2015

Identifying Key Determinants of Service Provider Effectiveness and the Impact it has on Outsourced Security Success

James B. Lewis
Nova Southeastern University, JLew15@hotmail.com

Identifying Key Determinants of Service Provider Effectiveness and the Impact it has on Outsourced Security Success

by

James B. Lewis

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2015

We hereby certify that this dissertation, submitted by James Lewis, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Gurvirender P. Tejay, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Ling Wang, Ph.D. Date
Dissertation Committee Member

_____ _____

Laurie P. Dringus, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Amon B. Seagull, Ph.D. Date
Interim Dean, College of Engineering and Computing

College of Engineering and Computing
Nova Southeastern University

2015

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Identifying Key Determinants of Service Provider Effectiveness and the Impact it has on Outsourced Security Success

by
James B. Lewis
November 2015

The purpose of this research was to identify key determinants of service provider effectiveness and how it impacts outsourced security success. As environments have become more robust and dynamic, many organizations have made the decision to leverage external security expertise and have outsourced many of their information technology security functions to Managed Security Service Providers (MSSPs).

Information Systems Outsourcing, at its core, is when a customer chooses to outsource certain information technology functions or services to a service provider and engages in a legally binding agreement. While legal contracts govern many aspects of an outsourcing arrangement, it cannot serve as the sole source of determining the outcome of a project. Organizations are viewing outsourcing success as an attainment of net benefits achieved through the use of a service provider. The effectiveness of the service provider has an impact on a company's ability to meet business objectives and adhere to service level agreements. Many empirical studies have focused on outsourcing success, but few have focused on service provider effectiveness, which can serve as a catalyst to outsourcing success.

For this research, Agency Theory (AT) was proposed as a foundation for developing the research model, which included key areas of focus in information asymmetry, the outsourcing contract, moral hazard, trust, service provider effectiveness, and security outsourcing success. Agency Theory helped uncover several hypotheses deemed germane to service provider effectiveness and provided insight into helping understand the principal-agent paradigm that exists with security outsourcing. Confirmatory Factor Analysis (CFA) and Partial Least Squares-Structured Equation Modeling (PLS-SEM) were used with SmartPLS to analyze the data and provided clarity and validation for the research model and helped uncover key determinants of service provider effectiveness.

The statistical results showed support for information asymmetry, contract, and trust, all of which were mediated through service provider effectiveness. The results also showed that service provider effectiveness is directly correlated to increasing security outsourcing success. This concluded that the research model showed significant results to support 4 of the 5 hypotheses proposed and helped uncover key findings on how security outsourcing success can be impacted. This research served as an original contribution to information security while viewing outsourcing success from the perspective of the client, security services, and customer expectations.

Acknowledgements

The dissertation journey is one that can push you to the brink of insanity. For the select few that have completed this voyage before me, I am humbled to be in such great company and thankful to be a part of something so enlightening and special. It was truly worth it.

First and foremost, I want to thank God for giving me the stamina to endure, the patience to listen, the strength to stay focused, and the discipline to keep pushing forward. Without him, none of this would have been possible.

I wish to express my appreciation to my Dissertation Advisor Dr. Gurvirender Tejay for keeping me on the narrow path and never giving up on me. I appreciate the countless hours, nights and weekends that he spent with me and other students working with each of us in an open forum to help foster open dialogue and accept feedback from one another. This approach was invaluable and the key to my success because it helped remove the unspoken taboo of only discussing idea papers and proposals behind closed doors. I look forward to his continued mentorship as I transition into a future professor and researcher.

I also would like to thank my committee members Dr. Ling Wang and Dr. Laurie Dringus for their patience and valuable feedback that I received throughout each stage of the dissertation process. Their efforts improved the quality of my work and I am sincerely grateful for having such a dedicated committee to help me succeed.

I am extremely thankful to my family and friends for their constant support and motivation. Special appreciation goes to Dr. Gerald Johnson for his unwavering assistance, friendship, and advice for not just my dissertation, but lessons in life as well.

Finally, I wish to dedicate this dissertation to my mother Patricia Bell and my late father, James B. Lewis, Sr. I love you both. Mama, you are my biggest fan and the brightest star in my life. Doddy, I know if you were here, you would be proud.

Table of Contents

Abstract iii
List of Tables iv
List of Figures v

Chapters

1. Introduction 1
Overview 1
Outsourcing IT Security 3
Problem Statement 5
Research Argument 6
Definition of Terms 9
Summary 10

2. Literature Review 11
Introduction 11
Information Systems Overview 11
Outsourcing Overview 16
Decision to Outsource 19
Outsourcing Management 23
Service Providers 29
Outsourcing Success 31
Literature Gaps 32
Summary 33

3. Research Methodology 35
Introduction 35
Theoretical Basis 35
Research Method 44
Data Collection 47
Data Analysis 50
Summary 59

4. Measurement Model Analysis and Findings 61
Introduction 61
Preliminary Screening 61
Demographics Information 62
Confirmatory Factor Analysis Results 66
Summary 71

5. Structural Model Analysis and Findings 73
Introduction 73
Structural Model 73
PLS-SEM findings 74

Alternative Model 77
Summary 78

6. Discussion and Conclusion 79
Introduction 79
Findings 79
Contribution to Research 81
Limitations 83
Future Research 85
Conclusion 87

Appendices 88
A. Survey Questions for Research Instrument 89
B. Institutional Review Board (IRB) Approval Letter 90
C. Sample E-mail request to participate in Internet Survey 91

References 92

List of Tables

Tables

1. Research Constructs and their Indicators 43

2. CFA Analysis Criteria for the Measurement Model 55

3. PLS-SEM Analysis Criteria for the Structural Model 59

4. Gender Distribution 63

5. Age Group 63

6. Education Level 64

7. Organizational Role 64

8. Work Industry Distribution 65

9. Size of the Organization 65

10. Previous Security Service Providers 66

11. Factor Loadings for Initial Instrument 67

12. Findings of Internal Consistency Reliability 68

13. Findings of Convergent Validity 69

14. Findings of Indicator Reliability 69

15. Findings for Discriminant Validity 71

16. Findings of the Collinearity Assessment 74

17. Bootstrapping results on the Path Coefficient 75

18. Results of the f^2 effect sizes 76

19. Findings of the Proposed Hypotheses 78

List of Figures

Figures

1. CIA Triad 13

2. Components of the Agency Theory Model 36

3. Research model for Information Security Outsourcing Success 37

4. Instrument Development Model 45

5. List of Analysis Techniques 51

6. Research constructs and their indicators 72

Chapter 1

Introduction

1.1 Overview

Organizations continue to rely on their Information Technology (IT) departments to provide support for their daily business functions and technical requirements. As the complexity of technology increases, the demand for services from IT functions is increasing along with exceeding expectations (Upadrista, 2014). Because of this complexity, IT environments have become challenging to manage (Kumbakara, 2008) and leading to higher work constraints for the internal staff. With the growth in application requirements and access to system resources, executives must find an effective way to maintain IT services and keep the organization focused on core competencies.

Many firms are now looking to external service providers to outsource common tasks because of their strong technical expertise and access to global talent (Nevo & Kotlarsky, 2014). Because of this new access to skilled personnel for IT outsourcing, organizations are looking to outsource more than ever before (Oladapo, Zavarasky, Ruhl, Lindskog & Igonor, 2009; Schneier, 2002). Smith, Mitra, and Narasimhan (1998) define outsourcing as "…the use of external agencies to process, manage, or maintain internal data and to provide information-related services" (p. 61). Outsourcing has become increasingly common because this allows organizations to offload the non-core processes and tasks to service providers and keep the focus on core business (Upadrista, 2014). Outsourcing IT services continues to grow in popularity (Gorla & Lau, 2010) and has transitioned to a

worldwide phenomenon (Bahli & Rivard, 2003; Gonzales, Gasco, & Llopis, 2005; Sloper, 2004).

Despite its popularity, many firms have failed to embrace outsourcing because of skepticism, legal contracts, and project issues with certain outsourcing arrangements. Clients as well as vendors have admitted to having a number of issues with outsourcing that ultimately led to unsatisfactory results (Pannirselvam & Madupalli, 2011). Past outsourcing ventures that have failed in certain organizations have caused other firms to be hesitant in their own IT outsourcing considerations.

A decision to outsource IT services should take into account all business and technical factors to ensure the highest level of success. Outsourcing itself is neither good nor bad (Aubert, Patry, & Rivard, 2005; Cullen & Willcocks, 2003), but "…there are only good and bad outsourcing decisions, as there are good and bad outsourcing arrangements (Aubert. Patry, & Rivard, 2005, p. 189)." Customers should have a clearly defined scope of what IT services they need and determine if the outsourcing of such services will provide value and a benefit to their organization.

Since organizations may lack expertise in certain areas, they are looking to form alliances with other firms to address and meet their needs (Raiborn, Butler, & Massoud, 2009). Whatever the reason, organizations are looking to help fill a void by leveraging outsourced IT services with companies that now offer a larger selection of IT functions (McFarlan & Nolan, 1995) today than in recent past. A good example of how IT outsourcing is being leveraged today is through the use of cloud computing services. Cloud computing is a service that provides users access to their controlled data over a network connection [usually the Internet] (Clarke, 2010). Organizations may choose to

outsource all or a portion of their IT services in the cloud to manage applications, databases, and servers on a virtualized infrastructure. IT costs are minimized when offloading data and resources to cloud computing services (Santos, Gummadi, & Rodrigues, 2009) because customers minimize the need for staff since an external provider manages the datacenter and manages the support.

In the early stages of outsourcing, success may have been defined through just cost saving, but today this is no longer the case as there are many other factors to consider. Aside from just reducing costs, a key objective of a successful outsourcing arrangement is that both client and service provider are satisfied. (Gonzalez et al., 2005) determined that the number one success factor of IS outsourcing was the understanding of client objectives. However, Webb (2005) believes that success in outsourcing depends significantly on the client/vendor relationship. There can be many factors that lead to a successful outsourcing arrangement, but open communication and discussions between both parties' increases the chance of expected outcomes. Outsourcing can be a great benefit to clients as long as their data is always available and has the highest level of information security. Having clearly defined roles and responsibilities to address information security issues in an outsourcing arrangement is critical.

1.2 Outsourcing IT Security

While many organizations have outsourced IT services, there is still a great concern over how information security is being managed internally. The challenges involving users and information security protection are affected by the quality of service that is delivered to the user community. As the protection of information increases and information security monitoring is being put in place, the demand is much greater to

transition security tasks to Managed Security Service Providers (Lee, Geng, & Raghunathan, 2013; Zhang, Borisov, Yurcik, Slagell, & Smith, 2006). Many firms are transitioning to external service providers to provide a range of security services to help them reduce costs and leverage skilled security expertise (Allen, Gabbard, & May, 2003).

Given that organizations continue to have challenges with managing security resources themselves, information security outsourcing has become an emerging phenomenon (Gupta & Zhdanov, 2012) as well. There are many facets of security that a provider can offer in IT security services such as security awareness and training, access control, intrusion detection and firewall management (Oladapo et al., 2009). As the demand for new security technology emerges, so does the offering of managed security services (Ding, Yurcik, & Yin, 2005). As customers separate core competency and commodity functions, the need for appropriate security services is paramount. With outsourcing security services, security objectives must be identified, understood, and implemented properly. Outsourcing security services can bring about many benefits such as cost advantages and a richer experience due to security expertise of the service provider (Ding et al., 2005). Karyda, Mitrou, and Quirchmayr (2006) concluded that organizations considering outsourced security services should factor in technical, organizational, and legal issues in their decision. This would help identify methods for security enforcement, identifying the appropriate security objectives, and help with security compliance. Notwithstanding these security decisions, it is critical to understand who will manage all aspects of the security spectrum.

Information security management has become a challenging business function due to security breaches and the complexity of IT environments (Cezar, Cavusoglu, &

Raghunathan, 2014). Customers see the need to outsource security, but without sacrificing control of their data. Given the perceived amount of control given up by the client to the vendor for security services, the successful management of the security service is greatly enhanced or reduced based on the expectations the client has towards the vendor.

With security now at the forefront of all services related to technology, clients need to know how their information will be protected and secured from breaches and attacks. It is the belief that effective, efficient, and innovative information security is needed to reduce overall risk (Silic & Back, 2014). Moreover, there should be specified responsibilities assigned to the vendor as well as the customer to effectively promote and enable the proper implementation of information security services. Value is created between clients and vendors when an effort is made to build and sustain a flexible relationship (Lee, Huynh, & Hirschheim, 2008). Some formal aspects of outsourcing are centered solely on the written contract while other informal areas, such as the relationship, help foster security management success. This study addresses the role of the security provider and how outsourced security services are managed successfully.

1.3 Problem Statement

While outsourcing IT security can provide benefits to customers, little focus has been given in literature on a service provider's ability to properly provide outsourced IT security services to their customers. The problem promoting this research is that key determinants of an effective service provider conducting outsourced IT security services successfully have not been identified and validated. Dean and Kiu (2002) states that "Inconsistent findings with respect to effectiveness outcomes, such as quality, highlight

the challenges associated with managing a service, but not the provider of that service (p. 397).” From this perspective, there are many inconsistencies and misunderstanding about service provider effectiveness and its impact on outsourcing arrangements and little understanding of the context of effectiveness and how it is used with security. According to Hamilton and Chervany (1981), effectiveness is determined by comparing performance to objectives and then developing criterion measures to assess how well those objectives are being achieved. For the purpose of this study, we will adopt this definition of effectiveness. Despite the fact that many organizations are hesitant about providing hard data about their security ineffectiveness (Knapp, Marshall, Rainer & Ford, 2007), the success of outsourcing is directly related to effectiveness (Dean & Kiu, 2002). Management needs to understand the benefits of IS security, know what security measures are effective and under what conditions. The research problem of this study should help identify key determinants of service provider effectiveness and the impact it has on security outsourcing success. The focus of this research study is on effectiveness from the viewpoint of the customer towards the service provider.

The argument for this research is that organizations need to acknowledge the symbiotic relationship between clients and service providers to protect the benefits for both parties (Qi & Chau, 2012) and ensure secure IT services. Little is known about how the nature of symbiotic relationships and how it affects outsourcing (Chou & Huang, 2011). Service providers managing security services must ensure that security to customers is provided properly or accept the consequences if things go wrong (Subashini & Kavitha, 2011). In addition to the work performed, service providers and customer must have a symbiotic ecosystem in place to increase the effectiveness and success of

outsourcing. Key determinants must be uncovered to establish segmentation between effective and ineffective security service providers. Outsourcing arrangements, particularly security, are beneficial when both parties have mutualistic interests and clearly defined responsibilities.

In many organizations, it might be difficult to establish the boundaries of what is considered effective security management. Wheeler (2008) posited that the effectiveness of security (protection) is reduced to a simple decision of: yes, security is effective or no, it is ineffective. As transition take place in organizations, it is becoming difficult to determine what functionalities are considered core competencies and commodity functions. These decisions have a significant impact on the outsourcing arrangement itself. There is a distinct separation between making IT outsourcing decisions and outsourced security services decisions. IT outsourcing decisions were generally based around savings and lowering costs (Aubert, Patry, &Rivard, 2005; Khidzir, Mohamed, & Arshad, 2010) which would then allow the in-house staff to focus their efforts on valuable work (Lacity & Willcocks, 1998) and remain focused on their own internal strategies (Hsu, Wu, & Peng, 2005).

The decision to outsource security services cannot be viewed in the same context as traditional IT outsourcing. Karyda, Mitrou, and Quirchmayr (2006) stated that security outsourcing should be reviewed under a different scope than traditional IS/IT outsourcing. No longer can a decision on outsourcing, especially security, look at just cost. The path of outsourcing has transitioned away from cost savings alone and takes into account a multitude of factors that promote its value and effectiveness. Aspects of security outsourcing involve complex decision making to ensure that environments are

protected. The objective of this research is to identify key determinants of service provider effectiveness and understand the impact they have on outsourced security.

In many instances, the outsourcing of security services has proven quite challenging to manage (Kern & Willcocks, 2000) which ultimately affects vendor-client relationships and the ability to achieve outsourcing goals (Kerns & Willcocks, 2002). Additionally, other challenges include the security culture or lack of security culture in organizations (Tsohou, Theoharidou, Kokolakis, & Gritzalis, 2007; Werlinger, Hawkey, & Beznosov, 2008), managing risks (Karyda, Mitrou, & Quirchmayr, 2006; Schneier, 2002; Zhao, Xue, & Whinston, 2009), and moral hazard (Ding, Yurcik, & Yin, 2005a). Unlike traditional IT outsourcing, which has many providers offering a variety of services to select from, security is specialized and fewer providers are available. Problems have risen with security with not only selecting the appropriate provider (Allen, Gabbard, & May, 2003), but also ensuring they possess the appropriate security expertise exists to do the job. Because of evolving technology, providers are having trouble managing new security tools that are needed to perform their security responsibilities for their clients (Debar & Viinikka, 2006). IT providers may state that security measures exist, but they fail to provide the client with a method of validating the existence of security (Demchenko, De Laat, and Lopez, 2010). It is imperative that security measures and countermeasures are discussed with the customer to give them assurance that their personal data is protected. The intent is to reduce risk for both organizations, but it is still unknown as to how the client and the service provider are managing their own individual risks while the security services are being performed.

1.4 Definition of Terms

Listed are some defined terms that are important within the research study and help provide a better understanding of the terms and the context of how those terms are used within the research study. ***Information security*** is protecting information and the systems that are processing it (Siponen & Oinas-Kukkonen, 2007). Information security is focused on how the system is providing security and how the information itself is being protected. Roses, Hoppen, Ballaz and Freire (2006) stated "***Information Systems (IS) outsourcing*** consists of transferring part of internal information technology (IT) activities from a contracting organization (client) to a contractor (seller, provider, and supplier) through a contract" (p. 268). ***Information Systems*** deliver information and communication services while providing functions that plan, develop, operate and manage the information systems in the organization (Davis, 2006). Information systems help combine many information technology components together for proper management and operations by users. ***Information Technology (IT) Services*** support business processes that are produced through the operation of application systems and delivered to users (Zarnekow, Brenner, & Pilgram, 2006). IT services are provided as a service to assist with the technology solutions within an organization. Service providers play a critical role in the success deployment of security and IT services. ***Managed Security Service Providers (MSSPs)*** provides security services such as security monitoring, vulnerability and penetration testing, firewall services, anti-virus, and information security risk assessments (Ding & Yurcik, 2005b). The core focus of an MSSP is on security and possible ancillary systems needed for security support. ***Managed Service Providers (MSPs)*** are responsible for network management and information systems

management services to various IT departments and end-users of their clients (Kumbakara, 2008). MSPs are commonly brought in to support specific areas of the business except security.

1.5 Summary

This chapter provided an overview of information systems, the research problem and argument of security outsourcing and service providers along with key definitions for the research study. Given the amount of research dedicated to outsourcing, there are limited studies on the expansion of information security outsourcing and outsourcing success. There is still a need to understand security specific success from both the contract and the expectations of the client. Having a better understanding of service providers and their overall effectiveness in managing security is limited in research and should be addressed. This research study was designed to understand what key determinants make a service provider effective and how this impacts overall outsourcing success.

Chapter 2

Literature Review

2.1 Introduction

For this literature review, the researcher will provide an overview of empirical studies that provides a background to the research topic and support for the problem statement identified in Chapter 1. Additional information will be provided on information systems, outsourcing, security outsourcing, managed security service providers, outsourcing success and literature gaps.

