound calls and lessen its overall loss mitigation timeline (Accenture, 2009). According to this study, the company saved almost $25 per call, and cut first-payment defaults by more than 60% simply by using a cloud-based dialer to deliver routine requests for borrower information (Sardet & Viale, 2012). This case study is a prime example of how adopting emerging technologies such as cloud-based dialers can help position financial firms to take advantage of unfolding opportunities.
- **Relationship management.** Cloud-based technologies can empower consumers by enhancing the financial services industry's relationship management process. A study by Wu et al. (2013) shows how a financial services firm saved a great deal of time and resources by having users from

across their organization use Salesforce, a collaborating tool, to access their data from a Web browser. The ability for financial services organizations to use a wide variety of cloud-based customer relationship management applications not only positions them against global competitors, but facilitates new business propositions through compelling insights into customer needs (Chuang & Hu, 2015).

- **Automated teller machines in the cloud.** A major advancement in banking is the development and evolution of automated teller machines (ATMs) in the cloud. Companies like Telcos and NCR, for example, have started using their network assets to offer ATMs in the cloud. This new technology innovation will reduce the cost of running an ATM network by up to 40%, as well as speed up deployment of new ATM services (Accenture, 2009; Hogben, 2016). Financial services core platforms in the cloud can deliver on both cost and flexibility.
- **Front-office apps in the cloud.** Interest in using cloud applications for financial services is still immature and often restricted to pilot projects and proofs of concept, mainly from outside core financial service areas (Aleem & Ryan Sprott, 2012). Accenture predicts that financial firms will need to use the cloud to stay ahead of their competition and to boost their agility and customer responsiveness (Accenture 2009).

As noted above, the financial services sector has compelling reasons to use cloud-computing, including lower costs, standardization, and consistency (Cegielski et al.,

2012). Cloud-computing has the potential to make financial firms more agile and responsive to dynamic business demands and unique customer needs. It is becoming a platform for financial organizations to deliver new products to market faster, accelerate their growth agendas, trim down costs, and survive a tough economic climate. Organizations adopting cloud-computing can yield the benefits of reduced head-counts and enjoy the use of advanced technology at relatively lower costs to run and maintain their businesses (Marston et al., 2011). Cloud-computing can provide better cash flow and greater financial visibility for financial services organizations by changing the cost model from Capex to Opex (Apostu et al., 2012). Cloud-computing offers important benefits, including a low-cost "pay-as-you-go" business model for organizations, greater portability, and the ability to access business information from virtually anywhere, any time, and from any device. Also, the rapid provisioning and elastic scaling of cloud services allows organizations in this market sector to focus on their core competencies and add value to their businesses (Son & Lee, 2011; Zimmerman, 2014).

Current Challenges with Using Cloud Platforms in the Financial Services Sector

A key issue with the adoption of cloud-computing in the financial services sector is that most cloud offerings have yet to meet the specialized functions that most financial firms need (Nicoletti, 2013). While a number of cloud applications such as human resources (HR), SaaS, and Disaster recovery apps, including other non-core operations apps, are gaining traction, others have yet to reach a viable scale (Kushida, Murray, & Zysman, 2015).

Another drawback is an organization's risk concerns with this technology model (Sommer, Nobile, & Rozanski, 2012). The ambiguity that comes with security and privacy concerns, particularly for organizations where customer data and/or the company trade secret is considered a strategic asset, continues to fuel the debate about the use of cloud-computing for core financial services (Ren et al., 2012). Other customer-related security risks, including loss of governance, vendor lock-in, isolation failure, compliance risks, insecure or incomplete data deletion, data leakage, and malicious insider sabotage continue to top the list of common risks associated with financial services firms' use of cloud-computing (Fernandes et al., 2014). Next, I further explore a detailed description and analysis of the inherent risks of cloud-computing for financial services firms.

Critical Analysis of Inherent Risks of Cloud-computing to Financial Services

Cloud-computing has many inherent risks, including: loss of control, internet reliability, availability, lack of regulatory guidance, and several other security concerns (Géczy, Izumi, & Hasida, 2012). The fact that data is stored, for example, outside an organization's data center reduces stakeholders' confidence in cloud services, and has essentially broken the traditional sense of security, particularly, the management assertion that the data will only be accessed by people with legitimate business needs of the organization. This lack of data-centric security approach at the cloud level causes much of the concerns of cloud-computing, and, has resulted in most often-debated issues on security and compliance risks of the cloud (Rani & Gangal, 2012). Fernandes et al. (2014) highlight the risk posed by using non-standard infrastructure for cloud-computing services. As these authors argue, providers today use different infrastructure standards

and formats for their cloud services. The packaging and features, licensing, and pricing vary from one cloud-offering vendor to another. Given these differences, it is very difficult to see two vendors that are similar both in service offerings or technology infrastructure. Buyers of such services are therefore locked in to a specific vendor technology or service, and thus are potentially deprived of switching services between vendors at will. From an economic perspective, this lack of standard service offerings or incompatible infrastructure limits competition, and subjects organizations to a failing vendor or technology.

Another fierce concern for cloud skeptics is the availability and reliability of cloud services (Habib et al., 2012). While cloud advocates may favor these services for several reasons (including the cost savings from equipment repairs, or even personnel required to run traditional technology services), there are potential costs of failure caused by system downtime, not the least of which is a bad reputation for providing a client's customers with unreliable services. For cloud-computing to become an attractive option, organization strategists must be certain that proper controls are in place to ensure services are available to their customers whenever they need them (Xu, 2012). One solution will be to evaluate the business impacts—the recovery time objectives—and incorporate those time objectives into a mutually developed business continuity plan. While this approach may work well for some cloud providers, the potential impact of committing to specific time objectives can be unacceptable for providers in a multitenant environment with a variety of supported applications and/or users. The other option would be to have the

provider commit to an agreed-upon service level and establish processes to monitor their compliance (Obeidat & Turgay, 2013).

Another highly debated issue when it comes to accessing business technology via the cloud is slow internet speed (Géczy et al., 2012). Internet speed is important for cloud services but continues to pose significant challenges in many geographical regions around the world, particularly in developing countries. Accessing business technology from the internet instead of a localized data center reduces speed and continues to aggravate the challenges that come with system availability and reliability of internet connectivity. For example, using security measures such as encryption to protect critical data in the cloud creates an additional bottleneck for connectivity given the time to decrypt the data. Even though it is a good practice to do so, it slows down information access and places an additional burden on the already strained network bandwidth.

With consistent threats from cyber-criminals, adopters of cloud ccomputing are likely to think twice about cyber-risks (Rabai et al., 2013) and the potential to lose their data privacy due to the multi-tenancy aspect of this technology. Among the chief security concerns are: high risks of data breaches, distributed denial of service (DDOS) attacks leading to significant service downtimes (Bhadauria et al., 2014), and the absence of visibility that adopters of this new delivery model have over who is accessing the organization's data, which potentially creates a lack of trust and elevated privacy concerns.

In addition to all the risks described above, adoption of cloud ccomputing comes with enhanced privacy concerns. For many large organizations with stringent privacy

requirements such as healthcare establishments, banks, and other financial industries, adoption of cloud-computing means such organizations need to relinquish their controls to the cloud provider. Any exposure of the business data, without doubt, will become a serious issue to the organization and can be problematic to solve. Such potential for data exposure thus raises the barrier for cloud adoption (Chopra et al., 2013).

Moreover, system unavailability that has traditionally been occasioned by unplanned technology changes may now be a trigger for cyber-attacks or data breaches. As theft-oriented cyber-attacks proliferate, adopters of cloud-computing will need to add to their worry list the responsibility for cyber incidents and the need to establish controls to reduce their impacts on brand image, customers, and the organization's long-term survival. The explosion of data breaches will adversely affect not only customers' and organizations' intellectual properties, but will also have a material impact on organizations' market competitiveness, resulting in the restricted use of cloud-computing to build their businesses and save costs (Brender & Markov, 2013).

The lack of regulatory guidance for cloud services is another potential risk of cloud-computing (Frăţilă et al., 2013). In the last few decades, there have been a record number of data-centric regulations enacted such as the Graham Leach Bliley Act (GLBA), the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security (PCI-DSS) requirements, which have created various alarming requirements for auditing and accountability over access to customer non-identifiable data (Fernandes et al., 2014).

Xiao and Xiao's (2013) article reveals concerns related to managing confidential business information in the cloud. Although these scholars acknowledge that cloud critics have decried the use of such services for storing sensitive data in the cloud because of various compliance and legal requirements, their position is that when organization stakeholders are properly armed with applicable requirements for their data and business functions, they will be able to address the regulatory and legal risks surrounding the privacy and security of such information assets, both internal and customer data. Pearson (2013) believes that as cloud-computing becomes more pervasive, pressure will intensify on both cloud providers and organizations to figure out key compliance and privacy requirements and integrate them into cloud services.

Cloud-computing, like any other innovation, has risks and benefits. It is very evident from the literature review that cloud-computing presents a class of strategic risks, from adoption risk to security and privacy concerns. Since cloud-computing has the potential to create significant opportunity and new forms of strategic advantage on both the provider and subscriber sides, it is critical for organizations' strategists to engage early to build capability and to systematically evaluate the associated risks and/or disruptive potentials. By analyzing the pros and cons of this innovation, cloud stakeholders can make informed decisions about the potential benefits of cloud-computing and integrate them with the array of differing business premises or concerns surrounding its adoption. In addition to understanding the risks and benefits, exploring key maturing capabilities of the cloud providers before procuring a cloud solution is a

proactive means of navigating the hurdles with cloud use (Smedescu, 2013) and taking advantage of the array of benefits that are inherent in cloud innovation.

Quantitative Research Relative to Cloud-computing Studies

Adoption and use of cloud-computing by organizations has received considerable scholarly evaluation in the last five years. Of the over 100 articles reviewed for this research study, the majority of cloud-computing scholars have used quantitative research methods. Using a quantitative research method seems appropriate for examining factors that influence administrators' decision to embrace innovation in their organizations. For example, Habib et al. (2012) conducted a study to evaluate the current landscape of cloud-computing, the benefits, and disadvantages of the cloud from consumers' perspective. Their study used cross-sectional survey methods to evaluate the existing trust and reputation systems in various application domains, characterizing their individual strengths and weaknesses. The goal of Habib et al.'s study was multiform: (a) to examine the importance of trust in cloud adoption, (b) to assess the significance of trust as a facilitator for cloud adoption, and (c) to discuss the requirements for establishing trust and supporting systems to guide consumers as they establish business relationships with their cloud providers. Habib et al.'s results show that many cloud providers are not forthright with their service dependability. The lack of meaningful information to gauge the service providers' dependability thus creates mistrust. A key conclusion from Habib et al.'s study was that for cloud-computing to truly be successful, cloud providers need to consider trust and reputation concepts as key facilitating factors for consumers to adopt and fully embrace cloud-computing in the U.S. financial sector.

A key strength of Habib et al.'s (2012) study derives from their evaluation of technical and non-technical factors that create mistrust in cloud-computing relationships. The selection and enumeration of the risks and their implications for cloud-computing justify the inferences drawn from the study. The researchers skillfully extended the taxonomy of cloud-computing to facilitate the reader's grasp of the various market structure aspects of cloud-computing. They also measured and established the internal consistency of the research data to further authenticate the correlation between trust, reputations, and cloud adoption from the consumers' perspective.

Wu et al. (2013) created a survey method to evaluate the impact of the cloud-computing model on an organization's supply chain. The authors targeted a sample of 1232 individuals, primarily managers, from three U.S. firms operating within manufacturing, logistics, and retail organizations. Individual members of these organizations who had expressed their willingness to participate in the study provided this sample frame. Of the individuals surveyed, about 350 completed the survey and the authors retained about 289 surveys, resulting in about 51 non-usable responses.

While the research design used in all these studies followed the same basic reasoning, the sphere of scientific writing captured their originality. A common approach used in studies with quantitative design includes the identification of question(s) sought after for the study, followed by presentation and clarification of the problem. The authors seem to pay attention to determining the information required for study, and provide detailed information on the instrument used in the study. For most articles, the authors tend to dedicate a section to offer convincing explanations about the methods used to

obtain the data, organize the data, and ensure the data was valid and reliable. Finally, each article contains a section where the authors present a careful analysis and interpretation of the results to justify their conclusions.

The use of quantitative study methods as noted in the above studies supports the theoretical approach of testing correlations between innovation attributes and risks associated with cloud-computing. A quantitative research method is relevant to this study, as it may offer insights into the required research approach for evaluating specific concerns and complexities related to adopting innovations like cloud-computing. By using quantitative methods, I examined subject-matter experts' critical views on discerning the cyber-risks associated with the nascent adoption of cloud-computing in the U.S. financial services sector.

Summary and Conclusions

As demonstrated in the literature review, Rogers's (2003) DOI theory and Tornatzky and Fleischer's (1990) TOE framework laid the foundation for much of the scholarly work that has been conducted over that last few decades in the realm of innovation adoption. These theoretical models are useful for understanding factors that influence the adoption of technology in organizations. The literature review has offered an historical review of innovation theories that led to the development and refinement of innovation adoption theory. It provided insights into technology (relative advantage, compatibility, complexity) and organization (size) factors influencing the *intent to adopt cloud-computing* in U.S. firms (Lee, 2015; Wu et al., 2013).

Some scholars have expanded the discussion by identifying security and compliance as two of the key factors inhibiting the adoption of cloud-computing in U.S. financial services organizations (Frăţilă et al., 2013; Ren et al., 2012) in recent years. However, still missing in this scholarly debate are the risk implications of those technological and organizational factors and the degree to which they influence the organization leaders' *intent to adopt cloud-computing*, particularly in the U.S. financial services sector. Although treating security as a classic risk factor may gain acceptance at the leadership levels for most organizations, the need for security and its implications for cloud adoption vary from one business to another. For example, while the need to store organization data in the cloud may not be as much of a concern in the accommodation and leisure sector, the privacy and confidentiality requirements for customer data in the financial industry may make security risks a go/no-go decision point for cloud decision-makers. Identifying security as a risk to cloud adoption decisions is one thing, but translating it to specific risks relevant to the organization has a greater potential for shaping executives' true risk perceptions and their effects on their adoption decisions (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013).

This research study is the first to present a survey focusing on the technical and non-technical assessment of risk factors impeding the adoption of cloud-computing in the financial services sector. In this literature review, I discussed cyber-risk as an extension of common security risk taxonomy of cloud-computing to better understand the diversified views of security and compliance risks relative to the adoption of cloud-computing in the financial services sector. My study will fill a gap in understanding of

the cybersecurity concerns with cloud-computing in the U.S. financial services sector and their implications for cloud innovation adoption decisions. I expect this study to be useful to business leaders and policymakers in this sector in their quest to facilitate the adoption of secure cloud services for financial services core operations. Insights from this study will help cloud-computing providers identify ways to strengthen their offerings to enable the adoption of secure cloud services. It expands the literature on strategies for secure cloud adoption and holds the potential to encourage financial services firms to better use the benefits of cloud-computing to position themselves for business competitiveness.

The use of quantitative methods for this study supported the theoretical approach of testing correlations between the cyber-risk attributes of innovation constructs and the *intent to adopt cloud-computing*. A quantitative research method was relevant to this study, as it offered the potential to empirically examine specific cyber-risk concerns related to cloud-computing and their degree of influence on innovation adoption decisions. By using quantitative methods, I brought a more informed approach to understanding cyber-risks that are responsible for the slow adoption of cloud-computing in the U.S. financial services sector.

Chapter 3 details the methodology used for this study. It provides information on this study's applications to professional practice, and their implications for social change.

Chapter 3: Research Method

The purpose of this cross-sectional study was to assess the relationship between the *intent to adopt cloud-computing* and key adoption cyber-risk variables—security and compliance—in the U.S. financial services sector. For this evaluation, I recruited IT leaders from the SurveyMonkey audience service who had been validated as employees of at least one of the U.S. active Federal Deposit Insurance Corporation (FDIC)-insured financial services firms.

In this chapter, I will define the research variables, highlight the hypotheses, and present the methodology used for gathering and analyzing the data. I will provide critical analysis of the instrument I used to capture data, analyze the data, and assess my findings. Finally, I will touch on the design protocols I followed to ensure an adequate coverage of this study's population, the ethical procedures to safeguard the privacy of the research participants, and plans to ensure clarity of my study.

Research Design and Rationale

I followed a traditional quantitative research methods framework using a cross-sectional survey design strategy to examine the effects of cyber-risks on the *intent to adopt cloud-computing* innovations in the U.S. financial services sector. The ease of conducting research in a natural, real-life setting anchored my choice of a cross-sectional research design for this study (Abbott & McKinney, 2013). The cross-sectional survey design is popular in social sciences to estimate the distribution of a population of interest at a given point in time (De Vaus, 2013). Cross-sectional scholars use surveys as key

instruments to elicit data necessary to evaluate the explanatory variables and outcomes of a study (Fowler, 2013).

I used cross-sectional survey design to examine the relationship between each of the independent variables comprising the perceived cyber-risks of cloud-computing and the dependent variable: financial leaders' *intent to adopt cloud-computing*. The use of a cross-sectional design was appropriate for this study given that I was working with professionals who had decision-making authority over adopting technological innovations in the financial services sector. Researchers can rely on the information acquired from them to make inferences about a larger population of firms in this sector.

The use of a cross-sectional survey design is popular in social sciences partly because of its flexibility (Blair, Czaja, & Blair, 2013). The ability to use statistical samples ensures an adequate representation of the population while eliminating systematic bias (Frankfort-Nachmias, Nachmias, & DeWaard, 2014). It also gives researchers the ability to use technology—email and internet, online questionnaires, telephone surveys or interviews— or non-technology channels such as mailed questionnaires, face-to-face interviews, or a combination of those channels, to reach out to a multitude of people who are geographically dispersed (Dillman, 2011; Frankfort-Nachmias et al., 2014).

Although researchers boast of cross-sectional design as an excellent way to bring to bear key associations between explanatory variables and outcomes, it is not without its limitations. Cross-sectional design is prone to sampling biases like length-biased sampling or recall bias (Kraemer, Yesavage, Taylor, & Kupfer, 2014). Poorly worded

research questions can expose such bias to the person completing the survey, for example, thus creating unintentional influence on how the survey questions are answered (Fowler, 2013). Researchers are advised to be cognizant of this potential design error when developing survey questions and thus take appropriate steps to limit them (Sobol, 2014). For the data-gathering phase of this study, I adapted questions from a previous study (Tweel, 2012) that has undergone proper due-diligence processes, and developed new questions focusing on cybersecurity. Given that I introduced additional questions, I subjected these to proper cognitive and pretest processes (Fowler, 2013). Pre-testing the questions confirms that the researcher will administer new questions to a sample population test group to spot-check poorly worded questions and/or identify those with the potential to lead to some types of bias (Fowler, 2013). As Fowler (2013) also warned, the questions used in surveys may sometimes be poorly worded or improperly arranged. Accordingly, the lack of proper sequence of the survey questions may thus influence low response rate.

Fincham and Draugalis (2013) agree on the importance of properly worded survey questions and the need for a high response rate as essential steps to ensuring a quality survey, but they caution researchers against perceiving them as the absolute criteria for quality survey research. These authors pointed out that, in some studies, standards for research methods may have been proposed, implemented, and well accepted but fall short of the requirements for other studies. I therefore conducted a thorough scrutiny of refereed journals and associated references lists to improve this study's design, methodology, quality, and validity of the conclusions. To compensate for any

residual limitations, I also used other strategies, including triangulation, to avoid exclusion and non-response (Lameck, 2013).

Traditional experimental designs were not appropriate for this research study given that no external response to a stimulus was required, nor was there a reason to investigate causation for any observed phenomenon. Experimental research is appropriate when investigators want to test the impact of a treatment by controlling for factors that influence the outcome (Mayoh & Onwuegbuzie, 2013). Since the primary goal of this study was to understand the relationship between perceived cyber-risks and the *intent to adopt* cloud innovations, it was logical to eliminate this type of design. Additionally, the use of a quasi-experimental design was not feasible for this study because it was impractical to put the research sample into a matched group given that their perceptions of risks may change over time (Arthur & Hardy, 2014).

In sum, a cross-sectional research design is useful in social sciences because of its flexibility and uniqueness in carrying out a study in natural settings. While the choice of this design may limit the internal validity of this study, controlling for external validity, ensuring a properly designed research instrument, and taking representative samples will enhance the quality of this study. In addition to using an instrument that has been previously validated, I adhered to best research practices in designing the contents of the measurement instrument to reduce common flaws associated with this type of research design and to increase the quality of my research outcome (Lameck, 2013).

Methodology

This study followed traditional quantitative research methods using a cross-sectional survey design strategy to examine the effects of perceived security and compliance risks on the intent to adopt cloud-computing innovations in financial institutions. The use of this design also allowed me to conduct this study at a point in time, as opposed to having to examine the research problem through multiple research studies covered over an extended period—an expensive research approach notably associated with longitudinal studies (Frankfort-Nachmias et al., 2014; Maxwell, Cole, & Mitchell, 2011).

I used the cross-sectional survey design to examine the relationship between each of the independent variables comprising the perceived cyber-risks of cloud-computing and the dependent variable: *intent to adopt cloud-computing*. This is preferred to other designs such as experimental or quasi-experimental given that volunteers who are Subject Matter Experts (SMEs) were relied on to be sampled for this study (Knight, 2010). Cross-sectional survey design provides researchers the ability to choose a large enough sample to ensure adequate representation of the population to arrive at logical findings without compromising the urge to randomize the selected sample (Frankfort-Nachmias et al., 2014).

Target Population for the Study

The target population for this study consisted of business and IT leaders from active financial institutions within the four U.S. geographical regions: West, Midwest, Northeast, and South. The participants were key technology decision-makers from the

U.S. active Federal Deposit Insurance Corporation (FDIC)-insured financial services firms. The population were primarily members of SurveyMonkey audience pool whose backgrounds were specifically tailored to ensure they provided diversified views of technology, security, and compliance functions relative to the adoption of cloud-computing in the financial services sector.

Sampling and Sampling Procedures

Evidence has shown that using accepted sampling procedures is less likely to result in biased samples but does not guarantee a representative sample (Leedy & Ormrod, 2013). To determine whether a correlation exists between cloud adoption cyber-risks and the organization leaders' *intent to adopt cloud-computing* in the financial services sector, I surveyed a sample set of leaders from the active FDIC insured institutions. Given the inherent cost and time implications associated with surveying all the financial institution leaders in the United States, the scope of this study was limited to a random sample of participants. The participants represented a sample of qualified financial services IT and business leaders from the four geographical zones of the United States: the West, Midwest, Northeast, and South. I collected the sample using a random systematic survey of participants from the SurveyMonkey Audience service pool. SurveyMonkey uses random sampling as a standard method of selecting participants from a pool of survey takers whose backgrounds have been compiled and run through their regular benchmarking process to ensure a representative sample of the U.S. population (Surveymonkey.com, n.d.).

Using the SurveyMonkey Audience service, I sampled 68 potential participants with strong backgrounds in the financial industry to participate in the study. This sample size was calculated using an a priori test, G*Power analysis 3.1.2 software program, as depicted in Figures 3 through 5. The G*Power analysis required that I select the type of test, the type of power analysis, the effect size, the alpha level (α), the power (1- β), and number of variables (Faul, Erdfelder, Buchner, & Lang, 2013). Using six independent variables (*relative advantage, complexity, compatibility*, *organization size* [*revenue*], *security*, and *compliance*), I set the significance level at $\alpha = 0.05$, indicating a 5% probability of Type I error; power at $1-\beta = 0.95$, where β represents probability of Type II error; and, an effect size of 0.3. These are generally accepted parameters based on previously published literature on multiple regression (Frankfort-Nachmias & Nachmias, 2008; Lee et al., 2013).

[1] -- -- Wednesday, January 06, 2016 -- 16:58:07
Exact - Multiple linear regression: Random model
Options: Exact distribution
Analysis: A priori: Compute required sample size
Input: Tail(s) = Two
H1 $\rho^2 = 0.3$
H0 $\rho^2 = 0$
α err prob = 0.05
Power (1-β err prob) = 0.95
Number of predictors = 6
Output: Lower critical $R^2 = 0.0194562$
Upper critical $R^2 = 0.2051260$
Total sample size = 68
Actual power = 0.9531301

Figure 3. Exact tests for multiple linear regression and random model, R^2 deviation from zero.

Note. The G*Power program is accessible online through the following site: http://www.psycho.uniduesseldorf.de/abteilungen/aap/gpower3/

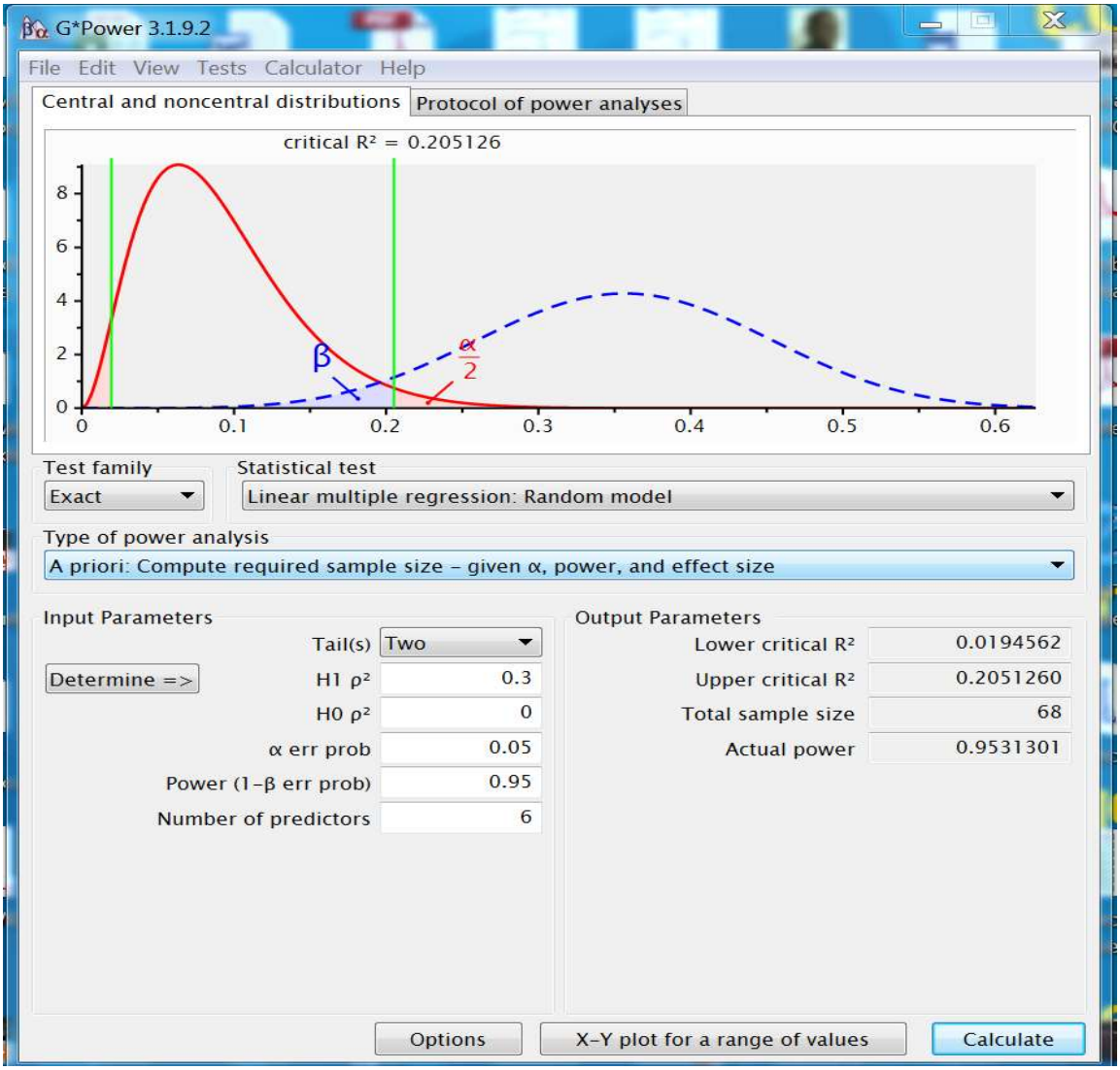

Figure 4. G*Power parameter screen indicating sample size calculation.

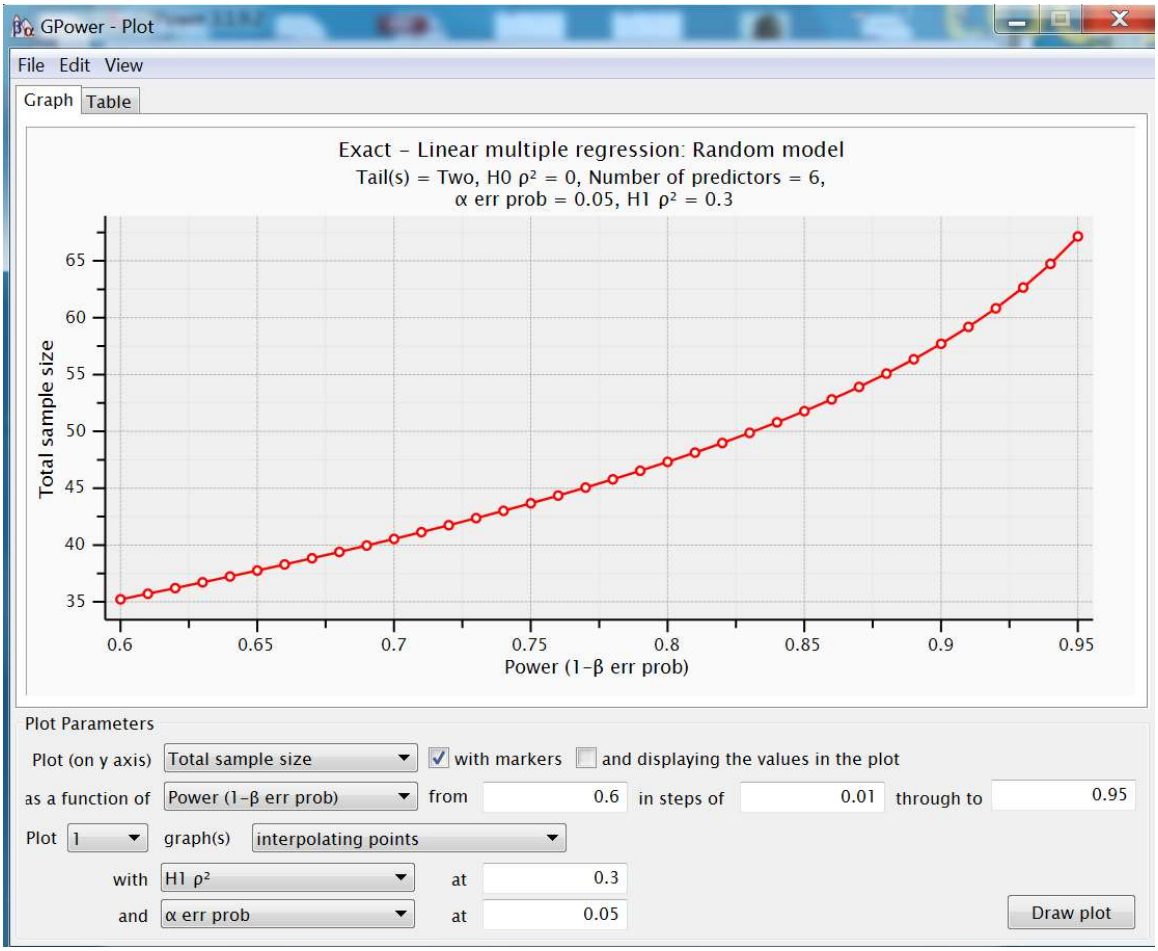

Figure 5. XY graphic representation of sample size and statistical power indicating the effect of sample size on statistical power.

Using these parameters, the result of the G*Power analysis indicated that I would need a minimum of 68 participants for this study. However, I pooled all the 450 participants available in the SurveyMonkey audience to ensure I maximized the survey participants and mitigated data quality risks that may have arisen from potentially low or incomplete response (Maronick, 2009; Powelson, 2012; Tweel, 2012). The survey attracted 118 valid responses. The use of the random sampling method to solicit participation in the online survey has several advantages over other methods. It ensures that every sampling unit of the population has an equal and known probability of being included in the sample (Lee et al., 2013). The fact that investigators can measure the errors of estimation or the significance of results from a random sample provides greater assurances of results obtained from the design (Kothari, 2005; Rea & Parker, 2014) and made it an attractive sampling method for this study.

While the random sampling method provides investigators the assurance of probability by treating the sample as a true depiction of the general research population, investigators may inadvertently introduce a bias by focusing only on the data collected and forego other important aspects of the study. For example, failing to calculate the most appropriate sample size needed for the study increases the risk of ineffective sampling, which consequently negates the validity of the findings. My use of random sampling along with proper sample size estimation using the G*Power version 3.1.2 software program helped avoid potential bias and maximized the probability that I have a representative sample.

To ensure individuals targeted for this study were key technology decision-makers, I surveyed only the participants from the pool of on-demand IT survey respondents from the SurveyMonkey audience who had been validated as having backgrounds specifically tailored to meet the sample characteristics required for this study. I requested that the participants be limited to people whose demographic information could be benchmarked with the FDIC list. By taking this approach, I hoped to control for errors from cluster elements, as well as mitigate risk from blank foreign elements or omission from either of the lists (Frankfort-Nachmias et al., 2014).

Procedures for Recruitment, Participation, and Data Collection

Quantitative research studies require the use of logical procedures to drive the data collection and to dictate the language for their findings. I used a cross-sectional survey to drive the data collection for this study. I administered the survey questions through SurveyMonkey to gather relevant research data needed to evaluate the strategic cyber-risk implications of cloud-computing adoption in the financial services sector. The nature of the research data and the level of precision required for the measuring instruments provided the rationale behind using surveys as the instrument of choice for this study. Online surveys provide a convenient means for research participants to provide their responses anonymously, and share their opinions and ideas at a convenient time (Hutchison, Fleischman, & Johnson, 2014). Recent studies have shown the viability of using e-mail as a convenient method for soliciting survey participation (Hanmer, Herrnson, & Smith, 2015; Schoenherr, Ellram, & Tate, 2015). To assess the dependent and independent variables for this study, the respondents were IT leaders from sample

FDIC-insured institutions. I used e-mail to solicit participation in the online survey for this research.

I apprised survey participants of the intent of the study and the measures I would take to ensure their privacy and ascertain the integrity of their data. I used the survey instrument to gather research data from 48 survey items (see Table 1) based on a 7-point Likert scale with scores ranging from 1 (*strongly disagree)* to 7 (*strongly agree*). I crafted each question to assess the participants' degree of disagreement or agreement with the cloud concepts under evaluation. The ability to capture ordinal data for the descriptions of mass populations made SurveyMonkey an excellent tool. Given that each variable represents a sum of ordinal variables, the resulting composite variable was an interval variable. Table 1 shows a summary of my independent variables, the corresponding survey items, how I calculated the composite variable, and their corresponding data type. I expected the measurements to show strong relationships between the research variables.