2.2 Information Systems Overview

Information assets have become a critical component to a company's competitive edge and business strategy. According to Singh, Gupta, and Ojha (2014), this increase in the dependency of information and assets has created an immediate need for information security. Information has begun to play a major role in not only supporting business operations, but in the demand for convenient access to that information (Posthumus & Von Solms, 2004). With data becoming so important to protect, it is just as critical to protect the systems that house this information. Organizations have begun to rely heavily on the operations of their information systems (Knapp, Morris, Marshall, & Byrd, 2009) and protecting these systems require the establishment of an acceptable level of information security management within the organization while implementing adequate security controls (Da Veiga & Eloff, 2010).

Given the evolution of information systems over time, concerns have been raised at the organizational and department level over the protection of data. At the

organizational level, the protection of information and resources is a mandate that must be enforced by every entity – whether enterprise or government (Pranata, Skinner, & Athauda, 2012). At the department level, Gavin (1994) posited that information systems managers are tasked with aligning information technology with the business and sustaining a competitive advantage with stricter budgets. Many organizations looked at information systems as a tactical function, but in the 1980s, executives began to look at information systems as a strategic role and the thought of what it could provide to their organization (Lacity & Hirschheim, 1993).

Information Security

Because of the use and value of information, information system security concerns continue to pose a challenge for executive management and professionals (Dhillon & Torkzadeh, 2006) and must be addressed at all levels of the organization. According to Posthumus and von Solms (2004), information security helps to mitigate the risk to information through the deployment of security controls.

Protecting data is important for organizations, as users may potentially need access to information safely and securely from anywhere in the world. Specific measures must be taken to protect this information from internal and external threats to the organizations. The basic concept of protecting data is linked to information security principles that are based on ensuring confidentiality, integrity, and the availability of data (Guttman & Roback, 1995; Von Solms, 2001). This is commonly known as the C.I.A triad.

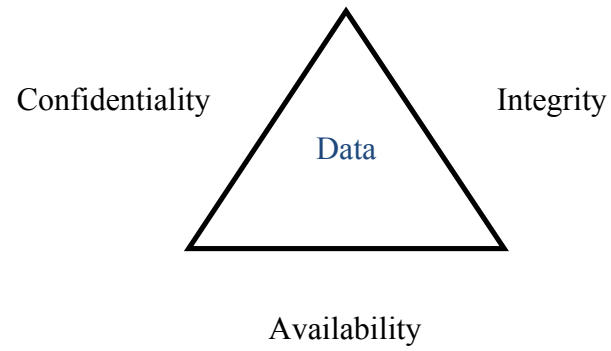

Figure 1. The elements of the C.I.A Triad

Confidentiality refers to limiting access to only specific individuals who are authorized (Dhillon & Backhouse, 2000; Shultz, Proctor, Lien, & Salvendy, 2001). Confidentiality has the initial control of limiting access and keeping data private and then authorizing only specific users to access this information. If a user does not have authorization to certain information, they should not be made aware of its existence. In some instances, confidentiality received greater attention considering many of the plans for authorization and access control were sponsored by the military (Ma, Johnston, & Pearson, 2008).

Integrity refers to information remaining consistent and that the original content or source has not been modified (Lee, Pipino, Strong, & Wang, 2004). Proper integrity is being able to validate that the source file has not been relocated or altered from its original state. Organizations base important decisions on the notion that data provided to them is complete. Information that is incomplete or inaccurate can cause executive management to make poor decisions that are detrimental to their organization (Posthumus & von Solms, 2004).

Availability is ensuring that information is readily available and accessible to authorized personnel (Chang &Wang, 2011; Dhillon & Backhouse, 2000). Without

availability, organizations cannot continue their day-to-day operations and function efficiently. The CIA triad has proven to be a critical foundation of information security and continue to be used in many organizations today along with other security principles.

When addressing information security issues, many organizations have looked to implement information security policies in their organization as an initial step. Information security policies state specific objectives and goals that organizations would like to accomplish or adhere to for information security. Information security policies are a key foundation of influencing organizations to govern security policies (Volonino, 2004), it has become a mandate than an option for public and private sector firms. Information organizational security programs (Knapp, Morris, Marshall, & Byrd, 2009) and security policies serve as the basis on how organizations measure their progress toward reaching security objectives.

Information security standards help organizations document security objectives and how those objectives will be achieved. For proper protection of information assets from internal and external attacks, different security standards and guidelines have been developed for protection (Ma, Johnston, & Pearson, 2008). Because of the diversity of business operations, many organizations may be required to adhere to information security standards that are applicable to the entire organization and to specific departments, depending on their role in the organization. Many of these departments will have established practices and procedures in place to help with meeting the information security standards that have been set by the organization.

Information Security Management

Information security has gone through several phases including a keen focus on the technical aspect (von Solms, 1996) of security management. Information security has transitioned from being historically a technical issue to now a management issue (von Solms, 2001). The management of information security is related to power and is usually a much deeper political issue than originally recognized (Anderson, 2001). There are a significant number of studies on IS security which has helped increase its importance and topic interest for academic literature (Ransbotham & Mitra, 2009) One key area is IS security management (ISM) and risk commonly discussed in this area. NIST (2011) defines the components of risks management for information security as frame, assess, respond, and monitor. With information security threats on the rise, organizations are running into challenges in areas of governance and information security management (ISM). Regardless of the size of organization, there are always challenges involved with the proper management of IS security in this digital era. With increases in data storage and network usage, ISM has begun to play a bigger in organizations (Yildirim, Akalp, Aytac, & Bayram, 2011) and firms have to come up with new ways to manage their data.

Organizations recognize security as an important issue and their members need to be aware of the security measures that exist (Kim, Kim, & French, 2013). Because information has been recognized as a critical corporate asset, information security has to be a component in planning and management (Chang & Ho, 2006). IS security management becomes extremely important when it comes to the proper protection and accessible of information assets. According to Von Solms (1996), Information Security Management (ISM) is used to enhance confidence and the effectiveness of information

services within an organization or with external partners. Chang and Ho (2006) conducted a study in Taiwan to examine the influence of organizational factors on effectiveness of implementing an ISM standard [BS7799]. They concluded that organizational factors were impacted by IT competence of managers, environmental uncertainty, industry type and organizational size.

Information security has evolved over the last few decades and has an impact on most information technology environments when looking to protect data. Because of organizational changes and the dependencies that exist on technology, IS security must be implemented properly and effectively to minimize threats and help reduce costs. When addressing security management, outsourcing is considered one of the most cost effective ways to do it (Bakari, Magnusson, Tarimo, & Yngstrom, 2006).

2.3 Outsourcing Overview

As mentioned in Chapter 1, Outsourcing is defined as transferring internal functions of the IS department for an external party to manage (Ketler & Willems, 1999). To expand on this definition of outsourcing, Hirschheim and Lacity (1997) defined outsourcing as "...the third party management of IS assets, people, and/or activities required to meet pre-specified performance levels" (p.1). During the early stages of outsourcing, external partners were typically brought in for specific functions and tasks. In the early stages of Information Systems (IS) outsourcing, it would usually involve the use of an external provider offering a single function of service to their customers (Dibbern, Goles, Hirschheim, & Jayatilaka, 2004), which was sometimes referred to as selective sourcing (Hirschheim & Lacity, 1997). Now as outsourcing has continued to

increase in demand, so has the diversity of the IT functions required from the external vendors.

Throughout literature, the outsourcing of IT services has been viewed in many different perspectives. Dibbern et al. (2004) acknowledged, "Information Technology (IT) has become the engine that drives the modern organization" (p. 6). IT has a direct effect on how services are managed today. Information technology outsourcing (referred to as ITO) has been around for almost 60 years. Outsourcing evolved over each decade and business reason to outsource began to change as the needs of the business changed.

The Outsourcing Era

From the 1950s till now, outsourcing has played a key role in addressing many organizations' IS problems. Yang (2000) noted that one of the first information systems outsourcing arrangements started back in 1954 when General Electric Corp outsourced to Arthur Anderson and Univac (as cited by Klepper & Jones, 1998) to address payroll processing and manufacturing. This installation of a Univac computer and printer served as one of the first successful projects to automate payroll processing. Kelter and Walstrom (1993) believed that different eras required different methods of outsourcing to address different problems within IS. Their research uncovered hardware challenges in the 1960s, expense of software development in the 1970s, lack of IS personnel and high demand for IS applications in the 1980s, and support for vertical integration and addressing complex technology in the 1990s.

Back in 1963, and outsourcing contract was made between Electronic Data Systems (EDS) and Blue Cross to provide data processing services (Hirschheim & Dibbern, 2002). What made this contract so different is that Blue Cross turned over their

entire data processing department to EDS, took over IS responsibilities from Blue Cross' IS personnel to help supplement many of the daily functions of the data processing department (Dibbern, Goles, Hirschheim, & Jayatilka, 2004). In the 1970s, EDS continued to expand their outsourcing services by contracting with Frito-Lay and General Motors (Dibbern et al., 2004) and automation of data processing continued to expand.

Another key IT outsourcing arrangement was with IBM and Eastman Kodak back in 1989 which served as the catalyst for IT outsourcing and the beginning of the IT outsourcing era (Loh & Venkatraman, 1992). This contract became more than just an outsourcing arrangement, but proved that Kodak was forming a strategic alliance with their IS partners (Dibbern et al., 2004) instead of the standard short-term contract fulfillment. By far, one of the most recognized strategic outsourcing contract was in 1994 when Xerox awarding a $3.2 billion award to EDS for a term of 10 years (Caldwell, 2002).

During the early stages of IT outsourcing, cost savings was the primary driver for creating outsourcing arrangements (Aubert, Patry, & Rivard, 2005; Livingston, 1992), but closer reviews of some outsourcing arrangements indicate that costs are actually increasing due to legal fees for contract negotiations (Raiborn, Butler, & Massoud, 2009), switching costs of moving from one partner to another (Porter, 1980; Whitten & Wakefield, 2006) and cost reductions not meeting company expectations (Caldwell, 2002). Gonzales, Gasco, and Llopis (2005) conducted an exhausted literature analysis on IS outsourcing from 1995 till 2006. There results showed the primary topics listed were outsourcing from the perspective of the client, success factors, reasons, and risks. Each

one of these components can have a positive or negative effect on costs as some of these topics are much harder to identify and correlate with one another.

Organizations recognize the complexity of outsourcing is no longer the choice to outsource or not to outsource (Loh & Venkatraman, 1992). Organizations have gotten selective on not just the outsourcing of information technology, but making decisions on which specific functions and services will be outsourced and which functions will remain in-house (Grover, Cheon & Teng, 1996). Despite its integration in organizational operations and level of needed expertise, information technology continues to be one of the most outsourced services (Domberger & Fernandez, 2000) and is made up of two primary classifications: assets and services (Grover, Cheon & Teng, 1996). The assets that are outsourced can be human assets or equipment and services outsourcing can be the specific IT function that it selected by the client.

The challenge in outsourcing IT services is knowing what value the vendor will brings to the outsourcing relationship (Levina & Ross, 2003) despite their current reputation, track record, and experience. Goles (2005) asserts that a vendor must possess technical competence and an understanding of the customer's business, while still having the ability to work through future challenges that may arise.

2.4 Decision to Outsource

Early considerations of outsourcing came from the manufacturing industry which, according to Yang and Huang (2000), believed that a decision to outsource should be based on whether an IS function was strategic or commodity (as cited by Venkatesan, 1992). With outsourcing becoming common across business industries, other factors should be considered that would help the organization's current and future needs.

Early stages of IS outsourcing established that many organizations chose to outsource to reduce costs, acquire access to expertise and focus on core competencies. Many of these decisions can be based on cost reduction, access to expertise, culture, and political reason. Organizations are trying to meet their business objectives with the right personnel in place and must deploy the best method of outsourcing required for the needs of the firm.

There have been many discussions on an organization's decision to outsource IT (Teng, Cheon, & Grover, 1995; Kahraman, Engin, Kabak, & Kaya, 2009), but due to the diverse needs of each organization, their different level of internal expertise, and their technical requirements, decisions become difficult to make on outsourcing. Some studies have included determinants of IT outsourcing (Loh & Venkatraman, 1992), decisions on outsourcing success (Grover, Cheon & Teng, 1996), managing outsourcing alliances (McFarlan & Nolan, 1995), and contracts and partnerships (Fitzgerald & Willcocks, 1994). Unfortunately, none of these studies go into details to determine the effectiveness or value needed to create a better relationship and maximize the contract for ideal outcomes for both parties.

Methods of Outsourcing

Since the inception of outsourcing, organizations have implemented different strategies on how they outsource their information systems functions. Many organizations have opted to outsource all of their outsourcing functions to one or more external providers in hopes of focusing their efforts on core business tasks. Other organizations feel that it is not cost effective to outsource all of its IT functions due to privacy and technological concerns (Lee, Geng, & Raghunathan, 2013). In lieu of

outsourcing all IS functions to an external provider, many organizations now have the ability to choose specific information systems components to outsource (Grover, Cheon, & Teng, 1996). In the early stages of technology outsourcing, total outsourcing may have been the only option considering that IS services were limited and options to either keep IS within the company or outsource it no longer applicable to the management of information system functions (Loh &Venkatraman, 1992).

Security Outsourcing

The challenges of information security can be technical, organizational, political, or legal and requires information security professionals to have new skills and orientations (Tipton & Krause, 2007). With the increased outsourcing of IT functions to service providers over the years, outsourcing of security services did not begin until decades later. This shift in security awareness required service providers with a higher level of managing IT functions. These security functions, which may have included firewall, networks, security monitoring, and virtual private networks, needed service providers that had increased expertise in security services. Organizations began to form partnerships with Managed Security Service Providers (MSSPs) to transfer information security responsibilities and operations (Allen, Gabbard, & May, 2003).

Organizations began to expand their environments to include sophisticated networks and firewalls, which meant greater risk and exposure if expert personnel did not manage these functions properly. Vijayan (2001) asserted that in anticipation of this demand for security, vendors began offering outsourced security services. Organizations eventually recognized that outsourcing their security services should be considered if they expected their organization to grow and address future security challenges.

The Decision to Outsource Security

The decision to outsource IS functions has increased in popularity as the need to acquire high level information services to sustain and increase competitiveness in the dynamic external environment grows (Lee & Kim, 1999). IS outsourcing is a common practice compared to the outsourcing of security services, which is still specialized. Security services are frequently associated with the functions of IT services when selecting what to outsource and what to keep in-house. There are many different types of security services that can be outsourced. Some IT security services that are outsourced include network boundary protection, security awareness, access control, audit, intrusion detection, and firewall management (Allen, Gabbard, & May, 2003; Oladapo, Zavarsky, Ruhl, Lindskog, & Igonor, 2009).

For organization's to achieve their goals and optimize security, accurate and informed decisions must be made to determine the best way to contract outsourced IT security services or whether to outsource it at all (Oladapo et al, 2009). Security services, whether outsourced or managed in-house are critical for the organization security state and whose core services are directly associated to the state of its information systems (Bakari, Magnusson, Tarimo, & Yngstrom, 2006).

One of the challenges with outsourcing of security is trying to determine who should be responsible for the information and for the information systems. As organizations continue to manage many of its IT services internally, providing the appropriate level of information security to critical assets is becoming a problem (Karyda, Mitrou, & Quirchmayr, 2006). They stated that although there are risk factors

in outsourcing IT security services, a lack of security expertise could create additional risk due to unnecessary costs and other complications like moral hazard.

Some organizations look at moral hazard as an issue before moving forward with outsourcing. How can an organization truly consider outsourcing if they do not know what the provider is doing? This can lead to issues of trust, legal drawbacks, and short-term engagements. To reduce moral hazard and increase trust, clients that outsource their security services to MSSPs must have mutually agreed upon audit processes in place to monitor the providers' activities and to ensure that all policies and procedures that were stipulated in the contract agreement are being followed (Bakari, Magnusson, Tarimo, & Yngstrom, 2006). To compliment Bakari et al (2006), Kavcic and Tavcar (2008) posited the most effective way to address moral hazard is establishing a defined level of performance [service level agreement] and monitoring. Having an SLA and monitoring in place provides accountability for the provider and visibility for the client.

Considering the complexity of how modern day firms are established with compliance and security, this can often create conflicts later if not addressed in the beginning. Bakari, Magnusson, Tarimo, and Yngstrom (2006) concluded that when outsourcing security to MSSPs, organizations should retain ownership and responsibility for securing and protecting their most valuable asset-information. As far as the information systems organizations should retain ownership for the secure operations of the information systems themselves (Allen et al., 2003).

2.5 Outsourcing Management

There is much debate about the proper governance and management of an outsourcing arrangement to make it successful. Loh and Venkatraman (1992) posited that

key determinants of IT outsourcing is the integration of both business and IT perspectives and is dependent on business governance. Business/IT alignment has been shown to be an important indicator of IT success (Feurer, Chaharbaghi, Weber, & Wargin, 2000) and a critical component to IT governance in outsourcing arrangements (Scholosser, Wagner, Beimborn & Weitzel, 2010). Gewald and Helbig (2006) mention a governance model for managing outsourcing partnerships. A governance model may assistance with management and structure, but little to no detail within their research list what effectiveness governance would have on the contract.

Managing Risk in Outsourcing

Risk can play a significant role in the success or failure of an outsourcing contract. Client organizations continue to struggle with the challenges of effectively managing IT outsourcing (Koh et al., 2004) and the risk that potential comes with outsourcing IT functions to external vendors. As with any outsourcing contract, there will always be a certain level of risk that is taken by both the client and the provider. A key strategy to minimizing risk is that both parties involved in the outsourcing contract share the risk (Yang, 2000). By doing this, both parties can have a better mutual understanding of how to address issues as they arise. Lee and Kim (1999) define mutual understanding as the level of understanding of behaviors, goals, and policies between parties. Have this in place can help avoid social, operational, and legal challenges with the outsourcing arrangement later.

To have a better of understanding of the potential risks that an organization may face with outsourcing, Endorf (2004) recommends having a risk analysis completed to determine the level of exposure or risk the company has. One aspect to consider from the

client's perspective is how much control is actually being given over to the outsourcing provider. Osei-Bryson and Ngwenyama (2006) postulated that a loss of control involves risk of shirking or under performance from a vendor and also opportunistic bargaining, in which vendors typically demand a higher than expected price for their services. For the client to protect themselves and limit their risk, they should have some knowledge about the provider's ability to perform the required outsourcing services. According to Whitten and Wakefield (2006), a lack of knowledge of a provider's ability to perform could represent considerable risk if the service provider has to be changed to one that has the capabilities. It is always best to reduce risk by validating a service provider prior to entering into a contract.

Managing the Outsourcing Contract

One critical way of managing an outsourcing arrangement properly is through the contract. What has to be taken into account is that contracts have both tangible and intangible components, which are categorized by Barthelemy (2003) as the hard and soft side of the contract. Barthelemy noted that the hard side of the contract is the design and implementation of a good contract, while the soft side deals with trust, relationships, and both client and provider not take advantage of one another and put mutual interest in the joint venture ahead of personal interest of either party. Barthelemy had several conclusions to his study. The first is that managing the hard and soft sides of the contract increased overall satisfaction and led to a higher degree of success for the outsourcing arrangement. The other is that managing the contract through the hard and soft side proved to be effective. Other findings determined that IT outsourcing management should

contain hard side management, soft side management or a combination of both for success and those do not incorporate one or both are destined for failure.

Another concern around the proper use of outsourcing is how the contract is written. Lacity and Hirschheim (1993, p. 80) asserted, “The contract is the only mechanism that establishes the balance of power in the outsourcing relationship.” Information written vague or incomplete can be a detriment to the entire outsourcing arrangement. Prado, de Souza, Hiroo, and Reinhard (2009) posited that contracts should be written in a way that will increase partnerships, increase flexibility of the agreement, and ensuring good levels of quality and productivity.