While I have praised SurveyMonkey as the research instrument to bring to bear the overarching research objectives guiding this study, it was not without some limitations. In particular, SurveyMonkey shares the issue of artificiality with other experimental instruments (Chytilova & Maialeh, 2015). Given that survey respondents can complete the surveys at a convenient time and place, it is easy for them to defer or neglect to complete them (Kasper, Hoffmann, Heesen, Köpke, & Geiger, 2012). It is also

Table 1

Summary of Research Variables and Corresponding Survey Items

#	Adoption Predictor Variables	Hypothesis	Corresponding Survey Item	Data Type of the composite variable
1-4			Q1 through Q4 are mainly to capture demographic information Q1- Industry affiliation Q2- Job role Q3- Organization primary category Q4- States	
5	Organization Size (Revenue)	$H1_0$: There is no significant relationship between organization size and the *intent to adopt cloud-computing* for core financial services operations. $H1_a$: There is a significant relationship between organization size and the *intent to adopt* cloud-computing technology for core financial services operations.	Use of descriptive statistics to capture annual revenue as a surrogate of organization size. Q5- What is your institution annual revenue? Revenue will be represented by a number of descriptive statistics	Interval

#	Adoption Predictor Variables	Hypothesis	Corresponding Survey Item	Data Type of the composite variable
6	Relative Advantage	$H2_0$**:** There is no significant relationship between *relative advantage* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations. $H2_a$**:** There is a significant relationship between *relative advantage* of cloud-computing technology and the *intent to adopt cloud-computing* for core financial services operations.	Use 7-point Likert scale to measure scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) for the following questions: Q6-Technology can be used for a number of objectives. To what extent is cloud-computing adoption important for the fulfillment of the following objectives in your organization: Use of cloud-computing allows us to: Q6.1- Optimize our branch network Q6.2- Gain deep understanding of customer needs Q6.3- Target customer with specific offerings Q6.4- Provide smart interactions with customer Q6.5- Empowers our frontline and mobile sales workforce Q6.6- Enhance our digital ecosystem Q6.7- Requires no upfront capital investment. Q6.8- Increases the profitability of our organization Q6.9- Reduces our operational cost savings from cloud-computing allows us to offer price-competitive products and services. Q6.1.0- Costs savings from cloud-computing allows us to offer price-competitive products and services. Composite variable calculation: Equally weighted average of Q6.1 through Q6.9 Composite variable calculation: Equally weighted average of questions Q6.1 through Q6.1.0	Interval

#	Adoption Predictor Variables	Hypothesis	Corresponding Survey Item	Data Type of the composite variable
7	Compliance	$H3_0$: There is no significant relationship between perceived *compliance risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations. $H3_a$: There is a significant relationship between perceived *compliance risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.	Use 7-point Likert scale to measure scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) for the following questions: Q7: Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from *strongly disagree* to *strongly agree* Q7.1- It is difficult to ensure compliance with industry /regulatory standards. Q7.2- It is difficult to ensure data privacy in the cloud. Q7.3- Government can gain access to business data in the cloud. Q7.4- It is difficult to meet data production and reporting requests by auditors/regulators. Q7.5- It is difficult to ensure clarity with responsibility and liability attribution in the cloud. Q7.6- Storing data in different geographical locations presents regulatory challenges (Safe harbor). Composite variable calculation: Equally weighted average of questions Q7.1 through Q7.6	Interval

#	Adoption Predictor Variables	Hypothesis	Corresponding Survey Item	Data Type of the composite variable
8	Security	$H4_0$: There is no significant relationship between perceived *security risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations. $H4_a$: There is a significant relationship between perceived *security risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.	Use 7-point Likert scale to measure scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) for the following questions: Q8: Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from *strongly disagree* to *strongly agree*. Q8.1- Malicious insiders may gain unauthorized access to business data in the cloud. Q8.2- Shared and multi-tenancy nature of cloud-computing creates a fertile ground for data loss or leakage. Q8.3- Business data in the cloud can be subject to abuse and nefarious use. Q8.4- Business data in the cloud can be subject to Man-in-the-middle attacks Q8.5- Business data or information stored in the cloud can be subject to message alteration. Q8.6- Business data in the cloud can be subject to message replay attacks. Q8.7- Confidential customer data or information stored in the cloud services can be subject to identity spoofing. Q8.8- Confidential customer information or business data in the cloud can be subject to denial of service attack. Composite variable calculation: Equally weighted average of questions Q8.1 through Q8.8.	Interval

#	Adoption Predictor Variables	Hypothesis	Corresponding Survey Item	Data Type of the composite variable
9	Compatibility	$H5_0$: There is no significant relationship between *compatibility* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations. $H5_a$: There is a significant relationship between *compatibility* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.	Use 7-point Likert scale to measure scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) or the following questions: Q9.1- Cloud adoption is not consistent with our organizational belief and value. Q9.2- Attitudes towards cloud adoption in our organization are unfavorable. Q9.3- Cloud adoption is not compatible with our organization's IT infrastructure. Q9.4- Use of cloud-computing is not consistent with our organization's business strategy. Q9.5- Cloud service is cumbersome to use. Q9.6- Using cloud services requires a lot of mental efforts. Q9.7- The user interface of cloud services is difficult and not user-friendly. Q9.8- Cloud services are difficult to purchase and set up. Composite variable calculation: Equally weighted average of questions Q9.1 through Q9.8.	Interval

#	Adoption Predictor Variables	Hypothesis	Corresponding Survey Item	Data Type of the composite variable
10	Complexity	$H6_0$: There is no significant relationship between *complexity* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations. $H6_a$: There is a significant relationship between *complexity* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.	Use 7-point Likert scale to measure scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) for the following questions: Q10.1- It is difficult to integrate legacy financial systems with the cloud. Q10.2- There is a potential vendor lock-in to a cloud service provider due to proprietary. Q10.3- It is difficult to audit technology services in the cloud environment. Q10.4- It is difficult to receive security logs in real time. Q10.5- It is difficult to conduct digital forensics and e-discovery in the cloud environment. Q10.6- Cloud solutions do not have good incident reporting mechanisms. Q10.7- There is a lack of control and accountability over business data in the cloud. Q10.8- It is difficult to classify data in the cloud. Composite variable calculation: Equally weighted average of questions Q10.1 through Q10.8.	Interval

#	Dependent Variable	Corresponding Survey Item	Data Type of the composite variable
11	Cloud-computing Adoption Intent	Use 7-point Likert scale to measure scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) for the following questions: Q11.1- Intends to adopt cloud-computing Q11.2- Likely to take steps to adopt cloud-computing in the future Q11.3- Likely to adopt cloud-computing for our core processes within the next 12+ months Composite variable calculation: Equally weighted average of questions Q11.1 through Q11.3.	Interval

difficult to predict whether respondents' answers reflect their true opinions about each survey question. There are other concerns, such as low response rates, questionable quality of expedited responses, and unsolicited e-mail filtering restricting access (Maronick, 2009). I attempted to mitigate these risks in my design strategy and sample size estimation, and during the pilot study, as discussed next.

Pilot Study

Pilot studies are an essential element of a good quantitative research design. They provide critical insights into where potential studies may fall short (van Teijlingen & Hundley, 2014). I used a group of personal contacts who are IT experts from my professional network with backgrounds in financial services to be the sample for my pilot study to answer the survey questions and offer feedback on the survey's flow as well as clarify practical implications in assessing the survey questions. I expected the pilot study to fulfill a range of important functions, including offering recommendations on ways to improve the questionnaire, evaluating the survey window's reasonableness, question sequence, and/or other feedback to improve the study's clarity and overall structure. My goal was to enhance the survey instrument and improve the study's quality by incorporating feedback from this group. I collaborated with each member of the pilot study sample to seek their feedback and/or recommendations on how to improve the survey, in general.

Instrumentation and Operationalization of Constructs

Use of validated instrument. The survey instrument used in this study was previously used by Tweel (2012) for a study which evaluated the correlation between IT

managers' adoption of cloud-computing using six independent variables from the TOE framework and DOI theory. Additionally, Lee (2015) used the same instrument (with a slight modification) in a study using regression analysis to study cloud-computing adoption for U.S. hospitals. Lee used a third-party vendor database to find appropriate participant hospitals. By taking this approach, the author's selected hospitals did not only represent a cross-section of U.S. hospitals, but obviated the need to develop an exclusionary generalization of the adoption principles in hospitals across the four geographical zones in the United States.

For this cross-sectional study, I modified Tweel's (2012) survey instrument to focus on cybersecurity risks as predictors of cloud adoption for the financial services sector. I mapped specific questions from the survey instrument with cloud-computing standards such as those from the Cloud Security Alliance (CSA) and the National Institute of Standardization of Technology (NIST). These security standards served as the channel for examining the security and privacy risks of financial institutions planning to operate in the cloud environment. The need to use a validated cross-sectional survey instrument similar to Lee's (2015) for this study was anchored by the fact that the survey instrument has a similar objective with this study. Theoretical constructs underlying Lee's study are also consistent with the theoretical framework of this study.

Given that I modified the survey questions slightly to focus on cybersecurity risks, I subjected the survey instrument to additional scrutiny. For example, the survey instrument underwent rigorous quality assurance tests to ensure the accuracy of test scores and ascertain the reliability of the study (Frankfort-Nachmias & Nachmias, 2008).

I benchmarked the results of this study with other studies in cloud adoption that used a similar measuring instrument (Lee, 2015; Tweel, 2012). Furthermore, I used the IBM SPSS statistical tools to re-affirm the internal reliability of the measuring instrument—factor analysis, the split-half estimates and Cronbach's coefficient alpha item analysis and validated scales for each of the tested variables (Green & Salkind, 2010).

Operationalization of research constructs. As I noted in the study variables section above, this research study included six independent variables from TOE dimensions (Rogers, 2003; Tornatzky & Fleischer, 1990), and a dependent variable: the *intent to adopt cloud-computing* in the U.S. financial services sector.

Data Analysis Plan

Evaluating whether a significant relationship exists between cyber-risks and the *intent to adopt cloud-computing* in the U.S. financial sector was of primary interest in this study. To establish the relationship between the independent variables and dependent variable for this study, I used the SPSS Windows-based program IBM© SPSS Statistics version 24 to analyze the sample datasets captured in the cross-sectional survey. As a basis for using multiple regression for hypothesis testing, I performed tests (detailed in Chapter 4) to ensure the data met the following statistical assumptions (Cohen, Cohen, West, & Aiken, 2013; Field, 2013):

- The dependent variable was measured as an interval variable (*intent to adopt cloud-computing* in financial services sector).
- My study included two or more independent variables.
- The variables were independent.

- There existed a linear relationship between the dependent variable and each of the independent variables.
- The error terms from the regression model (residuals) were distributed normally.
- The variance of error terms (residuals) was constant across all levels of the independent variables (that is, there is an assumption of homoscedasticity).
- The data showed no multicollinearity, which often occurs when two or more of the independent variables are significantly correlated with each other.

With these assumptions made, I carried out the multiple regression analysis using the SPSS program. The multiple linear regression model included each of the six predictors (relative advantage, complexity, compatibility, organization [revenue], security, and compliance) and the criterion to test their relationship to the dependent variable. I then used the SPSS program to determine the residual plots, collinearity, and variance inflation factors (VIFs) to verify appropriateness of the model.

Specifically, I used the SPSS multiple linear regression program to test the statistical significance (F-ratio) and an adjusted squared correlation (R^2). *Adjusted* R^2 measured the proportion of variance in the dependent variable that can be accounted for by the independent variables, taking into account the number of independent variables. The F-ratio helped me determine if the overall regression model was a good fit for the empirical data. I used *t* tests to evaluate the relationship between each of my study's predictors and the dependent variable. I also summarized information from the datasets by constructing frequency distributions, and converted the frequency to percentage measures to ensure a meaningful interpretation of the data (Leon-Guerrero & Frankfort-

Nachmias, 2014). Finally, I used graphs to create visual impressions of the data and to pictorially communicate the respondents' perceptions more effectively (Armstrong, 2012).

Threats to Validity

At every step, investigators using quantitative methods have the potential to fall short of the ideal measurement. Given that the quantitative strategy of inquiry involves a number of decisions that may affect the research estimates (Fowler, as cited in Babbie, 2013; Punch, 2013), it is important for investigators to depend on research validity to ensure that reliable conclusions are drawn from the research problem(s) under study. For example, scholars have cautioned against the use of random sampling because of internal validity concerns (Clark & Linzer, 2015). The lack of random assignment to treatment, intentionally or inadvertently, selection of extreme scores for study, participants' predisposition to certain outcomes, and selection bias all have the potential to affect a study's outcomes (Frankfort-Nachmias et al., 2014).

I subjected the survey instrument to visual inspections, and performed rigorous quality assurance tests to ensure the accuracy of the test scores and ascertain the reliability of my study (Frankfort-Nachmias et al., 2014). Additional controls included benchmarking the results of the study with scholarly publications that used the popular theoretical constructs of Rogers's DOI theory (2003) and the TOE framework (Tornatzky & Fleischer, 1990). I also used statistical tools such as IBM SPSS to re-affirm the internal reliability of the measuring instrument, using factor analysis, the split-half estimates, and

Cronbach's coefficient alpha item analysis to validate scales for each of the test variables (Green & Salkind, 2010).

Reliability and validity are other key measures of a good cross-sectional survey instrument in the social sciences (Lameck, 2013). Reliability measures the degree to which a research instrument can provide stable and consistent results (Frankfort-Nachmias et al., 2014). Validity refers to the "extent to which a test measures what the researcher intended to measure" (Cooper & Schindler, 2014, p. 231). To maximize the accuracy means that the investigator must minimize threats to validity while ensuring the reliability of the instrument. I carefully considered and controlled for different threats to validity, as discussed below.

External Validity

External validity is best established when a researcher focuses on the selection of research participants with the aim of selecting the largest sample possible from the research population (Frankfort-Nachmias & Nachmias, 2008). The implication of this concern for this study is that I drew most of the participants from the SurveyMonkey database. Given that the study subjects included a list of survey participants whose backgrounds and demography had been validated by SurveyMonkey, the data was not biased, and researchers will be able to generalize the results to financial institutions across the four geographic regions of the United States. The use of power analysis for determining the effect size that results in a larger effect size for the independent variables makes this study more generalizable to financial institutions in the United States (Leon-Guerrero & Frankfort-Nachmias, 2014). Additionally, I took proper precautions when

generalizing the results because there may be certain state or local laws that pose specific regulatory characteristics outside of the *compliance risk* predictors used in this study.

Internal Validity

Internal validity consists of the degree of independence of the research variables and its influence in demonstrating causality between dependent and independent variables (Schenker & Rumrill, 2004). Frankfort-Nachmias and Nachmias (2008) identify the following facets of validity:

- Content validity
- Empirical validity
- Construct validity

The descriptions for each of these are shown below.

Content validity. Content validity refers to the extent to which the measuring instrument covers all the attributes of the phenomenon the researcher is trying to measure. It focuses on ascertaining that an instrument comprehensively measures relevant attributes of a study (Frankfort-Nachmias et al., 2014). The issue of content validity is maximized by using research instruments that have been widely scrutinized and their content validity established by scholars in peer-reviewed journal articles (Streiner, 2016). Content validity can be further expanded into face validity and sampling validity. Face validity refers to the extent to which the researchers measured the phenomenon they claimed to have measured (Frankfort-Nachmias et al., 2014). It rests on the investigators' subjective judgment about the adequacy of the instrument instead of demonstrating whether the instrument measures the phenomenon under investigation.

Sampling validity, on the other hand, is a measure of adequacy of a sampled population (Frankfort-Nachmias et al., 2014). In other words, sampling validity refers to the extent to which the measuring instrument adequately sampled the target population. In practice, sampling validity is important when a researcher is constructing the research instrument and using it for the first time.

Empirical validity. Empirical validity refers to the extent to which the measuring instrument measured the outcomes of the experiment. Predictive validity refers to the extent to which the measuring instrument predicted the expected outcome of the experiment. It is a measure of both the predictive ability of the instrument and its potential to adequately predict future behavior.

Construct validity. Construct validity refers to the extent to which the measurement instrument logically and empirically adhered to the concepts, assumptions, and theoretical framework of the study (Frankfort-Nachmias & Nachmias, 2008). Given the challenges of measuring internal validity, it has become a good practice to establish the external validity of a cross-sectional research study. For this study, I addressed threats to internal validity through statistical regression analysis. During the pilot, I used a panel of experts from Walden University's School of Management to establish content validity of this survey questionnaire. This ensured that the survey instrument measured the key variables of this study and thus assured its reliability.

Ethical Procedures

Adhering to proper ethical standards is another important consideration for a cross-sectional study. Given that human subjects are involved in cross-sectional studies,

there is a potential for ethical issues to occur when one conducts this type of quantitative study. Such issues consist of the respondents' rights to privacy, or issues related to anonymity of the people who are involved in the study. It is therefore imperative for investigators to minimize risks to the respondents while ensuring that they maximize the quality of information obtained from their studies (Gillespie, as cited by Lameck, 2013). In this study, I managed the data acquisition, handling, and analysis in accordance with Walden University's Institutional Review Board (IRB) guidelines (IRB approval number 02-06-17-0087674).

As an investigator conducting research on social issues involving individuals, I am obligated to protect the participants in order to induce positive social change. In this quantitative study, I undertook proper ethical controls and procedures to ensure the integrity and confidentiality of the survey responders. Such procedures included ensuring that proper disclosure existed for the consent and withdrawal process, disclosure of incentives, and security safeguards to protect the participants' data during and after this study. I used the following safeguards to protect the participants:

- I was open with the participants about the purpose and scope of the research, while ensuring that they understood the interview questions;
- Participants were provided adequate time to answer the survey questions, and I coded the information obtained to ensure confidentiality;
- I made efforts to ensure that my prior experience working in the financial sector did not create any bias against the research participants or distort the results of the study. I followed the proper code of ethics throughout the research lifecycle;

- If I suspected an issue might be unethical, I was prepared to promptly file a research exemption form with Walden's IRB;
- The participants' privacy, rights, and interests were of the highest priority when I was confronted with making choices about reporting; and
- I protected the participants' anonymity, as promised in the disclosure form.

The results of this study are presented in a format that provides a clear picture of the data collection, analysis, and generalizations made during this study. This study also went through scholarly scrutiny by my dissertation committee and finally by the Walden University Research Reviewer (URR) to ensure the research questions were answered properly and the results provide the lens to address the problem concerning the slow adoption of cloud-computing in the U.S. financial services sector.

The methodology described in this chapter provides a structured approach to examining the practical cybersecurity risks posed by cloud-computing. In Chapters 4 and 5, I will discuss the results of this study and benchmark the findings with the current cloud adoption literature to corroborate or refute the results of my study. Specifically, Chapter 4 will include a discussion about the processes I used for the actual data collection, information about the participants' demographics, and finally the results of the data analysis.

Summary

This study fosters a quantitative cross-section plan for the exploration of the cyber-risk factors impeding the adoption of cloud-computing in the U.S. financial services sector. With the guidance of general technology diffusion concepts and the

application of quantitative techniques, this chapter has provided details on the scholarly approach to exploring the unique implications of security and privacy concerns of cloud-computing adoption in the U.S. financial services sector. Although scholars have suggested a correlation between innovation adoptions and risk (Jacobs, Weiner, Reeve, Hofmann, & Christian, 2015; Rogers, 2003), those risks cut across all technologies to different degrees. This study contributes to an understanding of the security and privacy risks of cloud-computing, and will offer a reasonable approach to ensuring sustainable cloud-computing adoption (Jacobs et al., 2015) in the U.S. financial services sector.

Although scholars have identified security and privacy risks as the key indicators for the slow rate of cloud adoption, this study will provide more insights into the specific security and privacy risks affecting the adoption of this technology. In this study, I will evaluate the cyber-risk implications of cloud-computing on the intent to adopt cloud-computing in the U.S. financial services setting. This study will help identify the inseparable bond that makes it difficult to prescribe cloud solutions in the financial services sector. Chapter 4 presents a detailed discussion of the results of the study.

Chapter 4: Results

The purpose of this quantitative cross-sectional study was to evaluate the cyber-risk implications of cloud-computing adoption and increase understanding of the key cyber-risk management strategies to facilitate the adoption of cloud services in the U.S. financial services sector. The research question examined the practical cyber-risks of six technological and organizational factors, which comprised the independent variables—*organization size, relative advantage, compliance, security, compatibility*, and *complexity*. The study's purpose was to measure the degree of perceived innovation risks influencing the dependent variable: the *intent to adopt cloud-computing* in the U.S. financial services sector. Based on the post-positivist, deterministic research approach (Pierce & Sawyer, 2013), I developed several hypotheses to address the research problem.

In this chapter, I cover the following topics: the pilot study, the results of this study, the participants' demographic information, and the statistical analysis of the research data.

Pilot Study

For the pilot phase of my study, I used six personal contacts who are IT experts with unique experience in financial services. They agreed to review my survey questions and offer feedback on both the clarity and the structural flow of the survey items. They determined that the questions were well structured and had no reservations about the clarity of the questions. No changes were recommended. Given the few number of users who were contacted for this pilot study, and the limited acquired data points, the results

of the pilot study were not sufficient to meaningfully impact this study. Thus, I decided not to analyze or incorporate the results of the pilot in this study.

A key recommendation from some of the pilot study's participants, however, was to ensure that no personal information was requested of the participants in order to minimize risks associated with privacy and anonymity. This recommendation was in line with Walden University's IRB guidelines. Thus, I ensured that no personally identifiable information was requested in the survey. I also advised the survey participants of their rights and obligations, and the protocols I had taken to ensure the security and privacy of their information. This disclaimer was included in the informed consent form provided to the participants on the landing page of the survey.

Data Collection

The survey questions for this cross-sectional study were administered through the SurveyMonkey audience tool to gather relevant research data needed to evaluate the strategic risk implications of cloud-computing adoption in the financial services sector. The targeting criteria for the survey participants were based on specific attributes including industry, work status, geographic zones, job function, employment status, and minimum age, to name a few. The participants' target criteria stipulated that they were IT and business leaders from U.S. financial services firms from the four geographical regions (West, Midwest, Northeast, and South). Four other criteria were mandated for the survey respondents. She or he

1. was at least 18 years of age,
2. was a technology leader from one of the FDIC list of U.S. financial institutions,

3. had IT knowledge, was familiar with cloud-computing concepts, and
4. played a critical role in influencing technology decisions.

The participants had to choose a yes or no response; choosing no automatically ended the survey.

In compliance with Walden's IRB requirement, the survey participants were informed of the reason why they were selected. Using a carefully crafted SurveyMonkey audience service, invitation was sent by SurveyMonkey to a number of its selected volunteers to participate in the survey. The participants were apprised via an informed consent form of the risks and benefits of the study, including the protection protocols I put in place to prevent them from loss of privacy, psychological distress, and physical harm. For example, the research participants were allowed to provide their responses anonymously, and share their opinions and ideas at times convenient for them. The survey was deliberately designed to include anonymous consent and data collection procedures so that survey participants' identities were completely protected from the researcher. Additionally, to ensure the privacy, integrity, and confidentiality of this survey's participants, no personally identifying information such names, address, social security number was asked in the survey.

The researcher's personal contact information, the IRB, and the supervising committee contacts were provided so that any issues or concerns could be directed to them for prompt resolution. The survey participants were informed of their right to withdraw from the study at any time. Additionally, participants were provided a sample of items on the survey so they could see the type of information they would be asked to

provide should they agree to complete the survey. Although no incentive was offered for completing the survey, participants were informed of their ability to access the results of this study in future by visiting the following link: https://www.researchgate.net/project/Strategic-Cyber-Risk-Implications-of-Cloud-Technology-for-Financial-Services-Sector. Participants were also advised to print a copy of the consent form and retain this link for future reference. At the end of the survey, participants were given the opportunity to review their responses before final submission.

The SurveyMonkey Audience data collection process was made available for an 18-day period, from February 6, 2017 through February 24, 2017. Throughout this period, I was able to view responses to the survey in real time, and monitored the status of the project as the responses came in. At the conclusion of the survey window, I had received a total of 125 responses, out of which only 7 responses were found not to be useful due to a relatively large number of incomplete responses. Thus, the 7 responses were rejected. The remaining 118 responses that were found to be useful amounted to about a 94.4% completion rate, and exceeded the minimum sample of 68 required to have a representative sample for this study (see the G*Power calculation in Chapter 3). I later downloaded the survey dataset from the SurveyMonkey.com audience tool into a Windows-based SPSS program for analysis. As described in Chapter 3, the final survey dataset was encrypted and securely stored both in the researcher's encrypted online vault and a filing cabinet encrypted format locked in the researcher's home office for safekeeping.

Research Questions and Hypotheses

Inferential statistics were used to draw conclusions from the sample collected. The Statistical Package for the Social Sciences (SPSS) was used to code and tabulate scores collected from the survey and provide summarized values where applicable including the mean, standard deviation, and central tendencies. Multiple regression analysis was used to evaluate the research question and hypotheses. The research question and hypotheses were:

Research Question 1 (RQ1): What are the practical cyber-risks of technological and organizational factors that strongly influence the *intent to adopt cloud-computing* in the U.S. financial services sector?

$H1_0$: There is no significant relationship between financial institution *size* and the *intent to adopt cloud-computing* for core financial services operations.

$H1_a$: There is a significant relationship between financial institution *size* and the *intent to adopt cloud-computing* for core financial services operations.

$H2_0$: There is no significant relationship between the *relative advantage* of cloud-computing technology and the *intent to adopt cloud-computing* for core financial services operations.

$H2_a$: There is a significant relationship between the *relative advantage* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H3_0$: There is no significant relationship between perceived *compliance risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H3_a$: There is a significant relationship between perceived *compliance risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H4_0$: There is no significant relationship between perceived *security risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H4_a$: There is a significant relationship between perceived *security risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H5_0$: There is no significant relationship between *compatibility risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H5_a$: There is a significant relationship between the *compatibility risk* of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H6_0$: There is no significant relationship between *complexity* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

$H6_a$: There is a significant relationship between *complexity* belief of cloud-computing and the *intent to adopt cloud-computing* for core financial services operations.

As a prerequisite to analyzing the research question, I evaluated the variables for missing data, univariate outliers, normality, linearity, homoscedasticity, and multicollinearity. Subsequently, I conducted multiple regression analysis to determine if there were any significant relationships between the variables of interest. The results of my data analysis are reported below.

Participant Demographics

Data were collected from a sample of 118 financial services IT and business leaders ($N = 118$). Displayed in Table 2 are frequency and percent statistics of participants' gender and age.

Table 2

Frequency and Percent Statistics of Participants' Gender and Age

Demographic	Frequency (*n*)	%
Gender		
Female	48	40.7
Male	70	59.3
Total	118	100.0
Age		
18 - 29	17	14.4
30 - 44	58	49.2
45 - 59	26	22.0
60+	17	14.4
Total	118	100.0

Note. Total $N = 118$.

Table 3 shows the frequency of distribution of demographics job role. There were 118 accepted participants' responses with roles ranging from an IT analyst to the executive level. The analysis of the descriptive statistics conducted on the job roles revealed that most of the highest percentage of the participants worked as either an IT engineer/analyst (28.8%) or an executive-level officer: that is, a vice president, information security officer, director, or higher (28.8%).

Table 3

Frequency and Percent Statistics of Participants' Job Role

Job role	Frequency (*n*)	%
IT Engineer/Analyst	34	28.8
IT/System Administrator/ Architect	15	12.7
IT/IS Management/Supervisor	28	23.7
VP/ISO/Director/C-level Executive	34	28.8
Other (please specify)	7	5.9
IT Auditor	1	0.8
IT Business Application Coordinator	1	0.8
IT Compliance Coordinator	1	0.8
IT Risk Assessor	1	0.8
IT Risk Specialist	1	0.8
IT Third Party Vendor Administrator	1	0.8
IT Vendor Management Coordinator	1	0.8
Total	118	100.0

Note. Total $N = 118$.

For participants' organizations' primary services, one third (a plurality) of the collected sample (33.9%) fell under the category of retail banking, credit unions, and savings and loans. Table 4 provides demographical statistics showing the comparison of the participants' organizations' primary financial services. For participants' annual income, 26.3% of the participants made between $150,000 and $174, 000. Additionally, frequency and percent statistics for the organizations' U.S. region and state locations are displayed in Table 5.

Testing of Hypotheses 1-6

Hypotheses 1-6 were tested using multiple regression analysis to determine if there were any significant relationships between practical cyber-risks of technological and organizational factors that strongly influence the *intent to adopt cloud-computing* in

Table 4

Frequency and Percent Statistics of Participants' Organizations' Primary Financial Services

Primary Financial Services	Frequency (*n*)	%
Commercial Bank	7	5.9
Investment Bank	8	6.8
Insurance Company	26	22.0
Stock Brokerage	11	9.3
Retail/Credit Unions/Savings/Loans	40	33.9
Mortgage services	10	8.5
All of the Above	12	10.2
Other (please specify)	4	3.4
Auto Loan	2	1.7
Community Bank	2	1.7
Total	118	100.0

Note. Total *N* = 118.

Table 5

Frequency and Percent Statistics of Participants Annual Income and Device Type

Demographic	Frequency (*n*)	%
Annual Income		
$0 to $9,999	6	5.1
$10,000 to $24,999	4	3.4
$25,000 to $49,999	5	4.2
$50,000 to $74,999	9	7.6
$75,000 to $99,999	9	7.6
$100,000 to $124,999	5	4.2
$125,000 to $149,999	16	13.6
$150,000 to $174,999	31	26.3
$175,000 to $199,999	17	14.4
$200,000 and up	7	5.9
Prefer not to answer	9	7.6
Total	118	100.0
Device Types		
iOS Phone / Tablet	15	12.7
Android Phone / Tablet	30	25.4
Windows Desktop / Laptop	65	55.1
MacOS Desktop / Laptop	6	5.1
Other	2	1.7
Total	118	100.0

Note. Total *N* = 118.

the U.S. financial services sector. The dependent variable for research question 1 was participants' *intent to adopt cloud-computing* in the U.S. financial services sector as measured by three items on the Cloud Security Survey (CSS). A 7-point Likert scale was used, with scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree)*. Composite scores were calculated by averaging case scores across the three items and were used as the dependent variable for the research question.

The six independent variables were financial organizations' *annual revenue(size)*, *relative advantage* (18 items), *compliance risk* (6 items), *security risk* (8 items), *compatibility risk* (8 items), and *complexity* belief (9 items) as measured by the CSS. A 7-point Likert scale was used, with scores ranging from 1 (*strongly disagree*) to 7 (*strongly agree)*. Composite scores were calculated for each variable by averaging case scores across the constructs' items and the composite scores were used as the independent variables in the multiple regression analysis of Hypotheses 1-6.

Data Cleaning

Before the research questions were evaluated, data were screened for missing values and univariate outliers. Missing data were evaluated using frequency counts and three cases missed/skipped one survey item. As Tabachnick and Fidell (2013) recommended, retaining as many participants as possible, the missing scores were replaced with survey items' series mean. The data were screened for univariate outliers by transforming raw scores to z-scores and comparing z-scores to a critical value of +/- 3.29, $p < .001$ (Tabachnick & Fidell, 2013). Z-scores that exceed this critical value are more than three standard deviations away from the mean and thus represent outliers.

When the distributions were evaluated, six cases with univariate outliers were found and these were removed from all further analyses. Thus, data were collected from a sample of 118 participants and 112 were evaluated by the multiple regression model ($N = 112$). Displayed in Table 6 are descriptive statistics of covariates used to evaluate the research question.

Survey Instrument Reliability Analysis

As discussed in Chapter 3, I adapted Tweel's instrument to focus my study on examining the cyber-risk implications of cloud-computing adoption for the U.S. financial services sector. Because I changed the survey items, it was important for me to check for the reliability and validity of the adapted survey instrument. I thus ran reliability analyses to determine if the dependent (*intent to adopt*) and independent variables (*relative advantage, compliance risk, security risk, compatibility risk,* and *complexity risk*) were sufficiently reliable. Reliability analysis allows one to study the properties of measurement scales and the items that compose the scales (Tabachnick & Fidell, 2013). Cronbach's alpha reliability analysis procedure calculates a reliability coefficient that ranges between 0 and 1. The reliability coefficient is based on the average inter-item correlation. Scale reliability is assumed if the coefficient is ≥ .70. Results from the tests found that no variables violated the assumption ($p > .80$). Thus, the dependent and independent variables were found to be sufficiently reliable as displayed in Table 7.

Test of Normality

Before the research questions were analyzed, I assessed basic parametric assumptions for the dependent (*intent to adopt*) and independent variables (*annual*

Table 6

Descriptive Statistics of the Dependent and Independent Variables

Variable	Min	Max	Mean	Std. Deviation	Skew	Kurtosis
Annual Revenue	$1,200,000	$35,000,000,000	$1,216,064,678	$4,317,694,246	6.010	40.158
Relative Advantage	3.500	6.556	5.412	0.684	-0.361	-0.612
Compliance Risk	1.333	7.000	5.186	1.198	-0.633	-0.321
Security Risk	2.125	7.000	5.425	1.135	-0.620	-0.451
Compatibility Risk	1.000	5.750	2.738	1.162	0.471	-0.744
Complexity Belief	2.222	7.000	5.204	1.114	-0.356	-0.937
Intent to Adopt	1.000	7.000	5.354	1.282	-0.913	0.719

Note. Total $N = 112$.

Table 7

Cronbach's Alpha Summary of Reliability Analyses for the Dependent and Independent Variables

Variable	No. of Items	Sig. (p)
Relative Advantage	18	0.837
Compliance Risk	6	0.927
Security Risk	8	0.946
Compatibility Risk	8	0.943
Complexity Belief	9	0.943
Intent to Adopt	3	0.883

Note. $N = 112$.

revenue, relative advantage, compliance risk, security risk, compatibility risk, and complexity belief): normally distributed residuals, independence, linearity, and homoscedasticity. I evaluated independence, linearity, and homoscedasticity using scatterplots and no violations were observed. Additionally, I produced a normal probability plot of residuals to evaluate the assumption of normality and no major deviations from normality were observed (see Figure 6). The remaining distributions did not violate the assumption of normality. Displayed in Table 8 are skewness and kurtosis statistics of the dependent and independent variables.

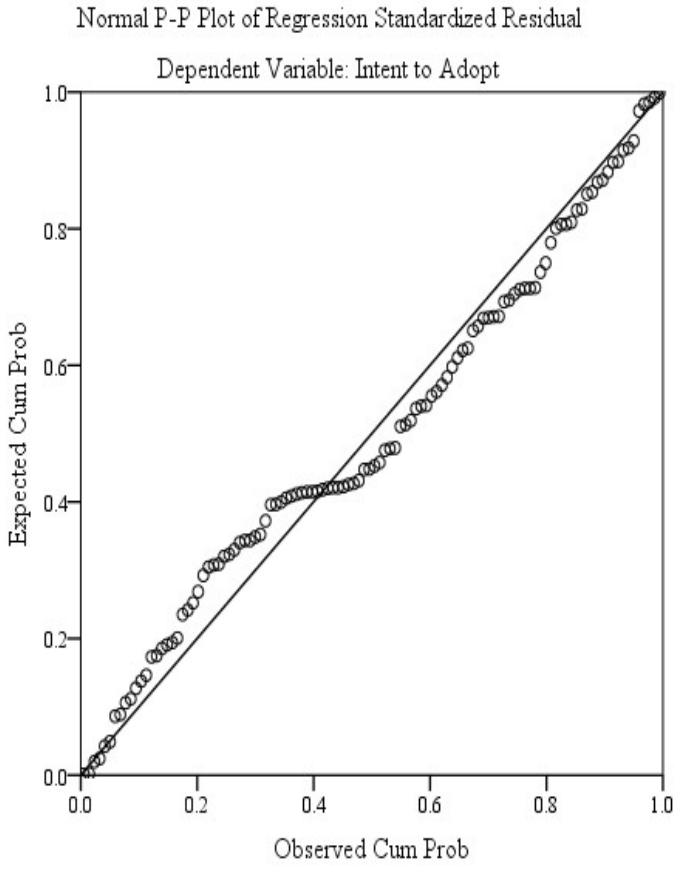

Figure 6. Normal probability plot of residuals.

Table 8

Skewness and Kurtosis Statistics of the Dependent and Independent Variables

Variable	Skewness	Skew Std. Error	*z*-skew	Kurtosis	Kurtosis Std. Error	*z*-kurtosis
Annual Revenue	6.010	0.228	26.360	40.158	0.453	88.649
Relative Advantage	-0.361	0.228	-1.583	-0.612	0.453	-1.351
Compliance Risk	-0.633	0.228	-2.776	-0.321	0.453	-0.709
Security Risk	-0.620	0.228	-2.719	-0.451	0.453	-0.996
Compatibility Risk	0.471	0.228	2.066	-0.744	0.453	-1.642
Complexity Belief	-0.356	0.228	-1.561	-0.937	0.453	-2.068
Intent to Adopt	-0.913	0.228	-4.004	0.719	0.453	1.587

Note. N = 112.

Multicollinearity

The assumption of multicollinearity was tested by calculating correlations among independent variables (*annual revenue, relative advantage, compliance risk, security risk, compatibility risk, and complexity belief*) and collinearity statistics (tolerance and variance inflation factor). Results indicated that correlations between independent variables did not exceed the critical value of .80. Tolerance was calculated using the formula $T = 1 - R^2$ and variance inflation factor (VIF) is the inverse of Tolerance (1 divided by T). Commonly used cut-off points for determining the presence of multicollinearity are $T < .10$ and $VIF > 10$. Results indicated that the independent variables did not exceed the critical values. Thus, since the correlation, tolerance, and VIF coefficients did not exceed their critical values, multicollinearity was not found. Table 9 shows a summary of correlation coefficients among the independent variables.

Table 9

Summary of Pearson's Correlations between the Independent Variables

	Independent Variable					
Independent Variable	1	2	3	4	5	6
Annual Revenue (1)	1.000	0.079	-0.010	-0.001	-0.096	-0.084
Relative Advantage (2)		1.000	0.379	0.410	-0.526	0.392
Compliance Risk (3)			1.000	0.677	-0.265	0.582
Security Risk (4)				1.000	-0.295	0.420
Compatibility Risk (5)					1.000	-0.279
Complexity Belief (6)						1.000

Note. $N = 112$.

Results of Hypotheses 1-6

Using SPSS 24.0, I evaluated Hypotheses 1-6 using multiple regression analysis to determine if there was a significant relationship between financial organizations' *intent to adopt cloud-computing* and six practical cyber-risks of technology (*annual revenue, relative advantage, compliance risk, security risk, compatibility risk, and complexity risk*). Results indicated that a significant relationship did exist between financial organizations' *intent to adopt cloud-computing* and a model containing six independent variables, $R = .679$, $R^2 = .461$, $F\ (6, 105) = 14.975$, $p < .001$. That is, 46.1% ($R^2 = .461$) of the variance observed in financial organizations' *intent to adopt* scores was attributed to a model containing six practical cyber-risks. Table 10 displays a summary of the multiple regression analysis conducted for Hypotheses 1-6.