Goo, Kishore, Rao and Nam (2009) view the outsourcing contract in a formal capacity and assert that properly documented service level agreements have an influence on relational governance. Hirschheim and Dibbern (2002) stated that there should be a clear separation between the formal outsourcing contract and the outsourcing relationship itself. They go on to say that while the relationship may have an effect on the contract, the two should be viewed as mutually exclusive in outsourcing arrangements.

Some researchers look at the outsourcing contract from a psychological perspective to manage relationships. Koh, Tay, and Ang (1999) identified 11 client and 10 vendor expectations around an outsourcing contract and looked at the variances between their expectations of one another. The tests consisted of 44 clients and 65 vendors and the study revealed that the psychological contract concept [as opposed to the formal contract] helps to develop a better understanding of mutual client vendor obligations and their impact on project outcomes. The authors conclude that the key differentiator of the psychological concept method is looking at perspectives from both

parties and this mutuality is helping identify expectations that lead to success instead of failure.

Koh, Ang, and Straub (2004) conducted research on outsourcing success from a psychological perspective. In Study 1, psychological contract obligations were identified from four of the largest customer organizations and four of the largest suppliers of outsourcing. Interviews were made with nine customer project managers and six supplier project managers and the results revealed some obligations were symmetric [supplier obligation for effective human capital management and knowledge transfer]. In Study 2, it was determined that project scoping and projecting pricing was related to project outcomes. While each of the outcomes did have some relevance to the formal contract, it was determined that the psychological components outweighed the formal aspect of the contract.

Proper outsourcing management can increase the probability of success with most outsourcing arrangements. Since the nature of outsourcing has grown complex, outsourcing management has become challenging given the business environment is continuously going through rapid changes (Sia, Koh, & Tan, 2008). Previous literature has mentioned several key areas of outsourcing management including relationships and contracts.

Managing Outsourcing Relationships/Partnerships

Previous studies have examined the management of outsourcing relationships from different perceptions (Goo & Nam, 2007) and the partner relationship itself (Lee & Kim, 1999; Rockart, Earl, & Ross, 1996; Shi, Kunnathur & Ragu-Nathan, 2005). Several studies mention the relationship in outsourcing related to client-vendors (Kern & Blois, 2002; Kern & Willcocks, 2002; Sun, Lin, & Sun, 2002), and this always has an effect on

outsourcing arrangement and risk if an unsteady relationship starts. Managing risk is extremely important in an IT outsourcing arrangement and sometimes it is difficult to determine when the benefits outweigh the risks, especially in a troubled outsourcing relationship (McFarlan & Nolan, 1995).

Although the growth of outsourcing is increasing for IT services, clients and vendors are admitting that issues still exist that have led to less than expected outcomes (Pannirselvam & Madupalli, 2011). If not managed properly, a poor relationship can create unnecessary risk that has to be managed if the outsourcing arrangement is to become successful. Logan (2000) stated that proper management of a customer-vendor relationship is being able to manage conflicts intuitively. Logan states that managing conflicts successfully will lead to successful long-term relationships. The strength or weakness of a relationship between organizations can determine the outcome of existing outsourcing contracts and future contracts, if any.

Some organizations are looking to enhance relationship through alliances and not through the contract itself. McFarlan and Nolan (1995) conducted a study on managing an IT outsourcing alliance and determined that the success or failure of IT outsourcing is managing the relationship less as a contract, but as a strategic alliance. Many organizations feel that IT outsourcing has to be managed based on the relationship, but other researchers feel that it contains other factors as well. Clients and service providers can have a successful outsourcing arrangement by properly managing all aspects of the contract, having contingency plans in place when problems occur and by building the relationship into a strategic partnership.

2.6 Service Providers

Empirical studies have discussed service providers and the roles they play in outsourcing arrangements. Much of the literature, in an outsourcing capacity, discuss the use of vendors to help reduce costs (Loh & Venkatraman, 1992), focus on core competencies (Lacity, Hirschheim, & Willcocks, 1994), and have access to expertise and new technology (Smith, Mitria, & Narasimhan, 1998). Lee and Kim (1999) opted to look at service providers for IS outsourcing through partner quality and how it affects outsourcing success. Other studies have discussed the vendor-client relationship (Lee & Kim, 2005) in which trust and formal contracts with the service provider are just as equally important (Poppo, 2002). Although service providers are aided in the effective use of outsourcing, studies are limited in the parallel discussion on service provider that provide It functions in addition to security as opposed to service providers who focus primarily on security services themselves.

Managed Security Service Providers

With the increased awareness of information security, Managed Security Service Providers (MSSPs) are playing a critical role in the outsourcing of security services in an effort to make security better (Lee, Geng, & Raghunathan, 2013). MSSPs are responsible for providing security services, which may include monitoring, remediation, and other security operations. IT service providers usually offer core information technology services to their customer along with some security services. MSSPs, on the other hand, provide security services as their core business offering which makes their value proposition appealing for a wider range of organizations (Gupta & Zhdanov, 2012). MSSPs usually have a higher level of security expertise than a standard IT service provider and can provide expertise at a lower cost (Allen et al., 2003). Selecting the

correct MSSP is just as important as it is to outsource security for the organization. With outsourcing, organizations are able to transfer some or all of their security risk to MSSPs, but there still has to be a continuous management process in place for the reliable security state of the organization (Bakari et al, 2006). Even with the best contracts in place and with the most experienced MSSP, a gap can still exist between the requirements of the outsourcing arrangement and the perceived level of satisfaction from the client. This gap can exist because service level agreements (SLAs) are not well developed to efficiently manage the IT outsourcing relationship (Karten 2004) between the MSSP and the customer.

Service Provider Effectiveness

Prior research on service provider effectiveness is limited, particularly around IS and security outsourcing. The dichotomy of outsourcing is no longer whether an outsourcing arrangement had successful and unsuccessful results, but additional focus looks at the degree of success with considerations such as delivery performance (Beaumont, & Sohal, 2004), relationship management (Zainuddin, Bassellier, & Benbasat, 2010), and expertise (Cullen & Willcocks, 2003). IT Outsourcing ventures have been termed successful or less successful in achieving their outsourcing objectives based on the operational effectiveness of the relationship between both parties (Kern & Willcocks, 2002)

Given that many outsourcing projects are not all successful, lack of competencies and poor management of client-vendor relationships are pivotal obstacles (Zainuddin et al., 2010), which can hinder a service provider from being both effective and successful. One of the key distinguishing factors with a service provider is ensuring maximum

effectiveness during all stages of the outsourcing arrangement. There is a critical distinction between the degree success of a service provider and the effectiveness of a service provider and this is applicable throughout the entire lifecycle of the outsourcing contract. Effectiveness can be a component which helps lead to success, but success itself can be achieved without effectiveness, thus not maximizing all benefits and reaching total customer satisfaction.

2.7 Outsourcing Success

IT services have continued to be a critical part of an organization's core business and the management of these services is key indicators of an organization's future success (Bagaya, 2007). Having an understanding of what functions to outsource and what to maintain in-house is critical to the success of outsourcing. Some organizations outsource all functions while others choose to be selective about the specific functions they outsource. Lacity and Willcocks (1998) concluded that selective outsourcing decisions achieved expected cost savings frequently as opposed to outsourcing all functions or no functions at all.

Outsourcing success is different for each customer. Success could mean a reduction in cost, leveraged expertise to complete a project or task or having the ability to focus on core competencies. Qi and Chau (2012) define IT outsourcing success is the overall advantage gained from the outsourcing strategy. Prior research defines successful outsourcing as being achieved when the customer has achieved both satisfaction and benefits from the outsourcing arrangement (Grover, Cheon, & Teng, 1996). Prior research has provided very little insight into successful outsourcing success within the context of IS security. Much of the literature discuss security risks affiliated with IS

outsourcing (Zhao, Xue, & Whinston, 2009). The relationship between vendor and customer in an outsourcing arrangement is paramount to its success or failure. (Lacity & Willcocks, 1998; Lee & Kim, 1999).

The success of the service is tangible and potentially measured by the contracts, the service level agreements defined, and the perceived cost savings of leveraging external expertise. While on the surface, it would appear to simply write better contracts to make service providers effective, but creating complex contracts potentially increases the risks of both the client and the provider, which directly affects the contract and its outcome.

2.8 Literature Gaps

A key objective of this study is to identify and address some of the gaps in the literature within the context of outsourcing security. This research is aimed at identifying determinants of service provider effectiveness and the impact that is has on overall outsourcing security success. When reviewing existing literature, an extensive number of empirical studies have various aspects of IS outsourcing as it relates to IT functions, but very few studies have looked at the outsourcing of security services within an IT department.

Other limitations in research include service providers and their ability to be effective when it comes to addressing the needs of the client, but very few have determined the client's perceived effectiveness of the service provider. While there are some factors that would perceive a service provider as effective such as reputation, status, and previous customers, setting criteria of effectiveness for a service provider has to come from the customer.

Another limitation within research for outsourcing is the lack of understanding around the needed symbiosis for IS outsourcing success. There are notable studies that discuss the importance of the having a good contract and having a good relationship to foster success. Symbiosis between client and vendor is when mutualistic interests are present before the contract is signed. True symbiosis is the belief that both parties will do the right thing throughout the outsourcing arrangement and that one specific party cannot benefit over another. Outsourcing success is viewed by Grover, Cheon, and Teng (1996) as the attainment of benefits whether strategic, economic or technological, so both parties, if symbiosis is present should experience these or other defined benefits as a result of a successful arrangement. Ultimately, symbiosis is what will help organization move towards better successful outsourcing arrangements and create better strategic partnerships clients and vendors.

2.9 Summary

Based on the information provided in the literature review, information security, IT outsourcing, and IT services management can have a significant impact to all levels of an organization. Given the studies that were reviewed, none of them took into account how IT service provider effectiveness is viewed, understood, and measured at the security, services, and outsourcing level. Key determinants have not been identified in existing literature to discuss service provider effectiveness. The focus of this study was to identify what the key determinants are of an effective service provider and understand what impact it has on the outsourcing arrangements. Given the complexity of IT services, combined with outsourcing and security, this has created new challenges that must be

uncovered and addressed within outsourcing security and the effectiveness of service providers.

Chapter 3

Research Methodology

3.1 Introduction

This chapter establishes the study and provides in depth the research methodology, which includes the theoretical basis, research model, hypotheses, the development process for the research instrument, data collection method, and the data analysis techniques. This chapter will conclude with a summary of the research methods.

3.2 Theoretical Basis

Agency Theory (AT) was selected for this study to help explain the phenomenon of effectiveness with security service providers and how this impacts outsourcing success. Understanding the context of a research problem is important when applying a theory. Several theories have been successfully applied to IS outsourcing such as Transaction Cost Economics Theory (Lacity & Willcocks, 1995) to assist as a decision making tool on what to outsource; Resource-based Theory (Barney & Hesterly, 1996) on the discussion of resources and capabilities for outsourcing; Knowledge-based View (Nasiopoulos, Sakas, & Vlachos, 2014) for knowledge sharing among partners and Social Exchange Agency Theory (Whitten & Wakefield, 2006) that looks at phases of reconsideration during outsourcing. While these theories provide extensive information on the overall concept of outsourcing, this research is looking to uncover how outsourcing arrangements can be improved by looking closer at the principal-agent relationship and addressing challenges that impede outsourcing success. Agency Theory

will be used to address this issue and detailed information will be provided on its purpose.

Agency Theory (Figure 2) was originated from the work of Alchian and Demsetz (1972) in which the economic organization faced two important problems: determining if gains from specialization and cooperative production could be obtained within the organization and understanding the structure of the organization itself. While set in an economics perspective, Jensen and Meckling (1976) looked at agency theory from the scope of agency costs associated with contractual agreements between owners and top management of the corporation. They discuss the incentives set by each party and properly determining a contract of equilibrium between the principal and the agent.

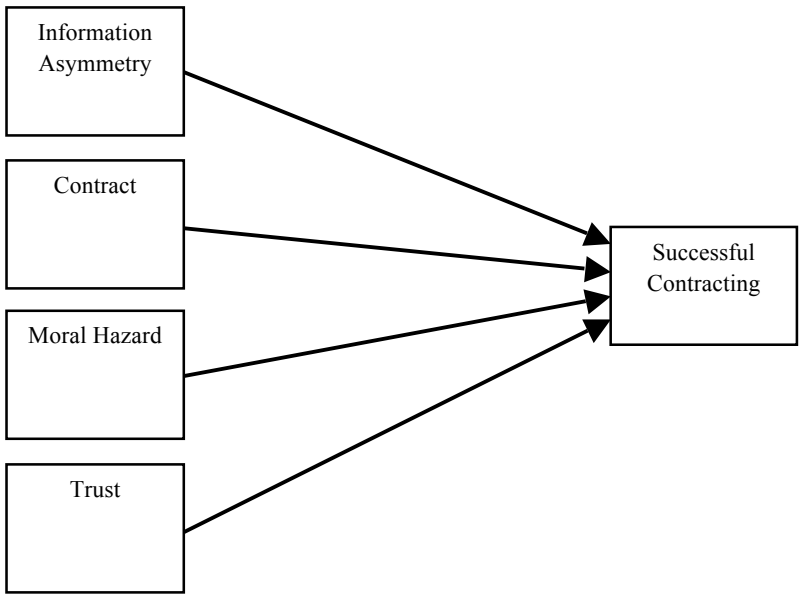

Figure 2. The components of the Agency Theory Model.

Eisenhardt (1985; 1989) asserted that agency theory is concerned with resolving problems related to conflicting goals, risk sharing and perceived risks taken between the principal and the agent. Eisenhardt stated that agency theory is directed at the ubiquitous agency relationship for delegated work and performing work between two parties. The

Agency Theory model consists of several variables that are associated with successful contracting (see Figure 2). These variables are information asymmetry, outsourcing contract, moral hazard, trust, and outsourcing success. Agency Theory helped establish the foundation for the research model.

3.2.1 Research Model

Through this research, each of the variables were described and the underlying hypotheses associated with those variables. For the purposes of this study, Service Provider Effectiveness (SPE) is related to a security service provider managing outsourced security services and Security Outsourcing Success (SOS) is related to the outsourcing of IT security services.

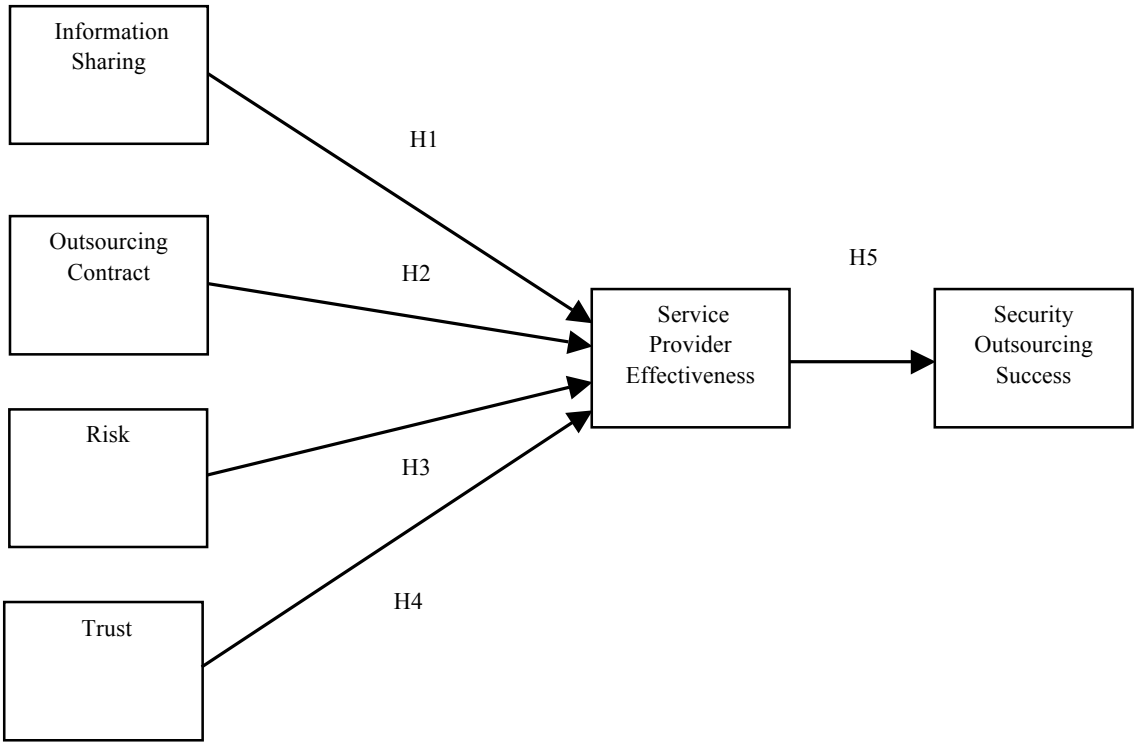

Figure 3. Research model for Information Security Outsourcing Success

3.2.2 Hypotheses Development

This section presents and describes the five hypotheses identified based on the research model and a brief description of each variable relationship.

Information Sharing & Service Provider Effectiveness

The hypothesis representing this relationship is: An increase in the level of information sharing leads to an increase in service provider effectiveness (**H_1**)

Organizations create value through the exchange of information sharing (Rollins, Pekkarinen, & Mehtala, 2011) and without it; information awareness is not as high as it should be. This lack of information awareness is known as information asymmetry (Clarkson, Jacobsen, & Batcheller, 2007). Information asymmetry is when an imbalance of information knowledge exists between one entity and another. Information asymmetry can occur because sellers of services usually have information about the true quality of their service and may exert less effort to reduce costs in the delivery of their services (Ding & Yurcik, 2005; Nayyar, 1993). This can be a major concern between principals and agents of service arrangements. Information asymmetry can have a significant impact on security outsourcing and service delivery. If a customer did not have all of the information needed to make a sound decision on security outsourcing, the service provider lack the security expertise needed to deliver the appropriate level of security services.

The independent variable, information sharing, was measured based on the transfer of information, through communication and knowledge sharing as perceived by the client towards the service provider. This will help establish if both parties have equal information about one and have a clear understanding of information is being

disseminated from one party to the other. An ideal outcome would be for both parties to have an adequate amount of information symmetry for one another to make the best decision on entering into an agreement.

Outsourcing Contract & Service Provider Effectiveness

The hypothesis representing this relationship is: The better the outsourcing contract agreement, the higher the service provider effectiveness (**H_2**)

A contract typically involves a formal [legal] and informal [relationship] agreement between a client and a service provider (Barthelemy, 2003). The formal contract is the legal contract established between the client and provider on service level agreements, costs, penalties, objectives, and deliverables. Barthelemy (2003) refers to the legal aspect of the contract as the "hard side", given that specific requirements and deliverables of the contract are documented. Good formal contracts must be precise (Saunders, Gebelt, & Hu, 1997) and written in a way to ensure good levels of quality and productivity. The informal component of the contract, considered the "soft side", involves a relationship built on trust between the client and the vendor (Barthelemy, 2003). The greater the trust built between the client-vendor partnership, the better chance of achieving ideal results (Anderson & Narus, 1990). Combined, the informal and formal contract has a significant impact on the effectiveness and success between clients and service providers.

Risk & Service Provider Effectiveness

The hypothesis representing this relationship is: A lower level of risk for IT security services leads to an increase in service provider effectiveness (**H_3**)

There are many risks associated with outsourcing such as hidden costs, contractual issues, and potential loss of organizational competencies (Aubert, 2005). These risks can increase because clients and service providers cannot observe and verify each other's efforts (Lee, Geng, & Ranghunathan, 2013), thus causing moral hazard between one or both parties. Moral Hazard is when two parties engage in risk sharing and the actions of individuals cannot be easily observed or monitored (Holmstrom, 1979). Moral hazard is when a contractor may avoid working without being discovered which makes output quality hard to discover (Ding & Yurcik, 2005a). Moral hazard in security can bring about many challenges when service providers are managing sensitive security information of customers. Clients and service providers, especially with security outsourcing, should work to create transparency between the two organizations if risk is a concern.