Table 10

Model Summary of Multiple Regression Analysis for Hypotheses 1-6

Source	*R*	R^2	Standard Error	*F*	*df1*	*df2*	Sig. (*p*)
Omnibus	0.679	0.461	0.968	14.975	6	105	< .001

Source	Unstandardized Coefficients		Standardized Coefficients			
	B	Std. Error	Beta	*t*	Sig. (*p*)	Part Correlation
(Constant)	4.607	1.055		4.365	< .001	
Annual Revenue	0.000	0.000	-0.072	-0.991	0.324	-0.071
Relative Advantage	0.070	0.171	0.037	0.409	0.683	0.029
Compliance Risk	0.304	0.117	0.284	2.609	0.010	0.187
Security Risk	0.061	0.113	0.054	0.536	0.593	0.038
Compatibility Risk	-0.542	0.094	-0.492	-5.774	< .001	-0.414
Complexity Belief	-0.005	0.105	-0.004	-0.048	0.962	-0.003

Note. Dependent variable = *intent to adopt*, $N = 112$

The influence of each independent variable was evaluated using the *t* statistic and *p* value for each. Results of the multiple regression shown in Table 10 indicated that Hypotheses 3 and 5 were rejected. Null Hypotheses 1, 2, 4, and 6 were not rejected. The conclusion was there was sufficient evidence supporting the alternate hypotheses, that two independent variables (*compliance risk* and *compatibility risk*) made significant contributions in explaining financial organizations' *intent to adopt* scores. Specifically, there was a significant positive relationship between *intent to adopt* and *compliance risk* ($B = 0.304$, $p = .01$). Additionally, there was a significant negative relationship between *intent to adopt* and *compatibility risk* ($B = -0.542$, $p < .001$). No other independent variables made a significant contribution in explaining the dependent variable (annual revenue $p = .324$, relative advantage $p = .683$, security risk $p = .593$, and complexity belief $p = .962$).

Exploratory Analysis

Based on findings from the previous analysis, I conducted another multiple linear regression analysis to test the null hypothesis that a model with *compliance* and *compatibility risk* does not predict *intent to adopt cloud-computing*. I included a two-factor interaction variable and I calculated by multiplying the two independent variable scores together (*compliance risk*compatibility risk*). I used the interaction variable to determine whether the shared variance between independent variables had a significant impact on the dependent variable (*intent to adopt*). Furthermore, I used SPSS 24.0, sequential multiple regression analysis to determine if there was a significant relationship between financial organizations' *intent to adopt cloud-computing* and two identified practical cyber-risks of technology (*compliance risk, compatibility risk*) and an interaction term (*compliance risk*compatibility risk*). Sequential multiple regression analysis summary statistics are presented in Table 11.

Table 11

Sequential Multiple Regression Analysis Summary Statistics

Omnibus	*R*	R^2	Standard Error	*F*	*df1*	*df2*	Sig. (*p*)
Model 2	0.719	0.518	0.903	14.376	1	108	< .001

	Unstandardized Coefficients		Standardized Coefficients			
Model 2 Source	*B*	Std. Error	Beta	*t*	Sig. (*p*)	Part Correlation
(Constant)	8.856	1.115		7.944	< .001	
Compatibility Risk	-1.960	0.377	-1.776	-5.196	< .001	-0.347
Compliance Risk	-0.353	0.200	-0.330	-1.764	0.081	-0.118
Interaction	0.267	0.070	1.291	3.792	< .001	0.253

Note. Dependent variable = *intent to adopt*. Interaction = compatibility risk * compliance risk. $N = 112$.

In Model 2, results indicated that a significant relationship did exist between financial organizations' *intent to adopt cloud-computing* and a model containing the two

independent variables and interaction term: $R = .719$, $R^2 = .518$, $F\ (1, 108) = 14.376$, $p < .001$. That is, 51.8% of the variance observed in financial organizations' *intent to adopt* scores was attributed to a model containing the final two practical cyber-risks and the interaction term. Based on the R^2, this model is a better predictor than Model 1.

As found by the sequential multiple regression analysis, the contribution of each independent variable, when the variance explained by all others was controlled, indicated that only one independent variable (*compatibility risk*) made a significantly unique contribution in explaining financial organizations' *intent to adopt* scores ($B = -1.776$, $p < .001$). That is, there was a significant negative relationship between *intent to adopt* and *compatibility risk*. *Compliance risk* did not have a significantly unique contribution in explaining the dependent variable ($B = -0.330$, $p = .081$) in the model containing the interaction term. However, since the p value was not substantially greater than .05, and since there was a significant interaction term, *compliance risk* is retained in the final predictive model.

In Model 2, the interaction between *compatibility risk* and *compliance risk* was significant. This means that the relationship of the dependent variable and each independent variable is dependent on the value of the other independent variable. That is, the individual relationships are conditional on the value of the other independent variable. Because the two independent variables were significant in Model 1; because the interaction term was significant in Model 2; and because Model 2 had a higher R^2 than Model 1; Model 2 is a superior predictive model of the dependent variable, even though the p value for *compliance risk* was greater than .05. Model 2, therefore, is the final

predictive model, and it is comprised of two independent variables and an interaction term as depicted in Table 11, Figure 7, and Figure 8. In Figure 7, the dotted lines display the interaction between *compliance risk* and *intent to adopt* when *compatibility risk* is set at low and high values (i.e., 1, 7). Conversely, Figure 8 displays the interaction between *compatibility risk* and *intent to adopt when compliance risk* is set at low and high values.

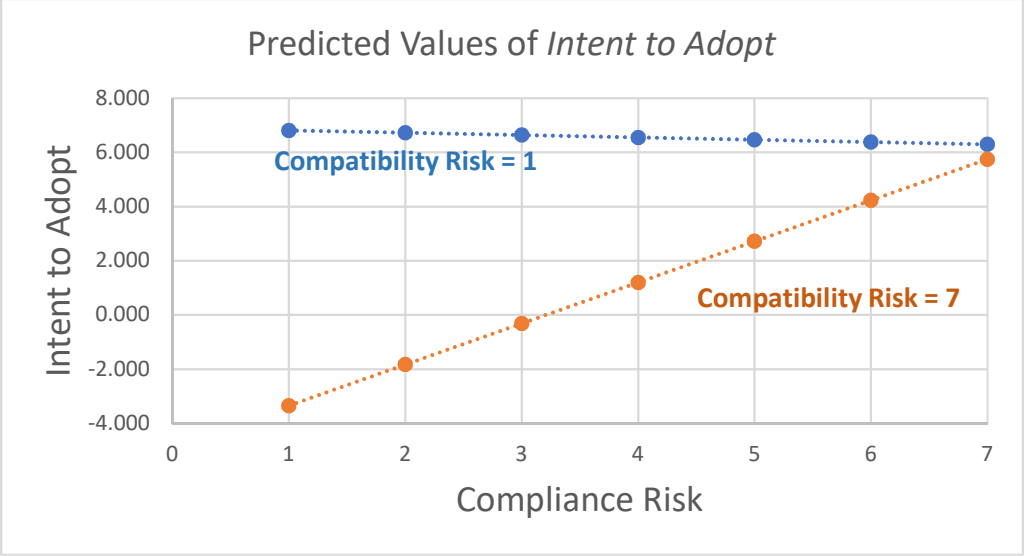

Figure 7. Interaction between compliance risk and *intent to adopt* when *compatibility risk* is set at low and high values.

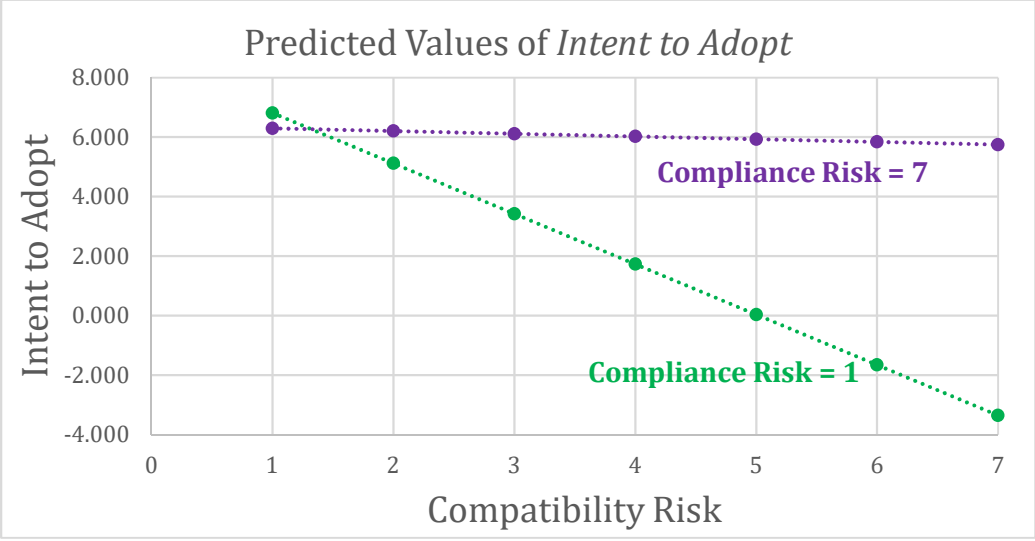

Figure 8. Interaction between *compatibility risk* and *intent to adopt* when *compliance risk* is set at low and high values.

Summary

I began Chapter 4 with information about the pilot study, and discussed the process that I undertook for the actual data collection to examine the cyber-risk implications of cloud-computing for the U.S. financial services section. The participants used for this study included IT and business leaders from U.S. financial services firms from the four geographical regions: The West, Midwest, Northeast, and South. Participants were presented with survey questions that focused on evaluating cyber-risks of six technological and organizational factors composing the independent variables—organization *size, relative advantage, compliance, security, compatibility, and complexity*—to measure the degree of perceived innovation risks influencing the dependent variable: the *intent to adopt cloud-computing* in the U.S. financial services sector. Information about these participants' responses including their demographics were analyzed.

I analyzed the research question, and conducted data cleaning and data screening to ensure the variables of interest in this study met appropriate statistical assumptions. Using this analytic strategy, I evaluated the variables for missing data, univariate outliers, normality of residuals, independence, linearity, homoscedasticity, and multicollinearity. Subsequently, I conducted multiple regression analysis to determine if there were any significant relationships between the variables.

Results from the multiple regression analysis conducted for Hypotheses 1-6 indicated that significant relationships existed between financial organizations' *intent to adopt* and two independent variables (*compliance risk*, $p = .01$, and *compatibility risk*, $p < .001$). There was no significant relationship between the dependent variable and the other four independent variables (*annual revenue, relative advantage, security risk, and complexity risk*, $p < .05$). Table 12 shows a summary of the results for Hypotheses 1-6.

Table 12

Summary of Results from the Multiple Regression Analysis Conducted for Hypotheses 1-6

Research Question	Dependent Variable	Independent Variable	Sig. (*p*)
H1	*Intent to Adopt*	Annual Revenue	0.324
H2	*Intent to Adopt*	Relative Advantage	0.683
H3	*Intent to Adopt*	Compliance Risk	0.010
H4	*Intent to Adopt*	Security Risk	0.593
H5	*Intent to Adopt*	Compatibility Risk	< .001
H6	*Intent to Adopt*	Complexity Risk	0.962

Note. $N = 112$.

Furthermore, I ran an additional regression analysis to test if a model consisting of *compliance risk, compatibility risk*, and an interaction term predicts *intent to adopt cloud-computing*. In Model 2, results indicated that a significant relationship existed between financial organizations' *intent to adopt cloud-computing* and a model containing the two independent variables and the interaction term.

In Chapter 5, I discuss this study's importance and its contribution to an understanding of the cyber risks for cloud-computing adoption in the U.S. financial services sector. I interpret the findings, present the theoretical implications, and offer recommendations for future research.

Chapter 5: Discussion, Conclusions, and Recommendations

The lack of information about cyber-risks represents a key gap in cloud-computing adoption in the financial services sector (Mandhala & Gupta, 2014). Therefore, the purpose of this cross-sectional study was to assess the relationship between the *intent to adopt cloud-computing* and key cyber risk adoption variables—security and compliance—in the U.S. financial services sector. Using DOI theory and the TOE framework as guidance, I used a cross-sectional quantitative instrument to survey businesses and IT leaders from the financial services sector in the four U.S. geographical regions—West, Midwest, Northeast, and South—via a SurveyMonkey audience pool. Respondents answered survey items to offer insight into their views of security and compliance risks relative to the adoption of cloud-computing in the financial services sector. The survey attracted 118 responses within 18 days. Six predictors of technological and organizational variables were specified: (a) annual revenue as a surrogate of organization size, (b) relative advantage, (c) compliance, (d) security, (e) compatibility, and (f) complexity. The dependent variable was *intent to adopt cloud-computing*.

The key findings that emerged from this study included significant relationships between the dependent variable and two of the six independent variables: *compliance* and *compatibility.* These two independent variables made significant contributions in explaining financial managers' *intent to adopt* scores. Specifically, there was a significant positive relationship between *intent to adopt* and *compliance risk* ($B = 0.304$, $p = .01$). and a significant negative relationship between *intent to adopt* and *compatibility risk* ($B = -0.542$, $p < .001$). Moreover, after conducting a regression analysis with just *compliance*

risk and *compatibility risk*, and an interaction term (*compliance*compatibility*), results indicated that a significant relationship existed between financial organizations' *intent to adopt cloud-computing* and a model containing the two independent variables and interaction term.

The remainder of this chapter provides a critical analysis and interpretation of the findings in light of DOI theory and the TOE framework . Subsequently, I present the study's limitations, recommendations for future studies, implications for positive social change, steps that members of the U.S. financial services sector can take to address the concerns and opportunities identified in this study.

Interpretation of Findings

Compatibility

In this study, the variable *compatibility risk* was found to be marginally related to *intent to adopt cloud-computing in the U.S. financial services firms*. It was retained in the final regression model because of the presence of an interaction term related to both remaining independent variables, which were significant in the original regression model. This variable construct, as operationally defined in Chapter 1, measured the degree to which an innovation is perceived to be consistent with an organization's needs, ideas, and socio-cultural values (Daugherty et al., 2011; Rogers, 2003). Results of the final model (Model 2) showed that there was a significant but negative relationship between *intent to adopt* and *compatibility risk* when participants' response to *compliance risk* was low. This suggests that as participant concern for compatibility increased, their likelihood to adopt cloud-computing conditionally decreased. Specifically, for low values of

compatibility risk, *intent to adopt* remain high, but for high values of *compatibility risk*, *intent to adopt* declined. This finding generally corroborated Rogers's (2003) DOI theory, and was found to be consistent with Fernandes et al.'s (2013) results that showed a strongly negative influence of compatibility on the *intent to adopt cloud-computing*. This influence of compatibility, according to Fernandes et al. (2013), may primarily be due to the current lack of standardization among cloud providers or proprietary formats. This lack of standardization may have provoked participants' concerns about whether their existing or legacy financial services technology infrastructure will be compatible with the current cloud solutions.

Compliance

The final model (Model 2) revealed that there was a significant positive relationship between *intent to adopt* and *compliance risk* provided participant's response to compatibility was high. In contrast, the relationship between *compliance risk* and *intent to adopt* remained weak when participants felt that *compatibility risk* was low. This suggests that *intent to adopt* varies as a function of *compliance risk* when *compatibility risk* is seen as a concern. That is, provided participants feel that *compatibility risk* is high, *intent to adopt cloud-computing* increases as participant's attitudes toward *compliance risk* increases. This finding is consistent with studies published by Wenge, Lampe, Müller, and Schaarschmidt (2014); and Gonzalez et al. (2012) that identified compliance as a critical reason why firms dread moving their infrastructure into the cloud. The results somewhat support the need for the U.S. financial services organizations considering cloud adoption, to seek out and understand specific regulatory requirements affecting

their market segment before extending their business to the cloud. While compliance covers a lot of ground, from government regulations such as the Sarbanes-Oxley Act for publicly traded organizations, industry regulations such as GLBA, Redflag for financial sector, PCI DSS for payment cards, and HIPAA for healthcare data, this variable should be operationalized within the context of maintaining compliance with financial industry specific regulatory requirements.

Interaction Between Compliance Risk and Compatibility Risk

As briefly discussed in Chapter 4, I conducted an additional regression analysis in which the alternate measure of my initial model consisting of two independent variables, *compliance* and *compatibility risk*, was substituted with another model consisting of *compliance risk, compatibility risk*, and an interaction term. Of greatest concern was whether the new model predicts *intent to adopt cloud-computing*. As found in Chapter 4, this model was superior to the first model. However, the relationship between the dependent variable and each independent variable was tempered by the presence of the interaction term.

The presence of a significant interaction indicates that the effect of one independent variable on the dependent variable is different at different values of the other independent variable. When *compatibility risk* is low (equal to 1), *intent to adopt* varies slightly with increases in *compliance risk*. When both *compatibility* and *compliance* are low, *intent to adopt* is high. Further*, intent to adopt* does not change significantly when *compatibility risk* is low, even with increases in *compliance risk*; in contrast, when *compatibility* is high (equal to 7), the relationship between *compliance risk* and *intent to*

adopt increases significantly. That is, as *compliance risk* values increase, *intent to adopt* scores increase. This may mean that when participants do not feel compatibility is a concern, their concern about compliance does not affect their willingness to adopt. This may be due to the importance that participants impose on compatibility. For example, when participants feel that compatibility issues can either be effortlessly resolved or do not really exists (due perhaps to a lack of understanding about the nature of technology cohabitation or supreme confidence in their own abilities) then *intent to adopt*, as a function of *compliance risk* is rendered neutral (Figure 8).

Referring back to Figures 7 and 8 in Chapter 4, when *compatibility risk* is low (equal to 1), the relationship between *intent to adopt* and *compliance risk* remains relatively constant with increases in *compliance risk*. But, *intent to adopt* changes significantly when *compatibility risk* is high, with increases in *compliance risk*. That is, when *compatibility* risk is high, a positive relationship between *compliance risk* and *intent to adopt*. Compatibility is the degree to which an innovation can be assimilated into the potential adopter's current practices, existing value system, and business needs (Rogers, 2003). Recent studies show that cloud-computing is more likely to be adopted when the adopters find it to be compatible with their business needs and value system (Tweel, 2012; Lee, 2015). Therefore, it may be expected that compatibility risks (the corollary of lack of compatibility) relates negatively to adoption. As revealed in this study, financial services leaders are less likely to adopt cloud-computing if its use does not align with their business needs or violates their cultural or social norms. In Figure 8, when *compliance risk* is low (equal to 1), *intent to adopt* decreases with increases in

compatibility risk. When both are low, *intent to adopt* is high. But, *intent to adopt* does not change significantly when *compliance risk* is high, even with increases in *compatibility risk*. This change in behavior may have been influenced by the participants' views of the cloud-computing's benefits versus risks. For example, if the purpose of cloud-computing adoption fits with the adopters' need to take advantage of the cost benefits of cloud-computing for their financial systems with low compliance concerns, then moving the systems to the cloud makes financial sense.

Complexity

Another important outcome from the analysis is that the independent variable *complexity* had no significant relationship with the *intent to adopt cloud-computing* in the U.S. financial services sector. One explanation for this is that because participants of this study were familiar with the concept of cloud-computing, it is possible that their previous experiences working with cloud-computing may have alleviated the perceived complexity risks surrounding the task of managing multiple cloud providers or shaped their views of the potential risks of extending financial services into the cloud. Although the result disconfirmed Rogers's (2003) DOI theory, and Lee's (2015) conjectures about the significant degree of influence of perceived complexity, it confirmed a result of Powelson's (2012) study that stipulated no correlation exists between the independent variable, *complexity* and *intent to adopt cloud-computing*.

As the final model combines two significant factors that influence cloud adoption, this perspective highlights the importance of understanding the benefits of technology risk (like compatibility) and the compliance aspects (such as compliance with industry

regulatory and standards) of cloud-computing in the U.S financial services sector. For example, the result provides a glimpse on the importance compatibility risk as it provides financial organizations' adopters great insights on whether their products will work in the cloud. The variance between compatible cloud products and the *intent to adopt cloud-computing* poses a variety of technical challenges, if not addressed, that could lead to a wasted investment down the road.

While it is important to mitigate product compatibility risk, simply moving products and customers' data from a traditional in-house data center to a compatible cloud environment does not absolve the financial organization of responsibility for regulatory compliance. A successful cloud-technology migration dictates a laser focus on compliance, as a single misstep can lead to escalating costs from poor regulatory control designs, and makes it difficult to ensure compliance with the industry regulations. To mitigate these risks and increase the rate of cloud-computing adoption, U.S. financial organizations' leaders must thoroughly understand the concepts of compatibility risk and regulatory compliance requirements of the cloud environment in which their organizations and their providers operate.

Other Factors

Results of the multiple regression analysis also revealed that there was no correlation between *revenue* and the dependent variable (*intent to adopt cloud-computing* in the U.S. financial services sector). As a recap of the operational definition presented in Chapter 1, revenue was used in this study as a surrogate of the organization's size to characterize the level of income. This is important when leaders

have to make quick and decisive adoption decisions to maintain and enhance the organization's competitive standing (Baker, 2012). A non-significant finding seems reasonable, as financial firms have the social and legal responsibility to protect their data irrespective of their size or their generated revenues.

For the third variable, *relative advantage,* this study showed no significant relationship with *intent to adopt cloud-computing* in the U.S. financial services sector. This result refutes the research conducted by Tweel (2012), and disconfirmed Rogers's DOI theory that stipulates that relative advantage is a critical factor for the adoption of new technology innovation (Rogers, 2003). This finding implies that financial organizations may not realize the relative advantage of cloud-computing adoption for their business over the traditional hosting environment. One possible reason is that given cloud-computing is a new technology with relatively complex costing model, financial organizations may consider trading off this relative advantage and thus, representing a major hurdle to cloud-computing adoption in the financial services sector (Wang et al., 2012).

Another interesting finding from the regression analysis was that *security* showed no significant relationship with the *intent to adopt cloud-computing* in the financial services sector. This result is contrary to Fernandes et al. (2014), who identified a list of cybersecurity threats as top contributors to factors impeding financial services firms' use of cloud-computing. One likely explanation for this is the organizations' reliance on third parties for securing the business in a cloud-computing environment. The fact that the financial organizations, upon adoption, would be migrating their business applications

and data to the third-party cloud relieves them of the burden to secure the business in the distributed environment, and proved a non-significant stumbling block for the *intent to adopt cloud-computing* in the U.S. financial sector.

A closer examination of the participants' responses, however, revealed some interesting insights. The majority of the participants surveyed for this study revealed security as a major concern that limits the adoption of cloud-computing in the U.S. financial services industry. On average, participants acknowledged security as a serious risk with the potential to affect their adoption of cloud-computing. For example, they indicated serious concerns with the idea of handing over important business data to another company or extending their critical technology infrastructure or strategic business data into the cloud as result of security. A majority of the participants also endorsed security risk as an issue for cloud-computing adoption. This empirical study thus confirmed that there is a continued concern for security regarding cloud-computing adoption.

Limitations of the Study

There were several limitations identified in this study. First, participants were IT and business leaders working in the financial sector. All participants were obtained via SurveyMonkey panels. According to SurveyMonkey, participants were incentivized to take the survey by donating money to recognized charities. As such, these participants may not fully represent the views of all financial sector leaders. This means that study participants may harbor different opinions, given their social perspective toward charitable giving compared to those leaders who did not voluntarily subscribe to

SurveyMonkey's conditions. Therefore, generalizability of results is restricted only to leaders with demographics similar to participants from this study.

Second, the general linear model (GLM) was used to test the hypotheses in the study. As such, study findings are limited by the unique characteristics of the data collected. Notwithstanding, the results provide evidence supporting the reliability of the instrument. Several other limitations related to this study were identified in Chapter 1 to address known areas of scholarly weaknesses that could potentially affect the execution of this study, or the reliability of its results. This section provides a disclosure of steps taken to mitigate those concerns, as well as the interpretation of the analysis and findings that were presented in this chapter.

A limitation presented in Chapter 1 was the potential to omit or underrepresent all the factors associated with cloud-computing innovation. The use of DOI and TOE as the theoretical framework and the extensive review of recent cloud-computing studies that focus on cybersecurity risks helped extend the theoretical constructs of this study. Specifically, the preliminary research I conducted to uncover the key factors affecting perceived cybersecurity risks surrounding cloud-computing adoption provided me with substantive evidence and informed strategies by which to identify the key cloud-computing cybersecurity risks. Additionally, this limitation was mitigated to a lesser degree by mapping out the DOI and TOE theoretical components, CSA, and NIST cybersecurity framework to explicitly identify key independent variables to measure the perceived cybersecurity risks surrounding cloud-computing adoption.

Another previously identified limitation of this study was related to potential sampling biases (Mandel & Rinott, 2014) resulting from poorly worded research questions, and their unintentional influence on the participants' answers to the survey questions (Fowler, 2013). For this study, I used an existing survey instrument, and modified it to focus on cybersecurity risks factors identified from preliminary scholarly studies that were recently conducted in this research area. Furthermore, I used six personal contacts from my professional network who are IT experts with backgrounds in financial services to review and cognitively verify the survey instrument for badly worded questions that could incite potential bias during the pilot phase of this study. These contacts also pretested the survey instrument prior to sending it out to the survey participants for data collection (Fowler, 2013). The result of the review showed no concerns about structure, wording, or sequence of the questions, thus mitigating this limitation. Furthermore, I conducted a Cronbach's alpha reliability test on the dependent and independent variables to examine the properties of measurement scales and the items that compose the scales (Tabachnick & Fidell, 2013). The results of the test showed no variables violated the assumption ($p > .80$), thus confirming the reliability of the dependent and independent variables.

Given that this cross-sectional study has the potential to extend the theoretical applicability of the cybersecurity factors underpinning cloud-computing adoption for the financial services sector, it was important that study participants were members of the U.S. financial services community (Romanosky, 2016). The study therefore used the SurveyMonkey audience service to source participants for this study from a sample of

qualified financial services IT and business leaders from the four geographical zones of the United States: the West, Midwest, Northeast, and South regions. The general nature of the research participants included IT and business leaders who are well grounded in this market sector and familiar with the concepts of cloud-computing. I entrusted SurveyMonkey audience service to acquire the required data from participants who met the aforementioned criteria and also provided those participants with an acknowledgement form to further verify that they met the key requirements of this study. Despite this effort to obtain participants who met the selection criteria, this study is limited by the accuracy of SurveyMonkey's selection algorithms.

Recommendations

Recommendations for Researchers

This study explored the relationship between six risk independent variables (*annual revenue, relative advantage, compliance risk, security risk, compatibility, and complexity belief*) and a dependent variable: *intent to adopt cloud-computing in the U.S. financial services sector*. The results of the study revealed that two of the six independent variables (*compliance* and *compatibility*) were negatively related to the *intent to adopt cloud-computing* in the financial services sector. The knowledge from this study can be used to fine-tune the predictive model for evaluating the *intent to adopt cloud-computing* within the targeted market sector. As Wenge et al. (2014) pointed out, the financial industry is one of the most highly regulated industrial sectors in the U.S; therefore, fulfilling the compliance requirements to ascertain the protection of its strategic business information is one of the most important objectives for any financial institution (Shue,

2013). A key challenge for financial institutions, as prospective cloud adopters, centers primarily on understanding the regulatory requirements for a secure cloud adoption, rather than technical challenges. To improve understanding about the cybersecurity risk of the cloud, it is important that designers of future studies also consider compatibility of cloud-computing with the adopters' business needs, existing value and strategic goals in their adoption decision models. Researchers may facilitate the adoption movement within the financial market segment through the predictive research model (Model 2) proposed in this study to operationalize compliance and compatibility concerns and test their hypotheses by specifying these as independent variables.

Adoption of cloud-computing in the financial services sector is relatively new, with limited regulatory guidance or studies providing a best-practices approach to evaluating cybersecurity risks for cloud adopters in the financial services environment. Since my research is a relatively new study examining the risk implications of cybersecurity on the *intent to adopt cloud-computing* in the financial services sector, it is recommended that further studies be conducted in this area as more regulatory guidance becomes available. Also, since this study broadly identified the financial services sector and focused only on the United States, there may also be a need to further conduct this type of study in other countries, in a broader context, to validate this study's hypotheses and to compare results.

Recommendations for Practice

Practitioners should consider findings from this study to help them make informed decisions about cloud-computing adoption. As discussed in Chapter 4,

compliance risk was found to be a negative predictor of *intent to adopt cloud-computing*. However, *intent to adopt* scores remained relatively high across low and high *compliance* values. Of interest, though, when *compatibility risk* was perceived to be high (values equal to 7), *intent to adopt* scores increased when *compliance risk* values changed from low to high. This implies that despite the perceived risk in complying with industry standards, the willingness to adopt cloud-computing depends on how participants feel about compatibility. As such, practitioners should concentrate on compatibility over compliance. That is, this information suggests that practitioners should focus on compatibility risk to mitigate internal resistance to cloud-computing adoption.

The identification of *compliance* and *compatibility risks* as significant negative but interrelated factors influencing t*he intent to adopt cloud-computing in the U.S. financial services*, in this study, buttresses the important roles and responsibilities of cloud service providers and regulators in the acceleration of cloud-computing services. These encompass a strategic involvement and partnership among the financial institutions, the industry-specific regulatory bodies, and cloud-computing providers. The cloud providers will need to work with financial firms to understand their industry-specific needs and requirements, especially from the standpoint of technology compatibility.

As compliance may be a factor in adoption-predicting requisite in the U.S. financial services sector, cloud adoption must be considered within the context of compatibility. A key recommendation for practice is that cloud providers should partner with leaders of financial services firms to gain a deeper understanding of their computer infrastructure

and depth of concern related to compatibility. As this specific guidance becomes mainstream, the U.S. financial services providers as well as institutions will become comfortable moving their critical business data to the cloud, thus resulting in wider adoption of cloud-computing services in the U.S. financial sector.

Implications

This study also holds the potential to positively influence the adoption of cloud-computing in the U.S. financial services sector in three ways. First, its contributions to social change can be realized through operational efficiency for the financial firms and cost saving for consumers. It contributes to the efforts to combat global warming. And last, it improves understanding of the predictive model for evaluating the theoretical and practical implications of cybersecurity risks on the adoption of cloud-computing, as discussed below:

Significance to Social Change

One can express the implications of this study for social change in terms of operational efficiency for organizations, and the area of cost improvements for consumers. Cloud-computing creates a significant opportunity for banks to improve or optimize their existing legacy technologies and add competitive dynamics to the way financial products are delivered to consumers. The transformative nature of cloud technologies provides financial services firms unique opportunities to expand their legacy systems and try completely new services and processes, such as reverse auctions and third-party core banking systems (Gartner, 2011). With a clear understanding of cyber-risks associated with cloud-computing, financial administrators can reduce security and

compliance concerns. This may lead to the emergence of successful cloud business delivery models for organizations in this sector. The new cloud business model will likely help financial services firms expand their products and services. Also, by understanding the true cyber-risks of cloud-computing and ways to mitigate them, financial services firms' administrators are more likely to adopt cost-effective cloud-computing to process their core business functions. Cost savings from this adoption will make financial products and services potentially more affordable to consumers.

Contribution to Efforts to Combat Global Warming

As noted in Chapter 1, this study also contributes to efforts to combat global warming. Research shows that carbon emissions are presenting an increasing threat to society as well as the climate (Singh et al., 2015). Cloud-computing has been identified as the IT method most capable of reducing paper consumption, thereby reducing environmental pollution resulting from paper disposal, saving energy, and increasing organizations' high efficiency (Liang at al., 2012). Also, the financial services sector's increased use of cloud-computing will help reduce the disposal of great amounts of data-center resources that often contribute to climate change and seriously threaten the quality of life on earth (Gattulli et al., 2012; Liang et al., 2012).

Contribution to Theory

Cybersecurity is a relatively new area of research, especially when evaluating its wide consequences on the adoption of new technology delivery like cloud-computing. Many studies have established the validity of DOI as a theoretical construct for determining adopters' intentions in innovation adoption studies. However, the

implication of cybersecurity risks and their influence on such intentions to adopt cloud-computing have not been addressed by scholars. This study contributes to closing this gap by providing a model that integrates two of the theoretical technology adoption models, and mapping them to two important cybersecurity risk management frameworks (NIST and CSA) to improve prediction of adoption.

Conclusions

Adoption of cloud technologies in the banks represents an innovation with potential to challenge the traditional means of technology delivery to consumers. Cloud-computing creates a significant opportunity for banks to improve or optimize their existing legacy technologies and add competitive dynamics to the way financial products are delivered to consumers. Unfortunately, the need for banks to safeguard their customer information has forced most bank leaders to take a back seat in cloud-computing adoption to manage their business functions. Bank leaders' concerns around security and privacy of their customer nonpublic information (CNPI) in the cloud and the computing orchestration about data locality across domains and jurisdictions appear to have impeded the adoption of cloud-computing in the U.S. financial services sector.

Prior studies have identified technology—particularly, information security and regulatory compliance requirements—as the major hurdle inhibiting the adoption of cloud-computing in financial services firms (Aleem & Sprott, 2013; Dutta et al., 2013). However, missing in the literature is the degree of influence of the various security and compliance factors on the *intent to adopt cloud-computing*. This study attempted to close this gap through a cross-sectional quantitative approach. In this study, I used a

questionnaire through the SurveyMonkey Audience service, to attract 118 IT and business leaders from the U.S. financial services sector across the four U.S. geographic regions to assess the cybersecurity factors— security and compliance risks—slowing down the adoption of cloud-computing in the U.S. financial sector. In this study, six predictable variables (*relative advantage, complexity, compatibility, annual revenue, security, and compliance*) were tested against the dependent variable (*the intent to adopt cloud-computing in the U.S. financial services sector*). The results from the multiple regression analysis conducted for Hypotheses 1-6 indicated that significant relationships existed between financial organizations' managers' *intent to adopt cloud-computing* and two independent variables (*compliance risk*, $p = .01$, and *compatibility risk*, $p < .001$). There was no significant relationship between the dependent variable and the four remaining independent variables (*annual revenue, relative advantage, security risk*, and *complexity risk*, $p < .05$).

Findings revealed that compatibility may be the main enabler of cloud-computing in the U.S. financial industry. They provided additional insights about the importance of understanding the broad regulatory requirements for a secure cloud adoption, rather than focusing only on technical challenge. With good understanding of compliance risk requirements, and concerted efforts to developing control standards that allow for sufficient system compatibility among providers, many of the cybersecurity risks impeding cloud-computing adoption can be reasonably mitigated.

References

Abbott, M., & McKinney, J. (2013). *Understanding and applying research design*. Hoboken, NJ: Wiley.

Accenture. (2009). A new era in banking: Cloud-computing changes the game. Accenture Technologies. Retrieved from http://www.accenture.com/ SiteCollection Documents/PDF/Accenture-New-Era-Banking-Cloud-Computing-Changes-Game.pdf

Ahmadalinejad, M., Hashem, S. M., & Branch, Q. (2015). A national model to supervise on virtual banking systems through the Bank 2.0 approach. *Advances in Computer Science: An International Journal*, *4*(1), 83-93. Retrieved from https://www. researchgate.net/profile/Mehrpooya_ Ahmadalinejad/ publication/271587675_ A_National_Model_to_Supervise_on_Virtual_Banking_Systems_through_the_Bank_2.0_Approach/links/54cd2b080cf29ca810f78f4a.pdf

Aleem, A., & Sprott, C. R. (2013). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime, 20*(1), 6-24. doi: 10.1108/13590791311287337

Aljabre, A. (2012). Cloud-computing for increased business value. *International Journal of Business and Social Science*, *3*(1), 234-239. doi: 10.1002/9781119204732.ch25

Al-Jabri, I. M., & Sohail, M. S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research*, *13*(4), 379-391. Retrieved from https://ssrn.com/abstract=2523623

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud-computing adoption by SMEs in the northeast of England: A multi-perspective framework. *Journal of Enterprise Information Management, 26*(3), 250-275. doi: 10.1108/17410391311325225

Alzahrani, A., Alalwan, N., & Sarrab, M. (2014, April). *Mobile cloud-computing: advantage, disadvantage and open challenge*. Paper presented at the annual meeting of the Seventh Euro American Conference on Telematics and Information Systems, Valparaiso, Chile. doi: 10.1145/2590651.2590670.

Apostu, A., Rednic, E., & Puican, F. (2012). Modeling cloud architecture in banking systems. *Procedia—Economics and Finance*, *3*, 543-548. doi:10.1016/S2212-5671(12)00193-1

Ardjouman, D. (2014). Factors influencing small and medium enterprises (SMEs) in adoption and use of technology in Cote d'Ivoire. *International Journal of Business and Management, 9*(8), 179-190.doi: 10.5539/ijbm.v9n8p179

Armstrong, J. S. (2012). Illusions in regression analysis. *International Journal of Forecasting*, *28*(3), 689. doi:10.1016/j.ijforecast.2012.02.001

Arthur, C. A., & Hardy, L. (2014). Transformational leadership: A quasi-experimental study. *Leadership & Organization Development Journal, 35*(1), 38-53. doi: 10.1108/LODJ-03-2012-0033

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research, 12*(1), 1-11., doi: 10.1080/13669 870802488883

Babbie, E. (2013). *The basics of social research* (6th ed.). Belmont, CA: Thomson Wadsworth.

Baker, J. (2012). The technology–organization–environment framework. In Y. K. Dwivedi et al. (Eds.), *Information systems theory: Explaining and predicting our digital society, Vol. I* (pp. 231-245). New York, NY: Springer. doi:10.1007/978-1-4419-6108-2_12

Bassett, W. F., Lee, S. J., & Spiller, T. P. (2015). Estimating changes in supervisory standards and their economic effects. *Journal of Banking & Finance*, *60*, 21-43.doi: 10.1016/j.jbankfin.2015.07.010

Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2014). Security issues in cloud-computing. *Acta Technica Corviniensis–Bulletin of Engineering*, *7*(4), 159.doi: 10.1007/978-3-662-45237-0_12

Bidgoli, H. (2011). Successful introduction of cloud-computing into your organization: A six-step conceptual model. *Journal of International Technology and Information Management*, *20*(1), 21-38. Retrieved from http://www.iima.org/index.php?option=com_phocadownload&view=section&id=11&Itemid=77

Blair, J., Czaja, R. F., & Blair, E. A. (2013). *Designing surveys: A guide to decisions and procedures* (3rd ed.). Thousand Oaks, CA*:* Sage.

Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013, January). *Cloudrise: Exploring cloud-computing adoption and governance with the TOE framework*. Paper presented at the 46th Hawaii International Conference on System Sciences (HICSS), Wailea, Maui, HI. doi:1109/HICSS.2013. 132

Bose, R., Luo, X. R., & Liu, Y. (2013). The roles of security and trust: Comparing cloud-computing and banking. *Procedia—Social and Behavioral Sciences*, *73*, 30-34. doi:10.1016/j.sbspro.2013.02.015

Brakerski, Z., & Vaikuntanathan, V. (2014). Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing, 43*(2), 831-871. doi: 10.1137/120868669

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

Carcary, M., Doherty, E., & Conway, G. (2013). The adoption of cloud-computing by Irish SMEs: An exploratory study. *Electronic Journal of Information Systems Evaluation, 16*(4), 258-269. doi: 10.1080/10580530. 2014.958028

Cegielski, C. G., Jones-Farmer, L. A., Wu, Y., & Hazen, B. T. (2012). Adoption of cloud-computing technologies in supply chains. *International Journal of Logistics Management, 23*(2), 184-211. doi:10.1108/09574091211265350

Chang, B. Y., Hai, P. H., Seo, D. W., Lee, J. H., & Yoon, S. H. (2013, January). *The determinant of adoption in cloud-computing in Vietnam.* Paper presented at the IEEE International Conference on Computing, Management and Telecommunications, Ho Chi Minh City, Vietnam. doi: 10.1109/ComManTel. 2013.6482429

Chen, D., & Zhao, H. (2012, March). *Data security and privacy protection issues in cloud-computing*. Paper presented at the International Conference on Computer

Science and Electronics Engineering, Hangzhao, China. doi:10.1109/ICCSEE. 2012.193

Chopra, M., Mungi, J., & Chopra, K. (2013). A survey on use of cloud-computing in various fields. *International Journal of Science, Engineering and Technology Research*, *2*(2), 480-488. Retrieved from http://ijsetr.org

Chuang, C. C., & Hu, F. L. (2015). Technology strategy-innovating for growth of ANZ Bank. *International Review of Management and Business Research*, *4*(3), 682. Retrieved from http://www.irmbrjournal.com/papers/1438579 293.pdf

Chytilova, H., & Maialeh, R. (2015). Internal and external validity in experimental economics. *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, *9*(6), 1904-1911.Retrieved from http://www.waset.org/ publications/10001764

Cisco, Inc. (2015). *Cisco global cloud index 2014–2019: Forecast and methodology*. San Jose, CA: Author. Retrieved from https://newsroom. cisco.com/press-release-content?articleId=1724918

Clark, T. S., & Linzer, D. A. (2015). Should I use fixed or random effects? *Political Science Research and Methods*, *3*(2), 399-408.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/ correlation analysis for the behavioral sciences*. London, UK: Routledge.

Cooper, D. R., & Schindler, P. S. (2014). *Business research methods* (12th ed.). Boston, MA: McGraw Hill Irwin.

Cope, D. (2015). Cybersecurity assessment tool: Helps combat risk. *American Bankers Association. ABA Banking Journal*, *107*(4), 48. doi: 10.1188/14. ONF.89-91

Cuomo, A. M., & Lawsky, B. M. (2014, May). *Report on cyber security in the banking sector*. Department of Financial Services, New York State. Retrieved from http://www.dfs.ny.gov/about/press2014/pr1405061.htm

Daugherty, P. J., Chen, H., and Ferrin, B. G. (2011). Organizational structure ande logistics service innovation. *International Journal of Logistics Management*, *22*(1), 26-51. doi:10.1108/0957409 1111127543

Dawson, C. (2016). Law enforcement and the attribution problem in cyberspace. *Journal of the Australian Institute of Professional Intelligence Officers*, *24*(2), 32. Retrieved from https://search. informit.com.au/ documentSummary;dn= 4563571762814 31;res=IELHSS

Demirkan, H., & Delen, D. (2013). Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud. *Decision Support Systems*, *55*(1), 412-421. doi:10.1016/j. dss.2012.05.048

De Vaus, D. (2013). *Surveys in social research* (6th ed.). New York, NY: Routledge.

Dhar, S. (2012). From outsourcing to cloud-computing: Evolution of IT services. *Management Research Review, 35*(8), 664-675. doi:10.11 08/0140917 1211247677

Dillman, D. A. (2011). *Mail and Internet surveys: The tailored design method* (Rev. ed.). Hoboken, NJ: Wiley.

dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2013, May). *Risk-based dynamic access control for a highly scalable cloud federation*. Paper presented at the Seventh International Conference on Emerging Security Information Systems and Technologies, Krakow, Poland. doi: 10.1109/ NOMS.2014.6838319

Doyle, G. J., Garrett, B., & Currie, L. M. (2014). Integrating mobile devices into nursing curricula: Opportunities for implementation using Rogers's Diffusion of Innovation model. *Nurse Education Today*, *34*(5), 775-782. doi: 10.1016/j.nedt. 2013.10.021

Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533-578. doi: 10.1017/S1816383113000246

Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in enterprise cloud-computing: The perspectives of IT experts. *Journal of Computer Information Systems, 53*(4), 39-48. Retrieved from http://eprints. whiterose.ac.uk/79144/2/WRRO_7 9144.pdf

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2013). *G* Power Version 3.1. 7 [Windows]*. Kiel, DE: Universität Kiel.

Fernandes, D. A., B., Soares, L. F., B., Gomes, J. V., Freire, M., & Inácio, P. R., (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*(2), 113-170. doi: 10.1007/s10207-013-0208-7

Fichman, R. G. (1992, December). Information technology diffusion: A review of empirical research. *Proceedings of the Thirteenth International Conference on*

Information Systems. (ICIS), 195-206. Retrieved from http://tx.liberal.ntu.edu.tw/ SilverJay/Literature/! Adoption/Fichman_1992_ICIS_IT_Diff_Review.pdf

Fichman, R. G. (2004). Real options and IT platform adoption: Implications for theory and practice. *Information Systems Research, 15*(2), 132-154. doi: 10.1287/isre. 1040.0021

Fichman, R. G., & Kemerer, C. F. (1997). The assimilation of software process innovations: An organizational learning perspective. *Management Science*, 43(1), 1345-1363. doi:10.1287/mnsc.43. 10.1345

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). London, UK: Sage.

Fincham, J. E., & Draugalis, J. R. (2013). The importance of survey research standards. *American Journal of Pharmaceutical Education*, *77*(1), 4. doi: 10.5688/ajpe7714

Fowler, F. (2013). *Survey research methods* (5th ed.). Thousand Oaks, CA: Sage.

Frankfort-Nachmias, C., & Nachmias, D. (2008). *Research methods in the social sciences* (7th ed.). New York, NY: Worth.

Frankfort-Nachmias, C., Nachmias, D., & DeWaard, J. (2014). *Research methods in the social sciences* (8th ed.). New York, NY: Worth.

Frăţilă, L. A., Zota, R. D., & Constantinescu, R. (2013). An analysis of the Romanian internet banking market from the perspective of cloud-computing services. *Procedia—Economics and Finance*, *6*, 770-775. doi:10.1016/S2212-5671 (13)00201-3

Garg, S. K., & Buyya, R. (2012). Green cloud-computing and environmental sustainability. *Harnessing Green IT: Principles and Practices*, 315-340. doi: 10.1002/9781118305393.ch16

Gartner, Inc. (2011, October 31). Gartner says cloud banking can drive "creative destruction" in the banking industry. [Press release, Egham, UK.] Retrieved from http://www.gartner.com/newsroom/ id/1835114

Gattulli, M., Tornatore, M., Fiandra, R., & Pattavina, A. (2012, June). *Low-carbon routing algorithms for cloud-computing services in IP-over-WDM networks*. Paper presented at the International Conference on Communications (ICC), Ottawa, Ontario, Canada. doi: 10.1109/ICC.2012. 6364347

Gaughan, D. J. (2015). Risk governance and culture frameworks for banks. Retrieved from http://www.aon.com/risk-services/asats/ attachments/Aon-BT-Risk-Governance-for-Banks-Whitepaper.pdf

Géczy, P., Izumi, N., & Hasida, K. (2012). Cloudsourcing: Managing cloud adoption. *Global Journal of Business Research*, *6*(2), 57-70. Retrieved from http://papers. ssrn.com/sol3/papers.cfm?abstract_id=1945858

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud-computing. *Journal of Cloud-Computing: Advances, Systems and Applications*, *1*(1), 11. doi: 10.1186/2192-113X-1-11

Green, S. B., & Salkind, N. J. (2010). *Using SPSS for Windows and Macintosh: Analyzing and understanding data* (6th ed.). Upper Saddle River, NJ: Pearson.

Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud-computing: A survey. *Journal of Cloud-Computing, 1*(1), 1-18. doi: 10. 1186/2192-113X-1-19.

Hanmer, M., Herrnson, P. S., & Smith, C. (2015). The impact of e-mail on the use of new convenience voting methods and turnout by overseas voters: A field experiment to address their challenges with new technology. *Election Law Journal*. *14*(2), 97-110. doi:10.1089/elj.2014.0266.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud-computing. *Journal of Internet Services and Applications*, 4(1), 1-13. doi: 10.1186/ 1869-0238-4-5

Hogben, A. (2016, August 22). Stepping into the clouds: The evolution of ATMs. NCR Corporation. Retrieved from https://www.ncr.com/ company/blogs/financial/ stepping-clouds-evolution-atms-1

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891-903. Retrieved from http://www.cyber-crimejournal. com/holtetal2012janijcc.pdf

Hoppermann, J. (2011, December). Off-the-shelf banking platforms are still scarce in the cloud. Small banks are cloud providers' primary target market in the banking space. Forrester Research. Retrieved from Forrester.com

Howell-Barber, H., Lawler, J., Desai, S., & Joseph, A. (2013). A study of cloud-computing software-as-a-service (SaaS) in financial firms. *Journal of Information*

Systems Applied Research, *6*(3), 4-17. Retrieved from http://jisar.org/2013-6/N3/JISARv6n3.pdf#page=4

Hutchison, P. D., Fleischman, G. M., & Johnson, D. W. (2014). E-mail versus mail surveys: A comparative study. *Review of Business Information Systems (RBIS)*, *2*(3), 43-56. Retrieved from http://cluteinstitute.com/ojs/index. php/RBIS/article/viewFile/8466/8477

Jacobs, S. R., Weiner, B. J., Reeve, B. B., Hofmann, D. A., & Christian, M. (2015). The missing link: A test of Klein and Sorra's proposed relationship between implementation climate, innovation-values fit and implementation effectiveness. *Implementation Science*, *10*(Suppl 1), A18. doi: 10.1186/1748-5908-10-S1-A18

Jadeja, Y., & Modi, K. (2012, March). *Cloud-computing-concepts, architecture and challenges.* Paper presented at the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Kumaracoil, India. doi: 10. 1109/ICCEET. 2012.6203873

Kamalian, A. R., Rashki, D. M., & Arbabi, M. L. (2011). Barriers to innovation among Iranian SMEs. *Asian Journal of Development Matters*, *5*(2), 251-265. Retrieved from http://www.indianjournals.com/ijor.aspx?target=ijor: ajdm&volume=5&issue=2&article=036

Kasper, J., Hoffmann, F., Heesen, C., Köpke, S., & Geiger, F. (2012). Completing the third person's perspective on patients' involvement in medical decision-making: Approaching the full picture. *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen*, *106*(4), 275-283. doi: 10.1016/j.zefq. 2012.04.005

Klein, K. J., & Knight, A. P. (2005). Innovation implementation: Overcoming the challenge. *Current Directions in Psychological Science*, *14,* 243-246. http://www-management.wharton.upenn.edu/klein/documents/New_ Folder/Klein_Knight_ Current_Directions_Implementation.pdf

Klein, K. J., & Ralls, R. S. (1995). The organizational dynamics of computerized technology implementation: A review of the empirical literature. In L. R. Gomez-Mejia and M. W. Lawless (Eds.), *Advances in global high-technology management* (Vol. 5, Part A, pp. 31-79). Greenwich, CT: JAI Press. Retrieved from http://www-management.wharton.upenn.edu/klein/ documents/Klein_ Ralls_1995.pdf

Klein, K. J., & Sorra, J. S. (1996). The challenge of innovation implementation. *Academy of Management Review*, *21,* 1055-1080. doi: 10.5465/AMR.1996. 9704071863

Knight, K. L. (2010). Study/experimental/research design: Much more than statistics. *Journal of Athletic Training, 45*(1), 98-100. doi:10.4085/ 1062-6050-45.1.98

Kothari, C. R. (2005). *Research methodology: methods and techniques (5th ed.)*. New Delhi, India: New Age International.

Kraemer, H. C., Yesavage, J. A., Taylor, J. L., & Kupfer, D. (2014). How can we learn about developmental processes from cross-sectional studies, or can we? *American Journal of Psychiatry*, 157, 163-171. doi: 10.1176/appi.ajp. 157.2.163

Kulkarni, G., Gambhir, J., Patil, T., & Dongare, A. (2012, June). *A security aspects in cloud-computing.* Paper presented at the Third International Conference on

Software Engineering and Service Science (ICSESS), Beijing, China. doi:10.1109/ICSESS.2012.6269525

Kallberg, J., & Thuraisingham, B. (2012, June). *Towards cyber operations - The new role of academic cyber security research and education.* Paper presented at the International Conference on Intelligence and Security Informatics (ISI), Arlington, VA. doi: 10.1109/ISI.2012.6284146

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

Lameck, W. U. (2013). Sampling design, validity and reliability in general social survey. *International Journal of Academic Research in Business and Social Sciences, 3*(7). 212-218. doi:10.6007/ IJARBSS/ v3-i7/27

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud-computing risk assessment: A systematic literature review. In J. J. Park, I. Stojmenovic, M. Choi, & F. Xhafa (Eds.), *Future information technology* (pp. 285-295). Berlin, DE: Springer. doi: 10.1007/978-3-642-40861-8_42

Lau, R. Y., Xia, Y., & Ye, Y. (2014). A probabilistic generative model for mining cyber-criminal networks from online social media. *Computational Intelligence Magazine, IEEE, 9*(1), 31-43. doi: 10.1109/MCI.2013.2291689

Lee, S. G., Trimi, S., & Kim, C. (2013). Innovation and imitation effects' dynamics in technology adoption. *Industrial Management & Data Systems*, *113*(6), 772-799. doi: 10.1108/IMDS-02-2013-0065

Lee, T. H. (2015). *Regression analysis of cloud-computing adoption for U.S. hospitals* (Order No. 3703337). Available from Dissertations & Theses @ Walden University. (1688791348).

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (8th ed.). Boston, MA: Pearson.

Leon-Guerrero, A., & Frankfort-Nachmias, C. (2014). *Essentials of social statistics for a diverse society*. Thousand Oaks, CA*:* Sage.

Liang, D. H., Liang, D. S., & Chang, C. P. (2012, January). *Cloud-computing and green management*. Paper presented at the Second International Conference on Intelligent System Design and Engineering Applications (ISDEA), Sanya, Hainan China. doi:10.1109/isdea.2012.583

Lin, A., & Chen, N. C. (2012). Cloud-computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, *32*(6), 533-540. doi: 10.1016/j.ijinfo mgt.2012.04.001

Mandel, M., & Rinott, Y. (2014). Estimation from cross-sectional samples under bias and dependence. *Biometrika*, *101*(3), 719-725. doi: 10.1093/biomet/ asu013

Mandhala, V. N., & Gupta, N. Y. (2014). Secure based financial transactions in banks using community cloud. *E-Commerce for Future & Trends*, *1*(1), 15-20. Retrieved from http://www.aisti.eu/risti/risti16a.pdf

Maronick, T. J. (2009). The role of the internet in survey research: Guidelines for researchers and experts. *Journal of Global Business and Technology*, *5*(1), 18-31.

Retrieved from https://www.questia.com/read/1P3-1741178861/the-role-of-the-internet-in-survey-research-guidelines

Marrero-Almonte, R., Marín-Tordera, E., Masip-Bruin, X., Nuez-Baldoma, R., Batlle-Ferrer, J., & Ren, G. (2014, November). *A smart drive to future transport systems*. Paper presented at the International Conference on Connected Vehicles and Expo (ICCVE), Vienna, Austria. doi:10.1109/ ICCVE.2014.7297615

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

Martens, B., & Teuteberg, F. (2012). Decision-making in cloud-computing environments: A cost and risk based approach. *Information Systems Frontiers*, *14*(4), 871-893. doi: 10.1007/s10796-011-9317-x

Maxwell, S. E., Cole, D. A., & Mitchell, M. A. (2011). Bias in cross-sectional analyses of longitudinal mediation: Partial and complete mediation under an autoregressive model. *Multivariate Behavioral Research*, *46*(5), 816-841. doi: 10.1080/00273 171.2011.606716

Mayoh, J., & Onwuegbuzie, A. J. (2013). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research*, *9*(1), 91-107. doi: 10.1177/1558689813505358.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23-41.doi: 10.1080/1533 2861.2010.487415

Mell, P., & Grance, T. (2011). The NIST definition of cloud-computing. *NIST Special Publication, 800*(145), 1-7. doi:10.6028/nist.sp.800-145

Moreno-Vozmediano, R., Montero, R. S., & Llorente, I. M. (2013). Key challenges in cloud-computing: Enabling the future internet of services. *Internet Computing, IEEE*, *17*(4), 18-25. doi:10.1109/mic.2012.69

Nicoletti, B. (2013). *Cloud-computing in financial services*. New York, NY: Palgrave Macmillan. doi:10.1057/9781137273642

Obeidat, M. A., & Turgay, T. (2013). Empirical analysis for the factors affecting the adoption of cloud-computing initiatives by information technology executives. *Journal of Management Research, 5*(1), 152-178. doi:10.5296/jmr.v5i1.2764

Olayemi, O. J. (2014). A socio-technological analysis of cyber-crime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116-125. doi:10.5897/ijsa2013.0510

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation*, *14*(1), 110-121. Retrieved from http://www.ejise.com/volume 14/issue1/p110

Paulauskas, N., & Garsva, E. (2015). Computer system attack classification. *Elektronika ir Elektrotechnika*, *66*(2), 84-87. Retrieved from http://www. kalbos.ktu.lt/index. php/elt/index

Pearson, S. (2013). Privacy, security and trust in cloud-computing. In S. Pearson & G. Yee (Eds.), *Privacy and security for cloud-computing, computer communications*

and networks (pp. 3-42). London, UK: Springer-Verlag. doi:10.1007/978-1-4471-4189-1_1

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597-611.

Pierce, W. C., & Sawyer, D. T. (2013). *Quantitative analysis*. London, UK: Wiley.