Trust & Service Provider Effectiveness

The hypothesis representing this relationship is: An increase in the level of trust between the customer and the service provider leads to an increase in service provider effectiveness (**H_4**)

Trust is the belief that a person or party has the intention of doing the right thing. Trust is established through a longstanding, successful relationship between a customer and a provider (Logan, 2000). According to Billhardt, Hermoso, Ossowski, and Centeno (2007), reputation mechanisms along with trust can be used as a complementary means of selecting the best provider for a service. In the scope of security, Josang (1996) defines trust as a belief that a passionate entity [people] will behave without malicious intent and a rational entity [system] will not be susceptible to malicious manipulation. Trust plays a significant role in a customer-vendor relationship and will have an effect on tactical and

strategic partnerships. Having trust with a provider helps organizations determine not only who will provide services, but which components of IT services will be outsourced.

Service Provider Effectiveness & Security Outsourcing Success

The hypothesis representing this relationship is: Higher service provider effectiveness leads to an increase in security outsourcing success (**H_5**)

Service Provider effectiveness is defined based on literature related to IS Effectiveness and Organizational Effectiveness. According to Hamilton and Chervany (1981), IS effectiveness is the extent to which an information system contributes to achieving organizational goals and effects organizational performance. Thong and Yap (1996) posited that these information systems are only deemed effective if they contribute to organizational effectiveness. Service providers are responsible for managing specific functions or services for their customers. For this study service provider effectiveness is the expertise and efficiency of the service provider and their ability to help organizations achieve their goals and objectives. There are many factors that can affect service provider effectiveness when dealing with the principal (the service provider) and the agent (the customer). The intent of the agent is to maximum the use of the principal's expertise to possibly cut costs and gain access to skills and knowledge that may not exist within the organization.

The dependent variable, security outsourcing success, is adapted from the study of Grover, Cheon, and Teng (1996) and is defined as the gained satisfaction and benefits received from the outsourcing arrangement. Because the outsourcing is specific to information security, the gained satisfaction is protected and secure information and the benefits received are leveraged expertise and experience from the security service provider. In their study, Grover Cheon and Teng (1996) measured outsourcing success

through the attainment of key benefits described as strategic, economic and technological. For this study, benefits are described in a similar context, but specific to IS security, and within the scope of satisfaction.

A summary is provided of all the hypotheses for this research study:

- H1: An increase in the level of information sharing leads to an increase in service provider effectiveness
- H2: The better the outsourcing contract agreement, the higher the service provider effectiveness
- H3: A lower level of risk for IT security services leads to an increase in service provider effectiveness
- H4: An increase in trust between the customer and the service provider leads to an increase in service provider effectiveness
- H5: Higher service provider effectiveness leads to an increase in security outsourcing success

3.2.3 Constructs and Indicators

The study contained several latent constructs that are not directly observable. The review of literature helped uncover specific indicators of each construct that was used to observe each construct within the context of security outsourcing. Table 1 lists the constructs, their indicators and brief description of how each was applied in the study.

Table 1

Research Constructs and their Indicators

Constructs	Indicators	Definition	References
Information Asymmetry	Information Sharing	Possessing the required level of knowledge and information about a service provider and customer	Aubert et al, (2005)
Outsourcing Contract	Contract Management	Managing the relationship and the development and enforcement of a written service contract between a service provider and the customer	Qi & Chau (2012), Barthelemy (2003), Lacity & Hirschheim, (1993), Goo & Nam (2007), Barthelemy (2003), Saunders et al, (1997)
Moral Hazard	Risk	The exposure, harm, or lose incurred due to their service provider	Kern et al., 2002
Trust	Trust (belief)	When one entity trusts another entity based on the belief that they are benevolent	Aubert et al., (2005), Josang (1996), Josang et al., (2007), Webb & Laborde (2005)
Service Provider Effectiveness	Service Quality	Meeting the expectation of the client through quality of work and adherence to service level agreements	Barthelemy (2003), Smuts & Merwe (2010), Goo & Nam (2007)
Security Outsourcing Success	Benefits	The organizational advantages gained from the IT outsourcing strategy	Grover et al., (1996), Goo & Nam (2007), Qi & Chau (2012)

The identified reflective constructs and their indicators represented in the study serve as a strong foundation for acquiring information about service provider effectiveness and how it is related to security outsourcing success. Given the focal point of this research is security in nature, information has been provided on the variables that will support the study.

3.3 Research Method

The researcher determined that the most appropriate path for addressing the research problem is to conduct a quantitative survey-based study. The researcher sought to uncover specific factors that promote the effectiveness of service providers and the success of outsourced security.

3.3.1 Survey

For the research method, a cross-sectional online survey was used. Babbie (1990) asserted that surveys include cross-sectional and longitudinal studies using questionnaires or structured interviews for data collection, with the intent of generalizing from a sample to a population. The use of a survey approach has several advantages. One advantage is that survey research provides a cost-effective way to gather information about a larger population and can be applied to almost any type of research (McCormack & Hill, 1997). Another advantage of survey research is that with the use of the Internet, web surveys can be sent to email addresses of targeted respondents, which could help reduce the timeline needed to conduct the survey (Schonlau, Fricker, & Elliot, 2002). A final advantage of utilizing a survey is that researchers find its popularity provides for versatility, efficiency, and generalizability of research (McCormack & Hill, 1997).

According to Creswell (2009), a survey design provides a quantitative description of trends, attitudes or opinions of a population by studying a sample of the population. Creswell (2009) noted that if a problem is identifying factors that influence or help understand predictors of an outcome, then the best approach would be quantitative approach.

3.3.2 Instrument Development

In this section, information is provided on the development of an instrument for the research study (see Figure 4).

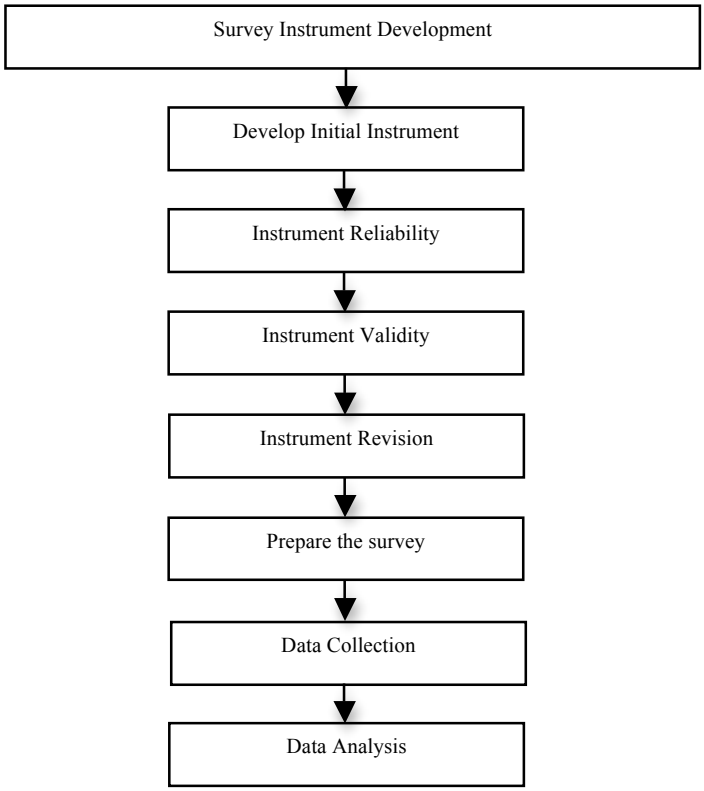

Figure 4. Instrument Development Model

The development of the research instrument started with identifying the survey questions that will be used within the study. These questions have been derived from the latent constructs and their indicators (see Appendix A). Having reliability in a survey instrument is important in research because reliable measures yield consistent results (Holton & Burnett, 2005). Reliability is a statistical measure of how reproducible the data is from the survey instrument and can be measured using internal consistency (Litwin, 1995). The reliability of the survey instrument used in this research leveraged Cronbach's alpha to measure internal consistency. "Cronbach's alpha is a model of

internal consistency reliability based on the average inter-item correlation of an instrument" (Rovai, Baker & Ponton, 2013, p. 465) and is commonly used to see how closely a set of items are as one group or unit. The alpha coefficient ranges for Cronbach's alpha are from 0 to 1. Gliem and Gliem (2003) state that a Cronbach's alpha coefficient greater than .70 indicates good internal consistency of the items in a measurement scale and the closer the value is to +1.0, the better the internal consistency of the measurement scale.

Validation of the initial instrument followed the process identified by Straub (1989) and used construct (the relation to other variables) and content (representation of the topic studied) validity along with reliability to ensure a working instrument is properly in place. Content validity is based on the extent to which measurements reflect the specific intended domain of content based on the professional aptitude of experts in the field (Anastasi, 1988). For content validity of this research instrument, the researcher sought ten security professionals for the expert panel, which was based on similar studies of information security (Knapp, 2006; 2007). Each of the security professionals possessed one or more of the following skills, experience or certifications:

- Certified Information Systems Security Professional (CISSP) certified
- Information Security Professional with 5+ years of practical experience
- Information Security Professionals specialized in Security Outsourcing
- Practitioner or Educator with extensive theoretical and practical knowledge of security outsourcing, outsourcing, or security practices

These individuals helped confirm the content validity of the survey questions and ensured that the information listed was relevant to the research problem, the hypotheses, and the outcome of the research study. Validity measurements are achieved when scores can

capture the ideas contained in the corresponding concept (Creswell, 2009). Demographics were collected along with information from the expert panel and the instrument validity began. After receiving feedback, revisions were made and the final instrument was completed and prepared for use.

3.4 Data Collection

After the final instrument was validated, data was collected through the use of an online web survey. A proprietary web address and link was created for the web survey and was sent via email requesting that participants click on the link, review the details of the research and voluntarily complete the survey. The link was generated from Survey Monkey and embedded within the email request. Each participant was advised of the survey window and the time frame needed to complete the survey for it to be considered valid.

The survey instrument used a combination of value labels – Strongly Agree to Strongly Disagree to identify the effectiveness of security service providers and the impact it had on outsourced security success. The measurement section within the survey instrument was based on a 5-point Likert scale. One of the key issues with the analysis of Likert data is the compilation of responses to question items (Masters, 1985). It is critical to utilize the proper scale to ensure that the model is aligned properly for the study. A five-point scale allows the participant to not only agree or disagree with a survey question, but also provides the ability to select a neutral option if the question or portion of the question is not known or verifiable. In previous studies using a five-point scale, it was determined that reliability was higher as compared to other scales (Jenkins & Taber,

1977). Preston and Colman (2000) concluded that when comparing indices of reliability and validity, two-point, three-point, and four-point scales performed relatively poorly.

The distribution method of the web-based survey was facilitated through the use of all customers receiving security services from the same service provider. This provider is based in the Southwestern part of the United States and provides security and cloud services throughout the United States and areas abroad. The survey was made available for approximately 120 days until the optimal number of surveys were received, which was greater than 200. Once the survey period expired, the URL will be disabled and responses were no longer accepted.

3.4.1 Population and Sample Size

As mentioned, the URL link to the web-based survey was disseminated to potential survey participants. To ensure that an adequate sample size was acquired, commercial marketing was used to properly identify, screen and gather the appropriate participants. Individuals participating in the research study represented a single organization and allowed the researcher to gather adequate information from diverse demographics and help operationalize the study and provide a true representation of the population.

The sample size needed to establish statistical validation for the research study is determined based on the guidance of factor analysis. Comrey and Lee (1992) asserted that a minimum of 200 valid responses is needed for a fair assessment and to meet sampling accuracy with a confidence level of 95 percent and a confidence interval of 5 percent, a minimum of 218 initial responses is required (Rhea & Parker, 2005). Tests conducted by Costello and Osborne (2005) reported that larger sample sizes using factor

analysis produces better accurate solutions to the population. Before any analysis began, the research collected 231 total responses that were subjected to validation with the intention of meeting statistical rigor and accuracy requirements. The outcome of the number of valid responses is discussed in Chapter 4.

3.4.2 Unit of Analysis

The unit of analysis relevant to the researcher's study is at the organizational level and serves as the population of which the research findings will be applied (Rhea & Parker, 2005). Each individual participating in the survey represented one unique organization that received security services from the service provider identified in this research study. All firms selected had an active subscription or contract with the same Managed Security Service Provider and receive at least one information security service from that provider.

3.4.3 Participants

With the unit of analysis at the organizational level, participants within each firm were Professionals, Management or Executive level personnel that meet the following requirements of the research:

- Formidable knowledge of the planning and existing security outsourcing contract between the organization and the security service provider
- Individuals who manage or have access to the security department or team that is working with the security service provider
- Individuals that have up to date knowledge on the operational aspect of the security service provider's day-to-day job functions and role

3.4.4 Data Preparation and Screening

Once the data was gathered, prior to beginning any analysis, it must be validated for completeness and accuracy. Unfortunately, in some instances, data collected can be

inaccurate, incomplete or missing and must be handled appropriately before analysis can begin. Hair et al. (2014a) contends that to address these issues:

- If reviewing the dataset and 15% or more of the observation is missing, it should be removed, but if only 5% or less is missing from the dataset, then it should be retained and mean replacement should be used.
- If straightlining [one answer for all] or inconsistent answer patterns are present, the dataset should be removed
- If outliers with extreme responses are present, typical this would be removed, but the researcher should determine if a distinct group exists in the dataset for it to be retained.
- Datasets that exhibit distribution deviation substantial from normal should be reviewed by the researcher to determine if the dataset would potentially distort the results

3.5 Data Analysis

After all the data had been collected and validated for completeness, several analysis techniques were used (see Figure 5) to analyze the data for the research study. Confirmatory Factor Analysis (CFA) and Partial Leased Squares-Structural Equation Modeling (PLS-SEM) was used for this research and the details explaining this justification are listed in the next section.

3.5.1 Analysis Techniques

This section will provide each analysis technique along with background information and relevance to this study. This section will conclude with the detailed steps involved in the analysis process.

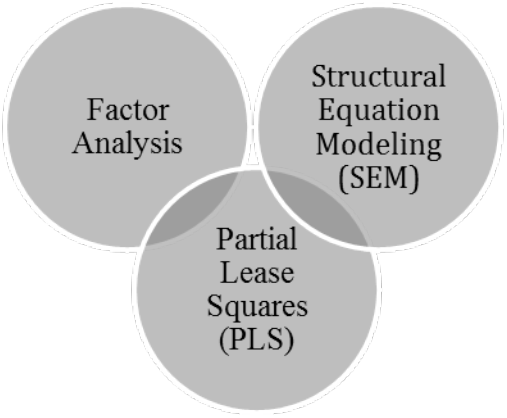

Figure 5. List of Analysis Techniques

3.5.2 Factor Analysis

The first technique is the use of factor analysis (FA) to confirm construct validity of the research instrument. FA is a parametric procedure that analyzes interrelationships for a large number of variables while explaining their common dimensions [factors] (Rovai, Baker, & Ponton, 2013). The purpose of FA is to find the underlying structure among variables, through data reduction (Rovai, Baker, & Ponton, 2013) and is the method of choice for interpreting questionnaires (Bryant, Yarnold, & Michelson, 1999), analyzing survey data (Yuan, Marshall, & Bentler, 2002) and scale assessment and development. Depending on the research objectives, several approaches can be taken when analyzing data. Some common factor analysis techniques include principal component analysis (PCA), exploratory factor analysis (EFA), and confirmatory factor analysis (CFA).

Principal Component Analysis (PCA) is "a multivariate technique that analyzes a data table in which observations are described by several inter-correlated quantitative dependent variables." (Abdi & Williams, 2010, p. 1). PCA makes no distinction when it comes to conceptualizing sources variance in measured variables, which means the

components contains a combination of common and unique variances (Conway & Huffcutt, 2003). PCA is regarded as a component of factor analysis and is the appropriate data analysis technique when the research purpose is to reduce the dimensionality for a set of direct measures (Yang, 2005).

Exploratory Factor Analysis (EFA) is a model used for investigating common, but unobserved sources of influence in a series of variables and has proven to be an efficient method of providing a way to study constructs and traits (Cudeck, 2000). EFA explores the underlying structure of a set of interrelated variables (Child, 1990) and helps to articulate the data used in scale development. EFA is normally used to explore underlying factors related to variables that indicate a phenomenon (Yang, 2005) and can be useful for refining measures, evaluating construct validity and hypotheses (Conway & Huffcutt, 2003).

Confirmatory Factor Analysis (CFA) is an approach used to test a proposed theory or model and has assumptions based on priori theory regarding the number of factors (Williams, Brown, & Onsman, 2012). CFA is used to confirm that a hypothesized model provides a good fit for the data (Hotlzman & Vezzu, 2011). CFA usually has a pre-determined number of underlying factors and is used to test whether a pre-determined correlation pattern can be support by the data.

PCA, EFA and CFA have several key differences. According to Conway and Huffcutt (2003), if the purpose of the research is pure reduction of variables without interpreting the resulting variables, then PCA is a good decision. With CFA, it does not assist in enhancing data representation and does not assess convergent validity (Farrell & Rudd, 2009). CFA does not provide evidence of cross-loading items to alleviate

discriminant validity issues (Farrell & Rudd, 2009), but can be used when there is a clear depiction about the factor structure (Burnette & Williams, 2005). CFA may be used to confirm factor structure, but EFA should be used to identify potential problems that may cause an improper CFA fit (Farrell & Rudd, 2009). According to Yang (2005), EFA is a better fit than CFA when dealing with early stages of scale development and how measurement items load on factors that have not been revealed.

Based on the literature, the information gathered from factor analysis and the research model, this study used confirmatory factor analysis for construct validity of the research instrument. This approach was selected because an existing theory (agency theory) is used in this research, a pre-determined number of factors have been identified and analysis should determine if the correlation pattern can support the data. Finally, CFA is the appropriate technique for this research because it can be used to confirm or disconfirm a hypothesized factor structure (Yang, 2005).

3.5.3 CFA Criteria

One of the important aspects of a CFA model is identifying and assessing the appropriate fit. Typically, goodness of fit is conducted with CFA research and covariance-base structural equation modeling (CB-SEM). This research is using Partial Leased Squares-Structural Equation Modeling SEM which looks at the measurement and structural models for analysis of the research data. Mohammed and Afthanorhan (2013) stated that the measurement model is commonly used for CFA and researchers should follow these requirements to obtain the true model of the study. SmartPLS (Ringle, Wende, & Becker, 2015) was used to conduct the CFA analysis, which is not based on goodness of fit indexes, but on factor loading, indicator reliability, internal consistency

reliability and validity of the measurement model. For the validity assessment of a reflective measurement model, convergent validity is analyzed along with indicator reliability and discriminatory validity (Asyraf & Afthanorhan, 2013). The first step of the assessment procedure of a reflective measurement model is factor loading. Factor loading is the correlation between the observed value and the latent of a factor (Vinzi, et al, 2010). Values should be higher than 0.50

The next step is measuring internal consistency. Internal consistency provides an estimate of reliability based on the different outer loadings of the indicator variables (Hair et al, 2012). It is measured as Cronbach's alpha or composite reliability and should be 0.70 or greater.

The next step is measuring convergent validity. Convergent validity is the positive correlation between alternative measures of a construct (Hair et al, 2011). It is determined based on the average variance extracted (AVE) and should be 0.708 or higher.

The next step is measuring indicator reliability. Indicator reliability is the square of the indicator's outer loadings and represents how much variation in an item is explained by the construct and should have a value of .40 for some exploratory studies, but .70 or higher is preferred (Hair et al, 2014a; Hulland, 1999).

The final step for the CFA process is discriminant validity. Discriminant validity is the distinction between other constructs (Hair et al, 2014b). Discriminant validity examine the cross loading of other constructs and the scale indicates that the outer loading of a construct should be higher than its cross loadings for the other constructs. Table 2 shows the CFA criteria and the required value ranges when evaluating the measurement model.

Table 2

CFA Analysis Criteria for the Measurement Model

Criteria	Value Range	Definition	References
Factor Loading	≥ 0.5 (acceptable)	Correlation between the observed value and the latent value for a given factor	Hulland, 1999, Vinzi et al., 2010
Internal Consistency Reliability [Cronbach's alpha (CA) and composite reliability (CR)]	0.70 and higher for both	CA- Based on average inter-item correlation of an instrument CR - Determines reliability based on the outer loadings of the indicator variable	Bagozzi & Yi, 1988, Gliem & Gliem, 2003, Hair et al., 2014a
Convergent Validity (based on AVE)	0.708 is preferred > 0.50 is acceptable	Measures correlations with alternative measures of the same construct	Bagozzi & Yi, 1988, Hair et al, 2011, Hair et al., 2014a
Indicator Reliability	.070 and higher .40 and higher for exploratory research	The variation of an item explained by the construct	Hair et al., 2012, Hulland, 1999
Discriminant Validity	Outer loadings should be greater than all cross loadings on other constructs	Uniqueness of constructs compared to other constructs	Fornell & Larcker, 1981, Hair et al., 2014a

3.5.4 Structural Equation Modeling

First generation techniques, which include regression-based approaches, analysis of variance, discriminant analysis, and logical regression belong to a core set of instruments which are used to confirm priori established theories or identify data patterns and relationships (Hair et al., 2014a). These first generation approaches had limitations, specifically around postulation of model structure, assumptions around all variables being observable, and conjectures that variables are measured without error (Haenlein & Kaplan, 2004). Additional robust techniques were needed, such as structural equation modeling.

Gefen, Straub, and Boudreau (2000) define Structural Equation Modeling (SEM) as a second-generation analysis technique that allows for simultaneous modeling of relationships among independent and dependent constructs. An SEM approach contains two different methods: covariance-based analysis, also known as CB-SEM, and variance analysis, also known as Partial Least Squares-SEM (Hair et al., 2014a; Lehner & Haas, 2010) or PLS-SEM.

CB-SEM develops a theoretical covariance matrix based on a specified set of structural equations (Hair, Ringle, & Sarstedt, 2011) and conducts model parameter estimations in which the difference between theoretical and estimation covariance matrixes are minimized (Rigdon, 1998). The objective of CB-SEM is to show that the null hypotheses are insignificant and that the complete set of specified paths in the model under analysis is plausible and based on the sample set given. CB-SEM is typically chosen when the goal is theory testing or theory confirmation, when error terms require additional specifications such as co-variation, and the research requires a global goodness of fit criterion (Hair et al., 2014a). CB-SEM is also used with principal component analysis.

PLS-SEM is a causal model approach with a purpose of maximizing the explained variance of the dependent latent variables (Hair et al, 2012). According to Hensler, Ringle, and Sinkovics (2009), PLS has become a popular data analysis technique in success factor studies, specifically in areas of marketing (Albers, 2009), knowledge management (Leher & Haas, 2010), and enterprise resource planning (ERP) systems (Ifinedo, 2008). PLS-SEM may be used if there is a small sample size and it works on

reflective and formative models that contain multiple or single item construct indicators. (Hair et al., 2014a).

Based on the information provided in the literature and the intent of the research study, PLS-SEM was used to analyze the data.

3.5.5 Evaluation of the structural model

In any research, it is important to understand not just the analysis technique selected, but also the steps involved in the process. The research model (Figure 3) contains reflective constructs and therefore classified as a reflective measurement model and the steps listed for PLS-SEM data analysis were adopted from Hair, Jr et al. (2014a). PLS-SEM follows a two-step process that involves a separate assessment of both the measurement model and structural model (Hair et al. 2011). The measure model was covered in the previous section, so the discussion continues with the structural model.

Listed below are the steps needed to properly analyze the structural model of the research study using PLS-SEM.

- Collinearity Assessment. This occurs when two indicators are highly correlated with one another. Measurement for the structural model is a tolerance level below .20 and a variance inflation factor (VIF) > than 5 to predict the presence of collinearity. (Hair et al., 2014a)
- Identify the Coefficients of determination (R^2) value. R^2 value is an inner model assessment that represents the amount of explained variance of each endogenous latent variable (Hair et al., 2012). R^2 values can range from 0 to 1 and the higher the number, the better the predictive accuracy. R^2 values of .75, .50, or .25 are described as substantial, moderate, or weak (Hair et al., 2014b)

- Identify the Predictive Relevance (Q^2). Q^2 is used to determine if an omitted construct from a model had a significant impact on the endogenous constructs. The scales for this measure is .02, .15, and .35, which represent small, medium, and large effects (Hair et al., 2014a)
- Identify the size and significance of the path coefficient. Path coefficients represent the hypothesized relationship linking the constructs and have a value range of -1 to 1, which indicates that a value closer to 1 signifies a strong positive relationship (Hair et al., 2014a).
- Identify the f^2 effect sizes. This is the effect of change in R^2 value when a specific construct is eliminated from the model (Hair et al., 2014a). The effect size of the omitted construct for a particular endogenous construct can be determined with values of .02, .15, and .35, which represent small, medium, and large effects (Cohen, 1988).
- Identify the q^2 effect sizes. This is the effect of change in Q^2 and the relative impact of predictive relevance on the exogenous construct and has a value of .02, .15, .35 for certain endogenous constructs, which represents small, medium, and large predictive relevance (Hair et al., 2014a).

Table 3 shows the PLS-SEM criteria and the required value ranges when evaluating the structural model.

Table 3

PLS-SEM Analysis Criteria for the Structural Model

Criteria	Value Range	Definition	References
Collinearity Assessment (VIF Value)	VIF value must be less than 5 and a tolerance level below .20	Collinearity issues arises when two indicators are highly correlated with one another	Hair et al., 2014a, Ringle et al., 2012
Coefficient of Determination (R^2 value)	Range is 0 to 1 for predictive accuracy .25 is considered weak, .50 is moderate, and .75 is substantial	Represents the amount of explained variance of each endogenous latent variable and assesses the quality of a PLS model	Hair et al., 2014a, Hair et al., 2014b
Cross-validated redundancy (Q^2 value)	Helps determined predictive relevance .02 is considered a small effect, .15 is medium, and .35 is large	Used to determine if an omitted construct from a model had a significant impact on the endogenous constructs	Hair et al., 2014a, Hair et al., 2014b
Path Coefficient	Size: Range is -1 to 1 closer to 1 is better Significance: t-value is 1.96 and above for a two tailed test at the 5% level	The hypothesized relationship linking the constructs	Hair et al., 2014a, Hair et al., 2014b
f^2 effect size	.02 is considered a small effect, .15 is medium, and .35 is large	The effect of change in the R^2 value when a specific construct is eliminated from the model	Hair et al., 2014a
q^2 effect size	.02 is considered a small effect, .15 is medium, and .35 is large	The effect of change in Q^2 and impact of predictive relevance on the exogenous construct	Hair et al., 2014b

3.6 Summary

This chapter included a detailed review of the model for this research study. A synopsis was listed discussing the theoretical basis of the research study and a validation of the selected theory. The research model was presented outlining the details of the associated constructs along with the hypotheses used to help validate the original research problem. The research method provided information on the research instrument, the

survey questions within the instrument and how the data was collected and analyzed. This chapter served as the cornerstone for the research study by helping to identify what the key determinants are to service provider effectiveness and its effect on security outsourcing success. The analysis results of the study are presented in the next two chapters.

Chapter 4

Measurement Model Analysis and Findings

4.1 Introduction

This chapter provides a detail of the preparation and screening process for the dataset used for this research study. Confirmatory factor analysis (CFA) was used during the first phase of the analysis for the reflective measurement model and the findings will be discussed.

4.2 Preliminary Screening

Prior to conducting the CFA and SEM analyses, preliminary screening was conducted in SPSS 22.0 (SPSS Inc., 2013) on all the participants in the study ($N = 231$). Screening was conducted following the approach of Curran, West, and Finch (1996). In reviewing the dataset, there were no missing data points, and all items were sufficiently normally distributed [Skew absolute value < 2; Kurtosis absolute value < 7]. All observed values of Skew < 1.03, and all observed values of Kurtosis < 1.42.

Cases were then screened for univariate outliers, which were operationalized as scores greater than 3.29 standard deviations from the mean of a respective variable (Tabachnick & Fidell, 2013). There were a total of 12 individuals that were identified as univariate outliers on at least one observed variable, and these cases were deleted. Data were then screened for multivariate outliers using a regression procedure outlined by Tabachnick and Fidell (2013). In this procedure, Mahalanobis distance is computed for each participant and then compared to a critical value, determined by the number of

variables and the chi-square distribution with p= .001. In the present analyses, there were 26 variables included in the study, so the critical chi-square was 54.1. There were 10 cases with a value on Mahalanobis distance that exceeded this value, and thus they were considered multivariate outliers and were removed from subsequent analyses. The resulting sample contained 209 cases with no missing values, univariate outliers or multivariate outliers, and with all variables sufficiently normally distributed.

Remaining analyses were conducted in a two-stage sequence, as recommended by Kline (2011). In the first stage the measurement model was evaluated, and then the full structural equation model was analyzed in the second stage. The primary purpose of dividing the analyses into two steps is to isolate and address any issues in each model separately. For the CFA analysis of the measurement model, factor loading, internal consistency, indicator reliability, and convergent and discriminant validity were analyzed. The level of acceptance for each category is .50 and higher for factor loading, .70 and higher for internal consistency, .70 and higher for indicator reliability, .50 and higher for convergent validity based on the average variance extracted (AVE). For discriminant validity, the outer loadings on a construct should be higher than all cross loadings with other constructs and the square root of the AVE of each construct should be higher than its highest correlation with any other construct (Hair et al, 2014a).

4.3 Demographics Information

209 valid responses were collected for this study. Respondents to the survey were asked to provide demographic information starting with their gender. 44.98% of the respondents were identified as female, and 55.02% as male. Table 4 shows the gender distribution.

Table 4

Gender Distribution

Gender	Count	Percentage Ratio
Female	94	44.98%
Male	115	55.02%

Respondents were asked to select their appropriate age group. 7.18% of the participants were members of the 18-24 age group, 28.23% of the participants were members of the 25-34 age group, 26.79% of the participants were members of the 35-44 age group, 22.97% of the participants were members of the 45-54 age group, 11.00% of the participants were members of the 55-64 age group, and 3.83% of the participants were members of the 65 and above age group. Table 5 shows the age group distribution.

Table 5

Age Group

Age	Count	Percentage Ratio
18-24	15	7.18%
25-34	59	28.23%
35-44	56	26.79%
45-54	48	22.97%
55-64	23	11.00%
65+	8	3.83%

Respondents were asked to select their highest level of education completed. 12.44% of the participants completed high school or had a high school equivalent, 10.05% of the participants had some college, 14.83% of the participants completed an Associate's degree or equivalent, 37.32% of the participants completed a Bachelor's degree or equivalent, 18.18% of the participants completed a Master's or Graduate degree, 7.18% of the participants completed a Doctorate degree or equivalent. Table 6 shows the Education Level distribution.

Table 6

Educational Level

Education	Count	Percentage Ratio
High School or equivalent	26	12.44%
Some College, but no degree	21	10.05%
Associate Degree	31	14.83%
Bachelor's Degree	78	37.32%
Graduate Degree	38	18.18%
Doctorate Degree	15	7.18%

Respondents were asked to select their organizational role during the outsourcing contract period. 26.79% of the participants were in an Executive Management role, 34.93% of the participants were in some type of management or leadership role, 10.53% of the participants were in a Project Management role, 11.00% of the participants were in a Security role, 11.96% of the participants were in some type of Professional role, 3.35% of the participants were in an individual contributor role, and 1.44% of the participants identified their role as Other. Table 7 shows the organizational role distribution.

Table 7

Organizational Role

Job function	Count	Percentage Ratio
Executive Management, (CEO/VP)	56	26.79%
Management (Director, Manager)	73	34.93%
Project Manager	22	10.53%
Security Role	23	11.00%
Professional	25	11.96%
Individual Contributor	7	3.35%
Other	3	1.44%

Respondents were then asked to select their work industry. 7.18% of the participants worked in Government, 8.61% of the participants worked in Healthcare, 7.18% of the participants worked in Education, 10.53% of the participants work in Financial, 9.09% of the participants worked in Manufacturing, 13.88% of the participants worked in Retail, 11.48% of the participants worked in Services, 27.27% of the

participants worked in Technology, and 4.78% of the participants listed Other for their work industry. Table 8 shows the Work Industry distribution.

Table 8

Work Industry Distribution

Industry	Count	Percentage Ratio
Government	15	7.18%
Healthcare	18	8.61%
Education	15	7.18%
Financial	22	10.53%
Manufacturing	19	9.09%
Retail	8	13.88%
Services	24	11.48%
Technology	57	27.27%
Other	10	4.78%

Respondents were asked to select the size of their organization based on the number of employees. 1.44% of the participants had less than 100 employees in their organization, 3.35% of the participants has between 100-499 employees in their organization, 9.57% of the participants had 500-999 employees in their organization, 21.05% of the participants had 1,000-4,999 employees in their organization, 37.32% of the participants had 5,000-24,999 employees in their organization, 19.14% of the participants had 25,000 or more employees in their organization, and 8.13% of the participants listed Unknown for the size of the organization. Table 9 shows the size of the organization distribution.

Table 9

Size of the Organization

Number of Employees	Count	Percentage Ratio
Less than 100	3	1.44%
100-499	7	3.35%
500-999	20	9.57%
1000-4999	44	21.05%
5000-24999	78	37.32%
25000+	40	19.14%
Unknown	17	8.13%

Respondents were asked to select a previous Managed Security Services Provider that they have worked with in the past, if any, on other projects other than the security services provider used in this research. 20.10% of the participants indicated they received security services in the past from AT&T, 7.18% of the participants indicated they received security services in the past from Dell SecureWorks, 7.18% of the participants indicated they received security services in the past from Hewlett Packard, 18.66% of the participants indicated they received security services in the past from IBM, 18.18% of the participants indicated they received security services in the past from Symantec, 17.22% of the participants indicated they received security services in the past from Verizon, 3.35% of the participants indicated they received security services in the past from Other security services providers, and 8.13% of the participants of indicated that the previous security services provider was unknown or they had not received previous security services at all. Table 10 shows the Previous Security Services Provider distribution.

Table 10

Previous Security Service Providers

Security Provider	Count	Percentage Ratio
AT&T	42	20.10%
Dell SecureWorks	15	7.18%
Hewlett Packard	15	7.18%
IBM	39	18.66%
Symantec	38	18.18%
Verizon	40	17.22%
Other	7	3.35%
Unknown/None	17	8.13%

4.4 Confirmatory Factor Analysis Results

SmartPLS was used to generate the results of Confirmation Factor Analysis. Although other analysis program were available to the researcher, SmartPLS provides a valid and reliable means to carry on a CFA analysis (Asyraf & Afthanorhan, 2013). The

first criterion measured was factor loading for the six constructs. All indicators were greater than the .50 threshold for the initial measurement instrument, so all items were retained within the scope of factor loading. Table 11 provides the factor loading values for each of the indicators for the six constructs.

Table 11

Factor Loading for Initial Instrument

Construct	Indicator	Factor Loading
Information Asymmetry	INFO1	.764
	INFO2	.805
	INFO3	.856
	INFO4	.817
Outsourcing Contract	CONT1	.802
	CONT2	.801
	CONT3	.787
	CONT4	.831
	CONT5	.781
Moral Hazard	RISK1	.733
	RISK2	.599
	RISK3	.954
Trust	TRUST1	.795
	TRUST2	.877
	TRUST3	.880
Service Provider Effectiveness	SPE1	.818
	SPE2	.852
	SPE3	.876
	SPE4	.852
	SPE5	.827
Security Outsourcing Success	SOS1	.833
	SOS2	.795
	SOS3	.760
	SOS4	.848
	SOS5	.817
	SOS6	.800

The next criterion that was evaluated was internal consistency reliability. Some research indicates that Cronbach's alpha tends to provide a conservative measurement in PLS-SEM (Kwong & Wong, 2013) and that composite reliability should be used as a replacement (Hair, Sarstedt, Ringle & Mena, 2012). The researcher wanted to ensure rigor and proper data validation, so both methods were included in the study. Cronbach's alpha had a required value of 0.70 and higher to show reliability. All constructs within

the research model met the minimum values needed. Composite reliability also had a required value of 0.70 or higher to be considered reliable. All constructs within the research model met the minimum values needed to show reliability. All values fell within the acceptable range for both internal consistency reliability methods and establishes reliability for each latent variable. Table 12 shows the results of Internal Consistency Reliability measured with Cronbach's alpha and Composite Reliability.

Table 12

Findings of Internal Consistency Reliability

Construct	Indicator	Cronbach's Alpha	Composite Reliability
Information Asymmetry	INFO	.827	.885
Outsourcing Contract	CONT	.860	.899
Moral Hazard	RISK	.767	.835
Trust	TRUST	.810	.888
Service Provider Effectiveness	SPE	.900	.926
Security Outsourcing Success	SOS	.895	.919

The next criterion measured was convergent validity, which looks at the average variance extracted (AVE). For the AVE, the value of the construct should be above 0.50. The value for the construct Contract is 0.6417; the value for the construct Information Asymmetry is 0.6583; the value for the construct Moral Hazard is .6026; the value for the construct Security Outsourcing Success is 0.6558; the value for the construct Service Provider Effectiveness is 0.7156; the value for the construct Trust is 0.7259. All of the construct met the AVE requirements for convergent validity. Table 13 provides the (AVE) values for each construct.

Table 13

Findings of Convergent Validity

Construct	AVE Value
Information Asymmetry	.6583
Outsourcing Contract	.6417
Moral Hazard	.6026
Trust	.7259
Service Provider Effectiveness	.7156
Security Outsourcing Success	.6558

Note: AVE value is Average Variance Extracted

The next criterion measured was indicator reliability. The acceptable value is 0.70 or higher for the outer loading values. All indicator met the requirements for indicator reliability except the indicator RISK2 for the construct Moral Hazard for the initial measurement instrument. Table 14 provides the Indicator Reliability values for each of the indicators for the six constructs.

Table 14

Findings of Indicator Reliability

	CONTRACT	INFORMATION ASYMMETRY	MORAL HAZARD	SECURITY OUTSOURCING SUCCESS	SERVICE PROVIDER EFFECTIVENESS	TRUST
CONT1	.8024					
CONT2	.8019					
CONT3	.7871					
CONT4	.8315					
CONT5	.7815					
INFO1		.7641				
INFO2		.8053				
INFO3		.8561				
INFO4		.8172				
RISK1			.7224			
RISK2			.5990			
RISK3			.9602			
SOS1				.8334		
SOS2				.7959		
SOS3				.7603		
SOS4				.8481		
SOS5				.8177		
SOS6				.8007		
SPE1					.8185	
SPE2					.8528	
SPE3					.8769	
SPE4					.8527	
SPE5					.8275	
TRUST1						.7950
TRUST2						.8778
TRUST3						.8804

Note: Indicator reliability values < .70 are in red

Based on the indicator reliability results, additional analysis was performed to determine if any indicators would need to be removed. In measuring indicator reliability, the indicator RISK2 had an outer loading value of 0.5990 and did not met the preferred threshold of .70. Typically, to determine if the indicator should be removed, an outer loading relevance test should be conducted (Hair et al., 2014a) along with an evaluation of the items contribution to content validity (Hair et al., 2011). The relevance test involves deleting the indicator if its value is less than 0.40, or check to see that the AVE and composite reliability values do not meet the minimum thresholds and by deleting the indicator, AVE and composite reliability would increase above the minimum thresholds of .50 and .70 respectively. The researcher determined that because the AVE value of .6026 and the composite reliability value of .835 already meet the minimum requirements for the Moral Hazard construct, the indicator should not be removed. In reviewing the content validity of the items, the researcher determined that removing the item would have an adverse impact on the Moral Hazard Construct because its defined items represent all facets of the construct itself. Based on these findings and conclusions, the RISK2 indicator was retained.