Powelson, S. E. (2012). *An examination of small businesses' propensity to adopt cloud-computing innovation* (dissertation). Retrieved from ProQuest Dissertations and Theses database. (Accession Order No. 3502302)

Prasad, M. R., Gyani, J., & Murti, P. R. K. (2012). Mobile cloud-computing: Implications and challenges. *Journal of Information Engineering and Applications*, *2*(7), 7-15. Retrieved from http://www.iiste.org/Journals/ index.php/JIEA

Punch, K. (2013). *Introduction to social research: Quantitative and qualitative approaches* (3rd ed.). London, UK: Sage.

Qi, C., & Chau, P. Y. K. (2013). Investigating the roles of interpersonal and interorganizational trust in IT outsourcing success. *Information Technology & People, 26*(2), 120-145. doi: 10.1108/ITP-09-2012-0088

Rabai, L. B. A., Jouini, M., Aissa, A. B., & Mili, A. (2013). A cybersecurity model in cloud-computing environments. *Journal of King Saud University—Computer and Information Sciences*, *25*(1), 63-75. doi: 10.1016/j.jksuci.2012.06.002

Rani, S., & Gangal, A. (2012). Security issues of banking adopting the application of cloud-computing. *International Journal of Information Technology*, *5*(2), 243-246. Retrieved from http://www.csjournals.com/IJITKM/PDF% 2052/3_ Sunita_Rani.pdf

Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide* (4th ed.). Hoboken, NJ: Wiley.

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, *16*(1), 69-73.doi: 10.1109/MIC.2012.14

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

Rogers, E. M. (1969). *Modernization among peasants: The impact of communication*. New York: Holt, Rinehart & Winston. doi: 10.1093/sf/49.2.342

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York, NY: Free Press.

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

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

Saarijärvi, H., Grönroos, C., & Kuusela, H. (2014). Reverse use of customer data: Implications for service-based business models. *Journal of Services Marketing*, *28*(7), 529-537. doi: 10.1108/jsm-05-2013-0111

Sardet, E., & Viale, E. (2012). A new era in banking—Cloud-computing changes the game. Accenture. Retrieved from accenture.com/cloudstrategy

Schenker, J. D., & Rumrill, J. D. (2004). Causal-comparative research designs. *Journal of Vocational Rehabilitation, 21*(3), 117-121. Retrieved from http://content.iospress.com/journals/journal-of-vocational-rehabilitation/46/2

Schoenherr, T., Ellram, L. M., & Tate, W. L. (2015). A note on the use of survey research firms to enable empirical data collection. *Journal of Business Logistics*, *36*(3), 288-300. doi: 10.1111/jbl.12092

Schwarcz, S. L. (2012). Regulating shadow banking. *Review of Banking and Financial Law, 31*(1), 619-642. doi: 10.2139/ssm.1993185

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011, July). *Cloud-computing security: Trends and research directions.* Paper presented at the *World Congress on Services (SERVICES).* doi: 10.1109/services.2011.20

Shue, L. (2013). Sarbanes-Oxley and IT outsourcing. Retrieved from http://www.isaca.org/Journal/Past-Issues/2004/Volume-5/Documents/jpdf045-Sarbanes-OxleSandITOutsou.pdf

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

Smedescu, D. (2013). Choosing the right cloud-computing solution for you. *Journal of Information Systems & Operations Management*, 1-7. Retrieved from ftp://ftp.repec.org/opt/ReDIF/RePEc/rau/jisomg/Wi13/JISOM-WI13-A26.pdf

Sobol, J. J. (2014). Cross-sectional research design. *The encyclopedia of criminology and criminal justice* (pp. 1-4). New York, NY: Springer. doi: 10.1002/97811185 17383. wbeccj017

Sommer, T., Nobile, T., & Rozanski, P. (2012). The conundrum of security in modern cloud-computing. *Communications of the IIMA, 12*(4), 15-40. Retrieved from htt://scholarworks.lib.csusb.edu/ciima/vol12/iss4/2

Son, I., & Lee, D. (2011, July). *Assessing a new IT service model, cloud-computing*. Paper presented at the Pacific Asia Conference on Information Systems (PACIS), Brisbane, Australia. http://aisel.aisnet.org/pacis2011/179

Streiner, D. L. (2016). Statistics commentary series: Commentary No. 17—Validity. *Journal of Clinical Psychopharmacology*, *36*(6), 542-544. doi: 10.1097/JCP .0000000000000589

SurveyMonkey (n.d.). SurveyMonkey audience. Palo Alto, CA: Author. Retrieved from www.surveymonkey.com/mp/audience

Tabachnick, B. C., & Fidell, L. S. (2013). *Using multivariate statistics* (6th edition). Boston, MA: Pearson.

Tajeddini, K., & Tajeddini, K. (2012). A synthesis of contemporary organisational innovativeness perspectives. *International Journal of Business Innovation and Research*, *6*(5), 532-555. doi: 10. l504/ijir.2012.048785

Talib, A. M., Atan, R., Abdullah, R., & Murad, M. A. A. (2012). Towards a comprehensive security framework of cloud data storage based on multi-agent

system architecture. *Journal of Information Security, 3*(4), 295-306. doi:10.4236/jis.2012.34036

Tang, Q, Mehrez, H., & Tal, M. (2014, May). *Performance comparison between multi-FPGA orototyping platforms: Hardwired off-the-shelf, cabling, and custom*. Paper presented at the 22nd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), Boston, MA. doi:10.1109/fccm. 2014.44

Thong, J., & Yap, C. (2011). CEO characteristics, organizational characteristics and information technology adoption in small business. *International Journal of Management Science*, *23*(4), 429-442. doi:10.1016/0305-0483(95)00017-I

Tornatzky, L., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington, MA: Lexington Books. doi: 10.1007/BF02371446

Tornatzky, L. G. & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*, (*29*), 28-45. doi: 10.1109/TEM.1982. 6447463

Tweel, A. (2012). *Examining the relationship between technological, organizational, and environmental factors and cloud-computing adoption* (dissertation). Retrieved from ProQuest Dissertations and Theses database. (Accession Order No. 3529668)

Valentine, L. (2013). Branches redefined. *ABA Banking Journal*, *105*(8), 22. Retrieved from https://www.questia.com/library/journal/1G1-34315 6129/branches-redefined

van Teijlingen, E., & Hundley, V. (2014). Pilot studies in family planning and reproductive health care. *Journal of Family Planning and Reproductive Health*

Care, *31*(3), 219-221. Retrieved from http://jfprhc.bmj.com/ content/31/3/ 219.short

Verizon Business. (2015). *2015 data breach investigation report*. Retrieved from https:// msisac.cisecurity.org/whitepaper/documents/1.pdf

Victor, J., & Mircea, G. (2014). Banking security characteristics in cloud-computing. *Ovidius University Annals, Economic Sciences Series*, *14*(1), 482-485. Retrieved from Researchgate.com

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97-102. doi: 10.1016/j.cose. 2013.04.004

Wang, L., Zhan, J., Shi, W., & Liang, Y. (2012). In cloud, can scientific communities benefit from the economies of scale? *Parallel and Distributed Systems, Transactions on IEEE 23*(2), 296-303. doi:10.1109/TPDS. 2011.144

Wenge, O., Lampe, U., Müller, A., & Schaarschmidt, R. (2014). *Data privacy in cloud-computing–An empirical study in the financial industry*. Paper presented at the Twentieth Americas Conference on Information Systems, Savannah, GA. Retrieved from https://pdfs.semanticscholar.org/7be0/0170ed4369cf039e4 fdef1323d2c48766273.pdf

Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud-computing. *Journal of Network and Computer Applications*, *40*, 325-344. doi: 10.1016/j.jnca.2013.08.004

Wisdom, J. P., Chor, K. H., Hoagwood, K. E., & Horwitz, S. M. (2014). Innovation adoption: A review of theories and constructs. *Administration and Policy in*

Mental Health and Mental Health Services Research, 41(4), 480-502. doi:10. 1007/s10488-013-0486-4

Wu, Y., Cegielski, C. G., Hazen, B. T., & Hall, D. J. (2013). Cloud-computing in support of supply chain information system infrastructure: Understanding when to go the cloud. *Journal of Supply Chain Management, 49*(3), 25-41. doi: 10.1111/j.1745-493x.2012.03287.x

Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud-computing. *Communications Surveys & Tutorials, IEEE*, *15*(2), 843-859. doi:10.1109/SURV.2012.060912. 00182

Xu, X. (2012). From cloud-computing to cloud manufacturing. *Robotics and Computer-integrated Manufacturing*, *28*(1), 75-86. doi: 10.1016/j.rcim. 2011.07.002

Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., & Yang, L. T. (2013, June). *CloudThings: A common architecture for integrating the Internet of Things with Cloud-computing*. Paper presented at the 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Whittier, BC, Canada. doi: 10.1109/CSCWD.2013.6581037

Zimmerman, D. (2014). Five cloud essentials for the boardroom: What banking and financial markets executives need to know about cloud-computing. *Journal of Payments Strategy & Systems*, *8*(1), 84-93. Retrieved from http://www.henry stewartpublications.com/jpss

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

Appendix A: Cloud Security Survey Instrument Tables

Table 13

Frequency and Percent Statistics of the U.S. Region in which Participants' Organizations Headquarters are Located

U.S. Region	Frequency (*n*)	%
New England	3	2.5
Middle Atlantic	19	16.1
East North Central	12	10.2
West North Central	6	5.1
South Atlantic	15	12.7
East South Central	15	12.7
West South Central	18	15.3
Mountain	8	6.8
Pacific	22	18.6
Total	118	100.0

Note. $N = 112$.

Table 14

Frequency and Percent Statistics of the State in which Participants' Organizations' Headquarters are Located

State	Frequency (*n*)	%
Alabama	1	0.8
Alaska	1	0.8
Arizona	2	1.7
Arkansas	1	0.8
California	10	8.5
Colorado	4	3.4
Connecticut	3	2.5
District of Columbia (DC)	1	0.8
Florida	3	2.5
Georgia	2	1.7
Idaho	1	0.8
Illinois	5	4.2
Indiana	1	0.8
Kansas	1	0.8
Kentucky	1	0.8
Louisiana	3	2.5
Maine	1	0.8
Maryland	1	0.8
Massachusetts	3	2.5
Michigan	4	3.4
Minnesota	4	3.4

Mississippi	1	0.8
Missouri	3	2.5
Nevada	1	0.8
New Jersey	6	5.1
New Mexico	1	0.8
New York	12	10.2
North Carolina	7	5.9
Ohio	3	2.5
Oklahoma	2	1.7
Oregon	2	1.7
Pennsylvania	2	1.7
Rhode Island	1	0.8
Tennessee	2	1.7
Texas	10	8.5
Vermont	1	0.8
Virginia	3	2.5
Washington	6	5.1
West Virginia	1	0.8
Wisconsin	1	0.8
Total	118	100.0

Appendix **B**: Cloud Security Survey Instrument

Intent to adopt cloud technology

General Participant Survey Questions

Instructions:
Please read the following questions carefully and click on the answer(s) that best represents you or fits your organizational profile. For where you might need to provide ***other*** information, simply click in the large text area below the question and type in your answer. Some questions may require that you decide on between multiple options. For example, you may need to decide on your level of agreement with a statement. Please select the option that best represents your level of agreement. Each decision presents its own challenges, and we all have different ways of viewing them.

Organizational Factor(Demographics)

1. For the purpose of this survey, the participant is expected to have IT knowledge, familiar with cloud computing concepts and play a critical role in influencing technology adoption decisions in the financial services sector. Please indicate whether you meet this profile

◯ Yes ◯ No

2. What is your job role?

◯ IT Analyst/Engineer
◯ IT/IS Manager
◯ IT/ Solution Architect
◯ ISO/CISO/CSO/C-Level
◯ Other (please specify)

3. Which of the following best represents your organization's primary category in the financial services? (primary category is defined as the economic services that account for your organization's principal activities)

◯ Commercial Banks
◯ Stock Brokerages
◯ All of the Above
◯ Investment Funds
◯ Credit Unions/Savings/Loans
◯ Insurance Company
◯ Mortgage services
◯ Other (please specify)

4. In what state or U.S. territory is your organization currently headquartered?

5. What is your institution annual revenue?

WALDEN UNIVERSITY
A higher degree. A higher purpose.

Intent to adopt cloud technology

Technological Factor: Benefits and Risks

The following questions are related to the benefits and risk implications of cloud technology

6. Relative Advantage:

Technology can be used for a number of objectives. To what extent is cloud computing adoption important for the fulfillment of the following objectives in your organization ?

	Strongly Disagree 1	2	3	Neutral 4	5	6	Strongly agree 7
Allows us to optimize our branch network.	○	○	○	○	○	○	○
Allows us to gain deep understanding of our customer needs.	○	○	○	○	○	○	○
Allows us to target customers with specific product offerings.	○	○	○	○	○	○	○
Provides smart interactions with our customers.	○	○	○	○	○	○	○
Empowers our frontline and mobile sales workforce.	○	○	○	○	○	○	○
Allows us to enhance our digital ecosystem.	○	○	○	○	○	○	○
Requires no upfront capital investment.	○	○	○	○	○	○	○
Increases the profitability of our organization	○	○	○	○	○	○	○
Reduces our operational costs	○	○	○	○	○	○	○
Costs savings from cloud computing allows us to offer price-competitive products and services.	○	○	○	○	○	○	○

7. Compliance Risks

Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from strongly disagree to strongly agree.

	Strongly disagree 1.	2.	3.	Neutral 4.	5.	6.	Strongly agree 7.
It is difficult to ensure compliance with industry /regulatory standards.	○	○	○	○	○	○	○
It is difficult to ensure data privacy in the cloud.	○	○	○	○	○	○	○
Government can gain access to business data in the cloud	○	○	○	○	○	○	○
It is difficult to meet data production and reporting requests by auditors/regulators.	○	○	○	○	○	○	○
It is difficult to ensure clarity with responsibility and liability attribution in the cloud	○	○	○	○	○	○	○
Storing data in different geographical locations presents regulatory challenges(Safe harbor)	○	○	○	○	○	○	○

8. Security Risks

Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from strongly disagree to strongly agree.

	Strongly disagree 1.	2.	3.	Neutral 4.	5.	6.	Strongly agree 7.
Malicious Insiders may gain unauthorized access to business data in the cloud	○	○	○	○	○	○	○
Shared and multi-tenancy nature of cloud computing creates a fertile ground for data loss or leakage	○	○	○	○	○	○	○
Business data in the cloud can be subject to abuse and nefarious use	○	○	○	○	○	○	○
Business data in the cloud can be subject to Man-in-the-middle attacks	○	○	○	○	○	○	○
Business data or information stored in the cloud can be subject to message alteration	○	○	○	○	○	○	○
Business data in the cloud can be subject to Message replay attacks	○	○	○	○	○	○	○
Confidential customer data or information stored in the cloud services can be subject to Identity Spoofing	○	○	○	○	○	○	○
Confidential customer information or business data in the cloud can be subject to denial of service attack	○	○	○	○	○	○	○

9. Compatibility as a measure of perceived risk:

Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from strongly disagree to strongly agree.

	Strongly disagree 1.	2.	3.	Neutral 4.	5.	6.	Strongly agree 7.
Cloud adoption is not consistent with our organizational belief and value.	○	○	○	○	○	○	○
Attitudes towards cloud adoption in our organization is unfavorable.	○	○	○	○	○	○	○
Cloud adoption is not compatible with our organization's IT infrastructure.	○	○	○	○	○	○	○
Use of cloud technology is not consistent with our organization's business strategy.	○	○	○	○	○	○	○
Cloud service is cumbersome to use.	○	○	○	○	○	○	○
Using cloud services requires a lot of mental efforts.	○	○	○	○	○	○	○
The user interface of cloud services is difficult and not user-friendly.	○	○	○	○	○	○	○
Cloud services are difficult to purchase and setup.	○	○	○	○	○	○	○

10. Complexity:

Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from strongly disagree to strongly agree.

	Strongly disagree 1.	2.	3.	Neutral 4.	5.	6.	Strongly agree 7.
It is difficult to integrate legacy financial systems with the cloud.	○	○	○	○	○	○	○
There is a potential vendor lock-in to a cloud service provider due to proprietary.	○	○	○	○	○	○	○
It is difficult to audit technology services in the cloud environment.	○	○	○	○	○	○	○
It is difficult to receive security logs in real time.	○	○	○	○	○	○	○
It is difficult to conduct digital forensics and e-discovery in the cloud environment.	○	○	○	○	○	○	○
Cloud solutions do not have good incident reporting mechanisms.	○	○	○	○	○	○	○
There is a lack of control and accountability over business data in the cloud.	○	○	○	○	○	○	○
It is difficult to classify data in the cloud.	○	○	○	○	○	○	○

Prev Next

WALDEN UNIVERSITY
A higher degree. A higher purpose.

Intent to adopt cloud technology

Current and Future Adoption Plans

11. Please indicate how much you agree or disagree with each of the following statements based on a scale ranging from Strongly disagree to strongly agree.

	Strongly Disagree 1.	2.	3.	Neutral 4.	5.	6.	Strongly disagree 7.
My organization intends to adopt cloud computing	○	○	○	○	○	○	○
It is likely that my organization will take steps to adopt cloud computing in the future	○	○	○	○	○	○	○
It is likely that my organization will take steps to adopt cloud computing for our core processes within the next 12+ months	○	○	○	○	○	○	○

Prev Done

Appendix C: Rogers Copyright Permission

SIMON & SCHUSTER

Christine J. Lee
Permissions Supervisor

1230 Ave of the Americas, 14th Fl
New York, NY 10020
Christine.Lee@simonandschuster.com

VIA EMAIL

January 4, 2017

Olatunji Mujib Arowolo
Walden University Ph.D Student
olatunji.arowolo@waldenu.edu

Dear Olatunji Mujib Arowolo:

You have our permission to include Figure 7-3: "Adopter Categorization on the Basis of Innovativeness" from p. 281 of our book, DIFFUSION OF INNOVATIONS, 5E by Everett M. Rogers, in your doctoral dissertation entitled "Strategic Cyber Risk Implications of Cloud Technology in the Financial Services Sector."

The following acknowledgment is to be reprinted in all copies of your dissertation:

From DIFFUSION OF INNOVATIONS, 5E by Everett M. Rogers. Copyright © 1995, 2003 by Everett M. Rogers. Copyright © 1962, 1971, 1983, by Free Press, a Division of Simon & Schuster, Inc. Reprinted with the permission of Free Press, a Division of Simon & Schuster, Inc. All rights reserved.

This permission applies to all copies of your dissertation made to meet the degree requirements at Walden University. You must re-apply to this department if you wish to include our material in your dissertation for any other purpose. We may require a permission fee at that time.

Sincerely,

Christine J. Lee

Christine J. Lee

AGREED TO AND ACCEPTED

Olatunji Mujib Arowolo