The next criterion that was measured was discriminant validity. This is measured by comparing the outer loadings of a construct with the cross loadings of other constructs (Hair et al, 2014a) to see if they are greater than all other loadings. For each construct, all indicator values exceeded the cross loading values of all other constructs and their indicators. Based on these findings, this indicated that there were no discriminant validity issues and each construct is unique. Table 15 shows the results of the cross loadings.

Table 15

Findings for Discriminant Validity

	CONTRACT	INFORMATION ASYMMETRY	MORAL HAZARD	SECURITY OUTSOURCING SUCCESS	SERVICE PROVIDER EFFECTIVENESS	TRUST
CONT1	**0.8024**	0.5831	-0.1704	0.5813	0.6605	0.6104
CONT2	**0.8019**	0.5099	-0.1219	0.5184	0.6501	0.5246
CONT3	**0.7871**	0.5309	-0.2693	0.5685	0.6348	0.5327
CONT4	**0.8315**	0.6377	-0.2767	0.6175	0.6801	0.5933
CONT5	**0.7815**	0.5922	-0.2861	0.6569	0.6840	0.5711
INFO1	0.5000	**0.7641**	-0.3042	0.5148	0.5057	0.4847
INFO2	0.5697	**0.8053**	-0.3371	0.6020	0.5259	0.5462
INFO3	0.6371	**0.8561**	-0.2990	0.6248	0.6305	0.5913
INFO4	0.5992	**0.8172**	-0.3351	0.5548	0.5854	0.5555
RISK1	-0.1097	-0.2189	**0.7224**	-0.2095	-0.1290	-0.2487
RISK2	-0.0471	-0.2415	**0.5990**	-0.1542	-0.0238	-0.1472
RISK3	-0.3083	-0.4018	**0.9602**	-0.4370	-0.3196	-0.4199
SOS1	0.5876	0.6295	-0.4052	**0.8334**	0.6249	0.5924
SOS2	0.5567	0.5792	-0.4085	**0.7959**	0.6068	0.5179
SOS3	0.5496	0.5597	-0.4006	**0.7603**	0.5644	0.5816
SOS4	0.6495	0.6137	-0.3308	**0.8481**	0.6953	0.5988
SOS5	0.5881	0.5370	-0.2322	**0.8177**	0.6420	0.5353
SOS6	0.6352	0.5275	-0.2659	**0.8007**	0.6652	0.6052
SPE1	0.6919	0.5416	-0.2444	0.6020	**0.8185**	0.6343
SPE2	0.7055	0.6206	-0.2618	0.6280	**0.8528**	0.6670
SPE3	0.7276	0.6298	-0.2914	0.6951	**0.8769**	0.6417
SPE4	0.7051	0.5534	-0.2119	0.6761	**0.8527**	0.6031
SPE5	0.6675	0.5956	-0.2448	0.7108	**0.8275**	0.6252
TRUST1	0.5490	0.5529	-0.4403	0.5718	0.5960	**0.7950**
TRUST2	0.6217	0.5805	-0.2814	0.6066	0.6497	**0.8778**
TRUST3	0.6351	0.5866	-0.3489	0.6255	0.6678	**0.8804**

Note: Cross loading values for each construct and their associated indicators are in boldface

4.5 Summary

With the findings identified for the measurement model, the CFA analysis revealed that the initial instrument showed favorable results when subjected to factor loading, internal consistency reliability, convergent validity, indicator reliability and discriminant validity. Based on these outcomes, all 26 indicators were retained (see Figure 6). No additional analyses were needed for this phase and with a valid measurement model in place, the analysis of the structural model will be discussed in the next chapter.

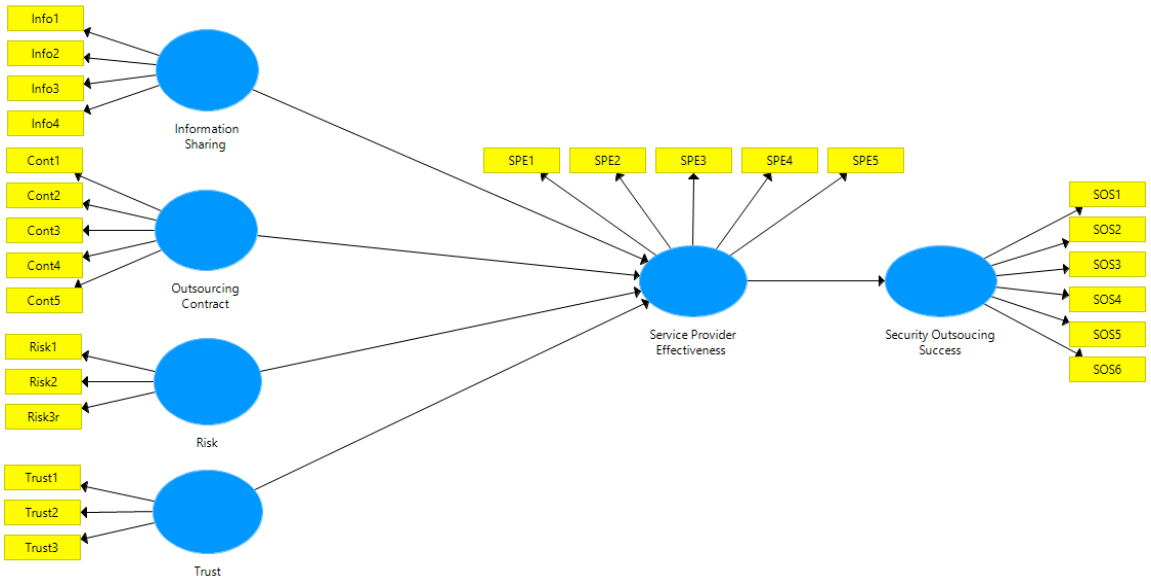

Figure 6. Research constructs and their indicators

.

Chapter 5

Structural Model Analysis and Findings

5.1 Introduction

In the previous chapter, Confirmatory Factor Analysis (CFA) techniques were used to validate the reflective measurement model. Based on the findings, the initial instrument did not require modification and will be used for the next step in the research study, which is structural equation modeling. This chapter provides a detail of the findings for the structural model. Partial Lease Squares-Structural Equation Modeling (PLS-SEM) was used for the second stage of the analysis and the selected software was SmartPLS (Ringle et al, 2015). The findings along with the SEM data will be presented and discussed.

5.2 Structural Model

As mentioned, the remaining analysis requirement is the evaluation of the structural model. The structural model contains the constructs as well as the relationship between each one (Hair et al, 2014a). For the structural model, the following assessment procedure were considered: assess the model for collinearity issues, access the significance and relevance of the relationships, assess the level of R^2 value, assess the f^2 effect size, and assess the predictive relevance of Q^2 and the q^2 effect sizes. Provided now is the level of acceptance for each category. Collinearity is measured based on tolerance levels and the variance inflation factor (VIF). If the tolerance levels are below 0.20 and (VIF) is above 5.00 for the predictor constructs, then collinearity issues exist and would need to be addressed. For the significance of the hypothesized relationships, path

coefficients range from -1 to +1 and closer to +1 indicate strong positive relationships. Also, the empirical t values (which determines the standard error) should be higher than the critical value which are 1.65 for a significance level at 10%, 1.96 for a significant level at 5%, and 2.57 for a significance level at 1. The R^2 value ranges from 0 to 1 for endogenous latent variables with the scale of 0.75 for significant, 0.50 for moderate, and 0.25 for weak. f^2 effect sizes for the exogenous latent variables are 0.02 for small effect, 0.15 for medium effect, and 0.35 for a large effect. Q^2 values larger than 0 indicate that the exogenous constructs have some level of predictive significance for the endogenous construct. q^2 values for the exogenous constructs are 0.02 for small predictive relevance, 0.15 for medium predictive relevance, and 0.35 for large predictive relevance for a certain endogenous construct.

5.3 PLS-SEM Findings

The first criterion evaluated was collinearity. If VIF is > 5.00, then collinearity problems exists. None of the constructs exceeded the 5.00 value which indicated that no collinearity issues existed. Table 16 shows the results of collinearity assessment.

Table 16

Findings of the Collinearity Assessment

Predictor Constructs	VIF Value	Collinearity Issues
Contract	2.5607	No
Information Asymmetry	2.4057	No
Moral Hazard	1.2562	No
Trust	2.4068	No
Service Provider Effectiveness	1.0000	No

The next criterion evaluated was the significance of the hypothesized relationships, which is conducted through bootstrapping. For an initial instrument, 500

random subsamples may be used, but to ensure stability of the results, a larger subsample such as 5,000 should be used for final results preparation (Hair et al, 2014a). Bootstrapping was completed with 5,000 subsamples and the path coefficients were measured for each relationship and the closer to 1, the stronger the relationship. The weakest relationship was Moral Hazard→Service Provider Effectiveness with a path coefficient of .0306 and the strongest relationship was Service Provider Effectiveness →Security Outsourcing with a path coefficient of .7842. Based on the findings of the t-values, all relationships were above the 1.96 significance level and are significant at the 5% level except Moral→SPE, which had a value of 0.8020. For the hypothesis to be supported, the P-Value should be less than .05. All relationships were below the .05 thresholds except (Moral→SPE), which had a value of .4226 and considered not significant. This concludes that 4 out of the 5 hypotheses were supported. Table 17 provides the results of the bootstrapping for the path coefficients.

Table 17

Bootstrapping results on the Path Coefficients

Relationships	Path Coefficients	T -Values	Significance Levels	P-Values
CONT➔SPE	0.5335	8.6900	***	0.0000
INFO➔SPE	0.1252	2.0327	**	0.0421
MORAL➔SPE	0.0306	0.8020	NS	0.4226
SPE➔SOS	0.7842	25.3555	***	0.0000
TRUST➔SPE	0.3002	5.0517	***	0.0000

Note: NS = not significant. *p < .10. **p < .05. ***p <.01.

The next criterion measured was the Coefficient of Determination (R^2 value). The R^2 value ranges from 0 to 1 with R^2 values being substantial at 0.75, moderate at 0.50, and weak at 0.25. The endogenous latent variables show the R^2 value of the Service Provider Effectiveness construct was .7445, which indicates a moderate level of predictive accuracy with only with just 0.0055 away from being considered substantial.

The R^2 value of the Security Outsourcing Success construct was 0.6149 which indicates a moderate level of predictive accuracy. Both measurements are closer to 1 than 0 and meet the requirements for predictive accuracy.

The next criterion measured was the f^2 effect size. This is determined when a specified exogenous construct is omitted from the model. f^2 values of 0.02 have small effect, 0.15 has a medium effect, and 0.35 has a large effect. The results show Contract with an f^2 value of .4351, Information Asymmetry has an f^2 value of 0.0249, Moral Hazard has an f^2 value of 0.0021, Trust has an f^2 value of .1449, and Service Provider Effectiveness has an f^2 value of 1.5968. These results indicate that if the Moral Hazard construct was omitted, it would have no effect on the exogenous latent variable. If the Information Asymmetry and Trust constructs were omitted, they would have a small effect on the exogenous latent variable. If the Contract and Service Provider Effectiveness constructs were omitted, they would have a large effect on the exogenous latent variable. Table 18 shows the results of f^2 effect sizes.

Table 18

Results of the f^2 effect sizes

Predictor Construct	**f^2 Value**	**Level of Effect**
Contract	0.4351	Large
Information Asymmetry	0.0255	Small
Moral Hazard	0.0029	None
Trust	0.1466	Small
Service Provider Effectiveness	1.5968	Large

The next criterion measured was Predictive Relevance or the Q^2 value. The blindfolding procedure was conducted using the default omission distance of 7 in SmartPLS. Q^2 values larger than zero for specific endogenous latent variable indicate the

path model's predictive relevance. The Service Provider Effectiveness and Security Outsourcing Success Construct had Q^2 values of 0.3999 and 0.5272 indicating both have path model predictive relevance.

The final criterion measured was the q^2 effect size of endogenous latent variables. Value range for q^2 effect size is 0.02 (small effect), 0.15 (medium effect), and 0.35 (large effect). The findings revealed that SPE →SOS had a q^2 effect size of .2174 which means it has a medium effect on predictive relevancy.

This concludes the analysis of the structural model and the hypothesis findings will be discussed. In this research study, there were five proposed hypothesis and four out of the five hypotheses were supported. Table 19 provides the results of the proposed hypotheses.

Table 19

Findings of the Proposed Hypotheses

Hypotheses	Relationship	Supported
H1	Higher information sharing leads to an increase in Service Provider Effectiveness	Yes
H2	The better the outsourcing contract, the higher Service Provider Effectiveness	Yes
H3	A lower level of risk for IT security services leads to an increase in Service Provider Effectiveness	No
H4	An increase in trust leads to an increase in Service Provider Effectiveness	Yes
H5	Higher Service Provider Effectiveness leads to an increase in Security Outsourcing Success	Yes

5.4 Alternative Model

For this research, the testing of an alternative model was not completed and not necessary. Unlike CB-SEM, PLS-SEM provides all the required data to properly interpret the model and determine how well the model fit for the research study. Jackson (2007)

stated that direct measures of fit are more prone to model misspecification that other fit indices. This research did not leverage fit indexes to determine model fit, but analyzed the measurement model for the first stage of the study with other recommended factors in PLS-SEM such as factor loading, internal consistency reliability, convergent validity and discriminant validity Hair et al., (2012; 2014a). The use of an alternative model or model modification should be guided carefully and have theoretically meaning (Baumgartner & Homburg, 1996). Without this consideration, Shreiber et al. (2006) stated that model modification now becomes exploratory in nature and increases the chances of a Type 1 error.

5.5 Summary

With the findings identified for the structural model, the PLS-SEM analysis revealed that the final instrument had no collinearity issues, and showed favorable results for the research model. Based on the outcome, 4 out of the 5 hypotheses were supported. Chapter 6 provides a discussion and the overall findings of the study.

Chapter 6

Discussion and Conclusion

6.1 Introduction

This chapter provides an overall summation of the findings, contribution to research, limitations, future research and finally a conclusion to the research study. The purpose of this research study was to identify key determinants of service provider effectiveness and the effect that it has out security outsourcing success. The foundation of the study was to understand the needs of the customer and what they deem as an effective security services provider.

6.2 Findings

The research model for this study was based on Agency Theory. Agency is based on the premise of understanding and addressing the principal-agent challenges that exist in outsourcing arrangements (Eisenhardt, 1989). Based on previous studies, several key constructs were selected to address the research problem, which included Information Asymmetry, Contract, Moral Hazard, and Trust as the independent variables, Security Outsourcing Success as the dependent variable and Service Provider Effectiveness as a mediation variable.

For all constructs, there were a combined total of 26 indicators that were analyzed through CFA and PLS-SEM with SmartPLS. Based on the finding for the measurement model, the CFA analysis revealed no issues with factor loading, composite reliability, convergent validity, or discriminant validity. Given these findings, all indicators met the minimum threshold requirements and all were retained for this first phase of the study.

The second phase of the study involved the evaluation of the structural model. The findings showed no issues with collinearity and revealed the model's predictive accuracy and overall significance.

There were five hypotheses proposed for this research and a summary has been provided:

- H1: An increase in the level of information sharing leads to an increase in service provider effectiveness
- H2: The better the outsourcing contract agreement, the higher the service provider effectiveness
- H3: A lower level risk for IT security services leads to an increase in service provider effectiveness
- H4: An increase in trust between the customer and the service provider leads to an increase in service provider effectiveness
- H5: Higher service provider effectiveness leads to an increase in security outsourcing success

Hypothesis H1 was supported which indicated that when organizations have better information sharing and information symmetry, this leads to an increase in service provider effectiveness. This reiterated how important information sharing is and how value is created between the customer and the service provider (Rollins, Pekkarinen, & Mehtala, 2011). Hypothesis H2 was supported which indicated that when a good contract agreement exists, the higher the service provider effectiveness. Within this study, the scope of the contract was not just the legal agreement or the formal agreement, but also the informal agreement made up of the relationship that exists between both parties. Barthelemy (2003) indicated that while a good formal contract is vital, it alone does not ensure success. Hypothesis H3 was not supported within this study, which possibly indicated that customers might not view Moral Hazard as an indication of risk if a relationship is already in place with the Managed Security Service Provider. Another possible reason for its lack of support could be because some of the survey questions

were listed in reverse order and that may have caused clarity issues for the participants when completing the survey. Hypothesis H4 was supported which indicated that an increase in trust between the customer and the service provider leads to higher service provider effectiveness. Trust is critical to any outsourcing relationship (Logan, 2000) and Billhardt, Hermoso, Ossowski, and Centeno (2007) asserted that a customer's reputation along with trust could help decide on selecting the best service provider. Hypothesis 5 was supported which indicated that higher service provider effectiveness leads to higher security outsourcing success. Grover Cheon and Teng (1996) deem success as key benefits being attained and with an effective service provider, the probability of achieving this would be higher.

6.3 Contribution to Research

This study has been empirically validated and identified key determinants that can make a service provider effective while increasing security outsourcing success. This research is one the early attempts to uncover the connection between key factors of service provider effectiveness and security outsourcing success. Because of the pervasive use of technology, organizations have become critically dependent on IT (Bahl & Wali, 2014). Through the context of information security, the research model and the findings helped address the original problem statement identified in Chapter 1.

There were several key items this study contributed to information security research. The first contribution of this study is a validated model for information security outsourcing success. Past studies have looked at single or minimal factors that have affected outsourcing success such as knowledge and information sharing (Lee, 2001), formal contract (Poppo, 2002), trust (Lee, Huynh, & Hirschheim, 2008), and moral

hazard (Lee, Geng, & Raghunathan, 2013). This only reveals a limited scope of factors as opposed to the key determinants that were identified in this research to help better understand outsourcing success. This research model can be used in future studies to further explain outsourcing challenges and how these issues can be mitigated.

Another contribution of this research is the emphasis on the importance of symbiotic relationships. In an outsourcing arrangement, symbiosis can positively influence security outsourcing success and the overall relationship between the principal and the agent. Many studies have discussed methods of finding the appropriate service provider and what to look for in a service provider. Ring and Van de Ven (1992) discussed a cooperative relationship and Lacity, Willcocks, & Feeny (1996) mentioned the value of selective outsourcing and total outsourcing with key relational factors (Barthelemy & Geyer, 2004). Although these studies provide value and help identify specific areas that promote outsourcing success, they do not reveal the effectiveness of service providers and their benefit to customers. A lack of commitment to a symbiotic relationship between the customer and the outsourcing service provider can have an adverse on the outsourcing arrangement (Bhagat, Byramjee, & Taiani, 2010). There are numerous factors that determine the success of an outsourcing relationship (Bahl & Wali, 2014), but having a symbiotic relationship helps between both parties helps promote higher mutualistic interests.

Another contribution to research is the introduction and establishment of a new mediating construct for effectiveness. The success of outsourcing is directly related to effectiveness (Dean & Kiu, 2002) and should be strongly considered in future studies. Depending on the scope of the study, Service Provider Effectiveness (SPE) can be

associated to Security Outsourcing Success, as conducted in the research study, or can be listed as Security Service Provider Effectiveness (SSPE) and outsourcing success. This research uncovered the importance of service provider effectiveness and how it can be leveraged with key factors of security outsourcing and outsourcing success. Wheeler (2008) associated a decision of effectiveness as dichotomous outcome: effective or ineffective. Given this conclusion, this would help explain why many outsourcing arrangements fail. As noted by Hui, Hiu, and Yue (2012), there is no guarantee of a high quality of service from a Managed Security services provider, so knowing how effective a service provider is prior to entering into an outsourcing arrangement can be vital in the early decision-making process.

A final contribution of the study was the attainment and use of 209 unique organizations that completed the survey. Acquiring data at the individual level through convenience sampling would have provided a myopic view of an organization's true perspective toward this study. The researcher went through a diligent process of qualifying the appropriate candidates to participate in the survey. This allowed for a more rigorous and thorough study and a better representation of the population regarding security outsourcing.

6.4 Limitations

Although this study has proven to provide a contribution to Information Security research, there are several limitations to that may need to be addressed. The first limitation is the security services received for each survey participant all came from the same security services provider. To become more generalizable, efforts should be made to survey customers who have dealt with multiple security services provider other than

just the single provider indicated in this research. Other research may contend that the use of a single provider may limit success depending on the services that are outsourced. Nevo and Kotlarsky (2014) postulated that multiple service providers could work together to pool resources and expertise, known as crowdsourcing, as a way to offer services to customers and help reduce permanent staff levels. Jarvenpaa and Mao (2008) discussed the benefits of a mediation outsourcing model in which a primary vendor works with the customer directly and other service providers provide sub-contracting to the primary vendor.

Another limitation to this study is the lack of identification of specific security services. This research cast a broad description around the information security services that were received from a security services provider, but details should be uncovered to determine the specific type of security services received. For example, if a customer received cloud security services, the outcome may be different if a service provider was providing different security services, such as firewall, network or a specific type of intrusion detection. This is important because each security services offering may have their own service level agreement (SLA) requirements. The SLA typically guarantees a certain level of performance, defines the basis of the outsourcing relationship and regulates the outsourcing arrangement (Karyda, Mitrou, & Quirchmayr, 2006).

Another limitation is this study is no industry segmentation or comparison. Demographic information for work industry was captured for the 209 organizations (see Table 8, but comparisons were not made between each work industry for the scope of this research. The outsourcing needs for healthcare organizations may be different for those firms in retail, but may align closely to technology or other services industries. Having a

better understanding of what services are being offered, the degree of outsourcing success, and the comparison between industries could invoke better insight into specific needs and requirements for organizations.

A final limitation of this study is the use of Agency Theory. As mentioned in the Chapter 3, there are many studies that associate specific theories to outsourcing. From the early stages of outsourcing up until now, cost savings are usually factored into the decision-making process. (Mclvor, 2009) presented the importance of Transaction Cost Economics and Resource-based View theory and their value to understanding outsourcing on transaction-specific investments and asset specific investments. Also, there is the belief that a single theory, despite its perspective, cannot fully explain the true nature of outsourcing (Poppo & Zenger, 1998).

6.5 Future Research

Future research should look to identify, report, and compare the different security offerings of service providers to better understand the impact of service level agreements (SLAs) and how each service affect the customer's business holistically. Although experts should handle security issues, many firms may be discouraged to outsource for fear of losing control over their systems (Karyda et al., 2006). This perception of lost control could differ from one security service to another. Also, a security service provider may be considered an expert, but their level of expertise may be stronger in some areas and weaker in others.

Another consideration for future research is how a service provider would select an effective customer. This research study focused on service provider effectiveness and what effectiveness means from the customer's perspective. Customers are looking to

establish that symbiotic relationship with their service provider. Service providers should take the same care in identifying what makes an effective customer to possibly solicit and offer services. Mutualistic interest should be ethically considered before entering into a contract between two parties, but service providers should be able to determine if a customer is a potential risk and likely to cause liability issues in the future.

Another consideration for future research is to compare multiple security service providers to understand the impact and degree of future outsourcing security success. Demographic information was gathered on identifying previous security service providers that customers have worked with (see Table 10) other than the service provider in this study. This type of information can be used to help compare quality of service, previous challenges, and how each security provider faired in a specific category, such as satisfaction, and planned future use of security outsourcing. Customer may not be aware that some or all security services provided by a security services provider may be sub-contracted based on business needs.

A final consideration for future research is to apply this research model across specific business industries. As mentioned earlier in this chapter, work industries may have different security services requirements, but what about organizations within the same business segments? Most healthcare organizations adhere to the same governing laws on compliance and regulations, but when it comes to outsourcing, a technology organization may not be subjected to the same stringent rules. Understanding and comparing the business requirements for security outsourcing within business industries could help explain similar challenges and provide a better mechanism of increasing

higher outsourcing success. Each of these considerations mentioned can help add to the information security body of knowledge.

6.6 Conclusion

The purpose of this research study was to identify key determinants of service provider effectiveness and the effect that it has on outsourcing success. The results of this research present empirical facts that supported several of the proposed hypothesis and contributes to a better understanding of effectiveness, security services, and outsourcing success. This foundational research will help service providers and customers better understand each other's needs and expectations.

Through the use of Agency Theory, researchers now have empirical data at the organizational level that provided key determinants and the degree to which these factors impact the effectiveness of security services and outsourcing success. The context of the study was driven by information security, but can be applied to other domains of information systems or other areas of research. The details and the findings were empirically validated and analyzed through the use of confirmatory factor analysis (CFA) for the measurement model and partial lease square-structural equation modeling (PLS-SEM) for the structural model. These analysis techniques were well suited for this research by providing the proper validation needed to uncover the key findings. This research study has built on existing empirical studies in hopes of fostering further discussions in the field of information security.

Appendix A

Table A1

Survey Questions for the Research Instrument

Construct	Indicator	Survey Questions	References
Information Asymmetry	Information Sharing	We and our security services provider share each other's information	Swar et al, 2012
		We and our security service provider share business knowledge of core business process related to security	Swar et al, 2012
		Information provided by us helps our security service provider's business execution	Swar et al, 2012
		We and our security service provider share information regarding business environment and technical change that affect each other's business	Swar et al, 2012
Outsourcing Contract	Contract Management	I feel we have a good contract management process in place with our security service provider	Qi et al, 2012
		I feel that our contract contains clear and concise requirements for our security service provider	Qi et al, 2012
		I feel that if a contract dispute arose, we would be able to address it with our security service provider	Qi et al, 2012
	Formal Contract	The extent to which the contact precisely defines the expected performance	Barthelemy, 2003
		The extent to which the contract takes as many elements as possible into account	Barthelemy, 2003
		The extent to which the contract is well balanced between the parties	Barthelemy, 2003
Moral Hazard	Risk	I feel that we are at risk with our current outsourcing arrangement with our security service provider	Aubert, 2005
		I feel that we may incur hidden costs with our current security service provider	Aubert, 2005
		I feel that we share equal risk with our current security service provider in our outsourcing arrangement	Aubert, 2005
Trust	Trust	The security service provider makes beneficial decision to us under any circumstances	Goo et. al, 2009
		The security service provider is sincere at all times	Goo et. al, 2009
		The security service provider has always provided us a completely truthful picture of the relevant IT security services	Goo et. al, 2009
Service Provider Effectiveness	Service Quality	I feel that our security service provider is meeting the expectations of the outsourcing arrangement	Grover et al, 1996
		I feel that our security service provider is managing our security service as expected	Grover et al, 1996
		I feel that our security service provider understands our security objectives and requirements	Grover et al, 1996
		Our security service provider is meeting the service level agreements listed in the outsourcing contract	Grover et al, 1996
		Our security service provider is delivering a high quality of service	Grover et al, 1996

Table A1 Continued

Construct	Indicator	Survey Questions	References
Security Outsourcing Success	Net Benefits	We have enhanced out IT security competence	Grover et al, 1996
		We have increased our access to skilled security personnel	Grover et al, 1996
		We have increased control of IS security management	Grover et al, 1996
		We have increased our access to key security technologies	Grover et al, 1996
		We have reduced our security risk through this outsourcing arrangement	Grover et al, 1996
		We are satisfied with our overall benefits (results) from the security outsourcing project	Grover et al, 1996

Appendix B

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: James B. Lewis

From: Ling Wang, Ph.D.
Institutional Review Board

Date: Dec. 3, 2014

Re: *Identifying Key Determinants of Service Provider Effectiveness and its Impact on Outsourced Security Success*

IRB Approval Number: wang12151401

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

Appendix C

Sample Email Request to Participate in Internet Survey

From: James B. Lewis, Ph.D. Candidate at Nova Southeastern University

To: Potential Survey Candidate for Information Security Research

I am writing to you to request your participation in an important survey. More organizations are looking to outsource their security services (firewalls, intrusion detection, network and perimeter threats, end point security, etc.). Before entering into a legal agreement with any external service provider, there should be a mechanism in place to determine their effectiveness in delivering these services with the highest level of quality, trust, and competency for both the formal and informal (relationship) contract.

Your feedback from this survey will help us to identify key determinants of an effective service provider and how these findings can help with overall outsourcing success of information security services.

To be considered for this survey, the potential survey recipient should have a basic understanding of the contract and outsourcing arrangements that were made with [security services provider] and can provide feedback about their performance, quality of work, and overall experience during the contract period.

The survey link is https://www.surveymonkey.com/s/XXXXXX
Please note that this website is secure and all content within the survey is private and will not be released to anyone other than the researcher and his research committee.

This brief survey should take approximately 10-15 minutes to complete. While the survey participant can opt-out at any time, to ensure maximum quality and thoroughness, the researcher is kindly requesting that all surveys be completed in their entirety.

Your participation in this survey is completely voluntary and all responses will be kept confidential. The survey participant will be anonymous and no personally identifiable information will be disclosed

By completing and submitting this survey, as a participant, you are providing your informed consent

Should there be any questions about this survey, please feel free to contact the researcher directly at jamelewi@nova.edu. All email correspondence will remain confidential as well.

Thank you in advance for taking the time to complete this survey and we hope to help improve the success of future outsourcing arrangements

Sincerely,

James B. Lewis

References

Abdi, H., & Williams, L. J. (2010). Principal component analysis. *WIREs Comp Stat, 2(*4), 433–459.

Albers, S. (2009). PLS and success factor studies in marketing. In V. Esposito Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds). *Handbook of partial least squares: Concepts, methods, and applications*. Berlin: Springer.

Alchian, A. A., & Demsetz, H. (1972). Production, information costs, and economic organization. *American Economic Review, 62(*5), 777-795.

Allen, J., Gabbard, D., & May, C. (2003). Outsourcing managed security services. *Software Engineering Institute* (Technical Report 600), 1-122.

Anastasi, A. (1988). *Psychological testing.* New York, NY: Macmillan.

Anderson, J., & Narus, J. (1990). A model of distributor firm and manufacturer firm working partnerships. *Journal of Marketing, 54(*1), 42–58.

Anderson, R. (2001). *Why information security is so hard – an economic perspective.* Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC 2001), New Orleans, Louisiana, USA.

Asyraf, W. M., & Afthanorhan, B. W. (2013). A comparison of partial lease square structural equation modeling (PLS-SEM) and covariance based structural equation modeling (CB-SEM) for Confirmatory Factor Analysis. *International Journal of Engineering Science and Innovative Technology, 2(*5), 198-205.

Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. *ACM SIGMIS Database, 36(*4), 9-28.

Babbie, E. R., (1990). *Survey Research Methods*, Wadsworth, Belmont: Wadesworth Publishing.

Bagaya, M. H. (2007). *An analysis of IT/IS offshore outsourcing: Educator perspectives.* (Doctoral dissertation). Retrieved from ProQuest Digital Dissertations. (UMI Number: 3258386).

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16(*1), 74-94.

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: A transaction cost and agency theory-based perspective. *Journal of Information Technology, 18*(3), 211-221.

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in the software service industry. *Information Management & Computer Security, 22*(1), 2-23.

Bakari, J. K., Magnusson, C., Tarimo, C. N., & Yngstrom, L. (2006). *Outsourcing ICT security to MSSP: Issues and challenges for the developing world.* Proceedings of the Information Security South Africa (ISSA) Conference, Johannesburg, South Africa.

Barney. J. B., Hesterly, W., (1996). Organizational Economics: Understanding the relationship between organizations and economic analysis, In Clegg, S. R., Hardy C., & Nord W. R. (Eds.). *Handbook of Organization Studies*. London: Sage Publications.

Barthelemy, J., & Geyer, D. (2004). The determinants of total IT outsourcing: An empirical investigation of French and German firms. *Journal of Computer Information Systems, 44*(3), 91-97.

Barthelemy, J. (2003). The hard and soft sides of IT outsourcing management. *European Management Journal, 21*(5), 539-548.

Baumgartner, H., & Homburg, C. (1996). Applications of structural equation modeling in marketing and consumer research: A review. *International Journal of Research in Marketing, 13(*2), 139–161.

Beaumont, N., & Sohal, A. 2004. Outsourcing in Australia. *International Journal of Operations & Production Management, 24*(7), 688-700.

Billhardt, H., Hermoso, R., Ossowski, S., & Centeno, R. (2007). *Trust-based service provider selection in open environments.* Proceedings of the 2007 ACM symposium on Applied Computing, New York, NY, USA, 1375-1380.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94.

Bryant, F.B., Yarnold, P.R., & Michelson, E. A. (1999). Statistical methodology: VIII. Using confirmatory factor analysis (CFA) in emergency medicine research. *Academic Emergency Medicine*, *64(*1), 54-66.

Bryant, F.B., & Yarnold, P.R. (1995). Comparing five alternative factor-models of the student Jenkins Activity survey: Separating the wheat from the chaff. *Journal of Personality Assessment*, *64*, 145-158.

Burnett, H. L., & Williams, L. J. (2005). Structural equation modeling (SEM): An introduction to basic techniques and advanced issues. In Swanson, R. A., Holton III, E. F. (Eds), *Research in organizations: Foundations and methods of inquiry,* (pp. 143-160). San Francisco, CA: Berrett-Koehler Publishers, Inc.

Caldwell, B. (2002*)*. Trends in IT outsourcing delivery, solution development, marketing, sales and alliances. Retrieved from https://www.gartner.com/doc/352044/-trends-it-outsourcing-delivery.

Cezar, A. Cavusoglu, H., & Raghunathan, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science, 60(*3), 638-657.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106(*3), 345-361.

Chang, K-C., & Wang, C-P. (2011). Information systems resources and information security. *Information Systems Frontier, 13(*4), 579-593.

Child, D. (1990). *The essentials of factor analysis*, (2nd Ed). London, England: Cassel Educational Limited.

Chou, T-C., & Huang, M-Y. (2011). Understanding the role of business ecosystems in large public IT infrastructure project development: The case of M-Taipei. *International Journal of Information Management, 32(*1), 88-92.

Clarke, R. (2010). *User requirements for cloud computing architecture.* Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud, and Grid Computing, Melbourne, Australia.

Clarkson, G., Jacobsen, T. E., & Batcheller, A. L. (2007). Information asymmetry and information sharing. *Government Information Quarterly, 24*, 827-839.

Cohen, J. (1988), *Statistical Power Analysis for the Behavioral Sciences*. Mahwah, NJ: Lawrence Erlbaum.

Comrey, A. L., & Lee, H. B. (1992). *A first course in factor analysis*, Hillsdale, New Jersey: Erlbaum.

Conway, J. M., & Huffcutt, A. I. (2003). A review and evaluation of exploratory factor analysis practices in organizational research. *Organizational Research Methods, 6*(2), 147-168.

Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research, & Evaluation, 10*(7), 1-9.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative and mixed methods approaches (3rd ed).*Thousand Oaks, CA: Sage Publications, Inc.

Cudeck, R. (2000). Exploratory Factor Analysis. In Tinsley, H. E., Brown, D. (Eds), *Handbook of applied multivariate statistics and mathematical modeling,* (pp. 265-296). San Diego,

CA: Academic Press.

Cullen, S., & Willcocks, L. 2003. *Intelligent IT outsourcing: eight building blocks to success*. Oxford:Butterworth-Heinemann.

Curran, P. J., West, S. G., & Finch, J. F. (1996). The robustness of test statistics to nonnormality and specification error in confirmatory factor analysis. *Psychological Methods*, *1*, 16-29.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Journal of Computers & Security, 29(*2), 196-207.

Davis, G. B. (2006). Information systems as an academic discipline: Looking back, looking forward, and ensuring the future. In D. Avison, S. Elliot, J. Krogstie, J. Pries-Heje (Eds), *The Past and Future of Information Systems: 1976-2006 and Beyond*, (pp. 11-25). Boston, MA: Springer.

Dean, A., & Kiu, C. (2002). Performance monitoring and quality outcomes in contracted services. *The International Journal of Quality & Reliability Management, 19(*4), 396-413.

Debar, H., & Viinikka, J. (2006). Security information management as an outsourced service. *Information Management & Computer Security, 14*(5), 417-435.

Demchenko, Y., de Laat, C., & Lopez, D. R. (2010). *Security services lifecycle management in on-demand infrastructure services provisioning.* Proceeding of the 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, Indiana, USA.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communication of the ACM, 43(*7), 125-128.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information security in organizations. *Information Systems Journal, 16(*3), 293-314.

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilka, B. (2004). Information systems outsourcing: A survey and analysis of the literature. *The Database for Advances in Information Systems, 35(*4), 1-97.

Ding, W., & Yurcik, W., & Yin, X. (2005). Outsourcing Internet security: Economic analysis of incentives for managed security service providers. *First International Workshop on Internet and Network Economics,* Hong Kong, China, 947-958.

Ding, W., & Yurcik, W. (2005a). A game theoretic economics framework to understanding information security outsourcing market. Retrieved from http://arxiv.org/pdf/cs/0506038v1.pdf.

Ding, W., & Yurcik, W. (2005b). *Outsourcing Internet security: The effect of transaction costs on managed service providers*. Proceedings of the International Conference on Telecommunication Systems-Modeling and Analysis, Dallas, TX.

Domberger, S., Fernandez, P., & Fiebig, D. G. (2000). Modelling the price, performance and contract characteristics of IT outsourcing. *Journal of Information Technology, 15(2*), 107-118.

Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31(*2), 134-149.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review, 14(*1), 57-74.

Endorf, C. (2004). Outsourcing Security: The need, the risks, the providers, and the process. *Information Systems Security, 12*(6), 17-23.

Farrell, A. M., & Rudd, J. M. (2009). *Factor Analysis and Discriminant Validity: A Brief Review of Some Practical Issues*. Proceedings of the Australia-New Zealand Marketing Academy Conference (ANZMAC), Melbourne, Australia.

Feurer, R., Chaharbaghi, K., Weber, M., and Wargin, J. (2000). Aligning strategies, processes, and IT: A case study. *Information Systems Management*, *17*(1), 23-34.

Fitzgerald, G., & Willcocks, L. (1994*). Contracts and partnerships in the outsourcing of IT.* Proceedings of the International Conference on Information Systems, Vancouver, British Columbia, pp. 91-98.

Fornell, C., & Larcker, D.F., (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gefen, D., Straub, D. W., & Boudreau, M. –C. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communication of the Association for Information Systems, 4(*7), 1-78.

Gewald, H. & Helbig, K. (2006). *A governance model for managing outsourcing partnerships: A view from practice* Paper presented at the Proceedings of the 39thth Annual Hawaii International Conference on System Sciences, Honolulu, Hawaii, USA.

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficients for Likert-type scales.* Proceedings of the Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, Columbus, OH, USA.

Goles, T. (2005). Information systems outsourcing relationship factors: Detailed conceptualization and initial evidence. *The DATA BASE for Advances in Information Systems, 36(*4), 47-68.

Gonzalez, R., Gasco, J., & Llopis, J. (2005). Information systems outsourcing success factors: A review and some results. *Information Management & Computer Security, 13*(5), 399-418.

Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2009). The role of service level agreements in relational management of information technology outsourcing: An empirical study. *MIS Quarterly, 33(*1), 119-145.

Goo, J., & Nam, K. (2007). *Contracting as a source of trust – Commitment in successful IT outsourcing relationship: An empirical study.* Proceedings of the 40th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, USA.

Gorla, N., & Lau, M. B. (2010). Will negatives experiences impact future IT Outsourcing? *The Journal of Computer Information Systems, 50*(3), 91-101.

Grover, V., Cheon, M. J., & Teng, J. T. C. (1996). The effect of service quality and partnership on the outsourcing of information systems functions. *Journal of Management Information Systems, 12*(4), 89-116.

Gupta, A., & Zhdanov, D. (2012). Growth and sustainability of managed security services networks: An economic perspective. *MIS Quarterly, 36*(4), 1109-1130.

Guttman, B., Roback, E. A. (1995). *An introduction to computer security: The NIST Handbook* (NIST Publication 800-12). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

Haenlein, M., & Kaplan, A. M. (2004). A beginner's guide to partial least squares analysis. *Understanding Statistics, 3(*4), 283-297.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014a). *A primer on partial least squares structural equation modeling (PLS-SEM).* Thousand Oaks: SAGE.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19(*2), 139-151.

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014b). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review, 26(*2), 106-121.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science, 40(*3), 414-433.

Hamilton, S., & Chervany, N. L. (1981). Evaluating information system effectiveness – Part 1: Comparing evaluation approaches. *MIS Quarterly, 5*(3), 55-69.

Henseler, J., Ringle, C., & Sinkovics, R. (2009). The Use of Partial Least Squares Path Modeling in International Marketing. *Advances in International Marketing, 20*, 277-319.

Hirschheim, R., & Dibbern, J. (2002). Information systems outsourcing in the new economy – An introduction. In Hirschheim, R., Heinzl, A, Dibbern, J. (Eds), *Information Systems Outsourcing: Enduring Themes, Emergent Patterns and Future Directions,* (pp. 3-23). Berlin: Springer.

Hirschheim, R., & Lacity, M. (1997) *Information systems outsourcing and insourcing: Lessons and experiences.* Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Brisbane, Australia.

Holton, E. F. III, & Burnett, M. J. (2005). *The basics of quantitative research*. In Richard A. Swanson and E. F. Holton III (Eds.) Research in Organizations: Foundations and Methods of Inquiry, San Francisco, CA: Berrett-Koehler Publishers.

Holtzman, S., & Vezzu, S. (2011). *Confirmatory factor analysis and structural equation modeling of noncognitive assessments using PROC CALI.* Proceedings of the Northeast SAS Users Group, Portland, ME, USA.

Holmstrom, B. (1979). Moral hazard and observability. *The Bell Journal of Economics, 10*(1), 74-91.

Hsu, C., Wu, C., & Peng, K. (2005). *Exploring constructs and indicators influencing information system outsourcing performance in Taiwan's market.* Proceedings of ICSSSM '05 2005 International Conference on Services Systems and Service Management, Chongquing, China.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic Management Journal, 20*(2), 195–204.

Infinedo, P. (2008). Impact of business vision, top management support, and external expertise on ERP success. *Business Process Management Journal, 14(*4), 551-568.

Jackson, D. L. (2007). The effect of the number of observations per parameter in misspecified confirmatory factor analytic models. *Structural Equation Modeling, 14(*1), 48–76.

Jarvenpaa, S. L., & Mao, J. Y. (2008). Operational capabilities development in mediated offshore software services models. *Journal of Information Technology, 23(*1), 3-17.

Jenkins, G. D. Jr., &Taber, T. D. (1977). A Monte Carlo study of factors affecting three indices of composite scale reliability. *Journal of Applied Psychology*, *62*(4), 392-398.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3(*4), 305-360.

Josang, A., Ismail, R., & Boyd, Collin, A. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43(*2), 618-644.

Josang, A. (1996). *The right type of trust for distributed systems.* Proceedings of the 1996 Workshop on new security paradigms, New York, NY, USA, 119-131.

Kahraman, C., Engin, O., Kabak, & Kaya, I. (2009). Information systems outsourcing decisions using a group decision-making approach. *Engineering Applications of Artificial Intelligence, 22*(6), 832-841.

Karten, N. (2004). With service level agreements, less is more. *Information Systems Management*, *21*(4), 43–44.

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security, 14*(5), 402-415.

Kavcic, K., & Tavcar, M. I. (2008). Planning successful partnership in the process of outsourcing. *Kybernetes, 37*(2), 241-249.

Kelter, K., & Walstrom, J. (1993). The outsourcing decision. *International Journal of Information Management, 13*(6), 449-459.

Ketler, K., & Willems, J. R. (1999). *A study of the outsourcing decision: Preliminary results.* Proceedings of the 1999 ACM SIGCPR Conference on Computer Personnel Research. New York, NY, USA, 182-189.

Kern, T., & Blois, K. (2002). Norm development in outsourcing relationships. *Journal of Information Technology, 17*(1), 33-42.

Kern, T., & Willcocks, L. (2000). Exploring the relationship in information technology outsourcing: Theory and practice. *Journal of Strategic Information Systems, 9*(4), 321-350.

Kern, T., & Willcocks, L. (2002). Exploring the relationship in information technology outsourcing: the interaction approach. *European Journal of Information Systems, 11*(1), 3-19.

Khidzir, N. Z., Mohamed, A., & Arshad, N. H. H. (2010). *Information security risk management: An empirical study on the difficulties and practices in ICT outsourcing.* Proceedings of the 2010 Second International Conference on Network Applications, Protocols, and Services, Alor Setar, Kedah, Malaysia.

Kim, G., Kim, S., & French, A. M. (2013). *What increases firms' performance of information security management and the role of regulatory pressure*? Proceeding of the Pacific Asia Conference on Information Systems, Jeju Island, Korea.

Klepper, R., & Jones, W. O. (1998). *Outsourcing information technology, systems, and services.* Englewood cliffs, NJ: Prentice-Hall.

Kline, R. B. (2011). *Principles and practices of structural equation modeling (3rd ed)*. New York, NY: The Guilford Publications, Inc.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K., Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. *International Journal of Information Security and Privacy, 1*(2), 37-60.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Journal of Computers & Security, 28*(7), 493-508.

Koh, C., Ang, S., & Straub, D. W. (2004). IT outsourcing success: A psychological contract perspective. *Information Systems Research, 15*(4), 356-373.

Koh, C., Tay, C., & Ang, S. (1999). *Managing vendor-client expectations in IT outsourcing: A psychological contract perspective*. Proceeding of the ICIS 20th International Conference on Information Systems, Charlotte, NC, USA, 512-517.

Kumbakara, N. (2008). Managed IT services: The role of IT standards. *Information Management & Computer Security, 16*(4), 336-359.

Kwong, K., & Wong, K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24,* 1-32.

Lacity, M. C., Hirschheim, R., & Willcocks, L. (1994). Realizing outsourcing expectations. *Information Systems Management, 11(*4), 7-18.

Lacity, M. C., & Hirschheim, R. (1993). The information systems outsourcing bandwagon, *Sloan Management Review, 35(*1), 73-86.

Lacity, M.C., Willcocks, L. and Feeny, D. (1996). The value of selective IT outsourcing, *Sloan Management Review* Spring, 13–25.

Lacity, M.C., & Willcocks, L. (1998). An empirical investigation of Information Technology sourcing practices: Lessons from experience, *MIS Quarterly, 22(*3), 363-408.

Lacity M., & Willcocks L. (1995). Interpreting Information Technology sourcing decisions from a Transaction Cost Perspective: Findings and Critique, *Accounting, Management and Information Technology*, *5(*3/4), 204-244.

Lee, C. H., Geng, X., & Raghunathan, S. (2013). Contracting information security in the presence of double moral hazard. *Information Systems Research, 24*(2), 295-311.

Lee, J. -N., Huynh, M. Q., & Hirschheim, R. (2008). An integrative model of trust on IT outsourcing: Examining a bilateral perspective. *Information Systems Frontier, 10*(2), 145-163.

Lee, J. -N., & Kim, Y. -G. (1999). Effect of partnership quality on IS outsourcing: Conceptual framework and empirical validation. *Journal of Management Information Systems, 15*(4), 29-61.

Lee, Y. W., Pipino, L., Strong, D. M., & Wang, R. Y. et al. (2004). Process-embedded data integrity. *Journal of Database Management, 15*(1), 87–103.

Lehner, F., & Haas, N. (2010). Knowledge Management Success Factors – Proposal of an empirical research. *Journal of Knowledge Management, 8(*1), 79-90.

Levina, N., & Ross, J. W. (2003). From the vendor's perspective: Exploring the value proposition in information technology outsourcing. *MIS Quarterly 27*(3), 331-364.

Litwin, M. S. (1995) *How to measure survey reliability and validity.* Thousand Oaks, CA: SAGE Publications.

Livingston, D. (1992). Outsourcing: Looking beyond the price tag. *Datamation, 38*(23), 93-97.

Logan, M. S. (2000) Using agency theory to design successful outsourcing relationships. *International Journal of Logistics Management*, *11*(2), 21-32.

Loh, L., & Venkatraman, N. (1992) Determinants of information technology outsourcing: A cross-sectional analysis. *Journal of Management Information Systems*, 9(1), 7-24.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

Masters, G. N. (1985). Common-person equating with the Rasch model. *Applied Psychological Measurement, 9*(1), 73-82.

McCormack, B. & Hill, E. (1997). *Conducting a survey: The SPSS Workbook.* Boston, MA: International Thomas Business Press.

McFarland, F. W., & Nolan, R. L. (1995). How to manage an IT outsourcing alliance. *Sloan Management Review, 36*(2), 9-23.

McIvorf, R. R. (2009). How the transaction cost and resource-based theories of the firm inform outsourcing evaluation. *Journal of Operations Management, 27*(1), 45-63.

Mohammad, W., & Afthanorhan, B. W. (2013). A comparison of partial least square structural equation modeling (PLS-SEM) and covariance based structural equation modeling (CB-SEM) for confirmatory factor analysis. *International Journal of Engineering Science and Innovative Technology, 2*(5), 198-205.

Nasiopoulos, K., D, Sakas, D. P., Sakas, & Vlachos, D. S. (2014). Modeling the scientific dimension of academic conferences. *Procedia - Social and Behavioral Sciences*, *147(*25), 576-585.

Nayyar, P. (1993). Performance effects of information asymmetry and economics of scope in diversified service firms. *Academy of Management Journal, 36*(1), 28-75.

Nevo, D., & Kotlarsky, J. (2014). Primary vendor capabilities in a mediated outsourcing model: Can IT service providers leverage crowdsourcing? *Decision Support Systems, 65*, 17-27.

NIST (2011). *Managing information security risk: Organization, mission, and system view.* (NIST Special Publication 800-39). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Oladapo, S., Zavarsky, P., Ruhl, R., Lindskog, D., & Igonor, A. (2009). *Managing risks of IT security outsourcing in the decision-making stage.* Proceedings of the 12th IEEE International Conference on Computational Sciences and Engineering, Vancouver, BC, Canada, 456-461.

Osei-Bryson, K. –M., & Ngwenyama, O. K. (2006). Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. *European Journal of Operational Research, 174*(1), 245-264.

Pannirselvam, G. P., & Madupalli, R. (2011). Antecedents of project success: The perception of vendor employees. *The Quality Management Journal, 18*(3), 7-21.

Poppo, L., & Zenger, T. (1998). Testing alternative theories of the firm: Transaction cost, knowledge-based and measurement explanations of make-or-buy decisions in information services. *Strategic Management Journal, 19*(9), 853-877.

Poppo, L. (2002). Do formal contracts and relationship governance function as substitutes or complements? *Strategic Management Journal, 23*(8), 707-725.

Porter, M. (1980). *Competitive strategy: Techniques for Analyzing Industries and Competitors*. The Free Press: New York.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Journal of Computers and Security, 23*(8), 638-646.

Prado, E. P., de Souza, C. A., Takaoka, H., & Reinhard, N. (2009). Contracting outsourced information technology services in Brazil. *Journal of Global Information Technology Management, 12*(4), 52-72.

Pranata, I., Skinner, G., & Athauda, R. (2012). A distributed secure mechanism for resource protection in a digital ecosystem environment. *Journal of Information Security, 3*(1), 25-38.

Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: Reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica, 104*, 1-15.

Raiborn, C. A., Butler, J. B., & Massoud, M. F. (2009). Outsourcing support functions: Identifying and managing the good, the bad, and the ugly. *Business Horizons, 52*(4), 347-356.

Qi, C., & Chau, P. Y. K. (2012). Relationship, contract and IT outsourcing success: Evidence from two descriptive case studies. *Decision Support Systems, 53(*4), 859-869.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Rhea, L. M., & Parker, R. A. (2005). *Designing and conducting survey research: A comprehensive guide* (3rd ed). Hoboken, NJ: Wiley.

Rigdon, E. E. (1998). Structural equation modeling. In: G. A. Marcoulides (Ed). *Modern Methods for Business Research*. Mahway, NJ: Lawrence Erlbaum.

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly, 36*(1), iii-xiv.

Ringle, C. M., Wende, S., & Becker, J-M. (2015). SmartPLS 3. Hamburg: SmartPLS. Retrieved from http://www.smartpls.com.

Rockart, J. F., Earl, M. J., & Ross, J. W. (1996). Eight imperatives for the new IT organization. *Sloan Management Review, 38*(1), 43-55.

Rollins, M., Pekkarinen, S., & Mehtakam M. (2011). Inter-firm customer knowledge sharing in logistics services: An empirical study. *Internal Journal of Physical Distribution & Logistics Services, 41(*10), 956-971.

Roses, L. K., Hoppen, N., Ballaz, B., & Freire, K. D. M. (2006). *Quality Evaluation in Information Systems Outsourcing.* Proceedings of the 11th International Conference of the Association Information and Management Luxembourg City, Luxembourg, 268-280.

Rovai, A. P., Backer, J. D., & Ponton, M. K. (2013) *Social Science Research Design and Statistics: A Practioner's Guide to Research Methods and SPSS Analysis.* Chesapeake, VA: WaterTree Press.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). *Towards trusted cloud computing.* Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, Berkeley, California, USA.

Saunders, C., Gebelt, M. and Hu, Q. (1997) Achieving success in information systems outsourcing. *California Management Review, 39(*2), 63–79.

Schneier, B. (2002). The case for outsourcing security (supplement to computer magazine), *Computer, 35(*4), p. 20-21.

Scholosser, F., Wagner, H-T., Beimborn, D., & Weitzel, T. (2010). *The role of internal business/IT alignment and IT governance for service quality in outsourcing arrangements.* Proceedings of the 43rd Annual Hawaii International Conference on System Sciences, Honolulu, Hawaii, USA.

Schonlau, M., Fricker, R. D., & Elliott, M. N. (2002). *Conducting research surveys via email and the web.* Santa Monica, CA: RAND.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of Educational Research, 99(*6), 323-338.

Schultz, E. E., Proctor, R. W., Lien, M-L., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computer & Security, 20*(7), 620–634.

Shi, Z., Kunnathur, A. S., & Ragu-Nathan, T.S. (2005). IS outsourcing management competence dimensions: instrument development and relationship exploration. *Information & Management, 42*(6), 901-919.

Silic, M., & Back, A. (2014). Shadow IT-A view from behind the curtain. *Journal of Computers & Security, 45*(6), 274-283.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management, 27*(5), 644-667.

Sia, S. K., Koh, C., & Tan, C. X. (2008). Strategic maneuvers for outsourcing flexibility: An empirical assessment. *Decision Sciences, 39(*3), 407-443.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38(*1), 60-80.

Sloper, A. (2004). Meeting the challenge of outsourcing. *Engineering Management Journal, 14*(3), 34-37.

Smith, M. A., Mitra, S., & Narasimhan, S. (1998). Information systems outsourcing: A study of pre-event firm characteristics. *Journal of Management Information Systems, 15*(2), 61-93.

Smuts, H., Kotze, P., Van Der Merwe, A., & Loock, M. (2010). *Information systems outsourcing issues in the communication technology sector.* Proceedings of the IADIS International Conference Information Systems, Porto, Portugal.

SPSS Inc. (2013). *SPSS Base 17.0 for Windows user's guide*. SPSS Inc., Chicago, IL.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13(*2), 147-169.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Networking and Computer Applications, 34*(1), 1-11.

Sun, S-Y., Lin, T-C., & Sun, P-C. (2002). *The factors influencing information systems outsourcing partnership – A study integrating case study and survey research methods.* Proceedings of the 35th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, USA.

Swar, B., Moon, J., Oh, J., & Rhee, C. (2012). Determinants of relationship quality for IS/IT outsourcing success in public sector. *Information Systems Frontiers, 14(*2), 457-475.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Boston: Allyn and Bacon.

Teng, J. T. C., Cheon, M. J., & Grover, V. (1995). Decisions to outsource information systems functions: Testing a strategy-theoretic discrepancy model. *Decision Sciences, 26(*1), 75-103.

Thong, J. Y. L., & Yap, C. –S. (1996). Information systems effectiveness: A user satisfaction approach. *Information Processing & Management, 32(*5), 601-610.

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook* (5th ed). Boca Raton, FL: CRC Press.

Tsohou, A., Theoharidou, M., Kokolakis, S., & Gritzalis, D. (2007). *Addressing culture dissimilarity in the information systems outsourcing relationship.* Proceedings of the 4th International Conference on Trust, Privacy, and Security in Digital Business, Regensburg, Germany.

Upadrista, V. (2014). *Managing your Outsourced IT services provider: How to unleash the full potential of your global workforce*, New York, NY: Apress.

Venkatesan, R. (1992). Strategic sourcing: To make or not to make. *Harvard Business Review, 70*(6), 98-107.

Vijayan, J. (2001). Outsourcers rush to meet security demand. *Computerworld, 35*(9), 34.

Vinzi, V. E., Chin, W. W., Henseler, J., &Wang, H. (2010). *Handbook of Partial Least Squares: Concepts, Methods and Applications research.* Berlin: Springer.

Volonino, L., Gessner, G. H., & Kermis, G. F. (2004). Holistic compliance with Sarbanes-Oxley. *Communication of the Association for Information Systems, 14(*1), 219.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security, 20*(1), 215-218.

Von Solms, R. (1996). Information security management: The second generation. *Computers & Security, 15*(4), 281-288.

Webb, L., & Laborde, J. (2005). Crafting a successful outsourcing vendor/client relationship. *Business Process Management Journal, 11*(5), 437-443.

Werlinger, R., Hawkey, K., & Beznosov, K. (2008). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 61-93.

Wheeler, T. L. (2008). Organizing security metrics: Can organizations protect themselves? *Information Security Journal: A Global Perspective, 17*(5-6), 228-242.

Whitten, D., & Wakefield, R. (2006). Measuring switching costs in IT outsourcing services. *Journal of Strategic Information Systems, 15*(3), 219-248.

Williams, B., Brown, T., & Onsman, A. (2012). Exploratory factor analysis: A five-step guide for novices. *Journal of Emergency Primary Health Care, 8*(3), 1-9.

Yang, C., & Huang, J. B. (2000). A decision model for IS outsourcing. *International Journal of Information Management, 20*(3), 225-239.

Yang, B. (2005) *Factor Analysis Methods*. In Richard A. Swanson and E. F. Holton III (Eds.) Research in Organizations: Foundations and Methods of Inquiry (pp. 181-199)., San Francisco, CA: Berrett-Koehler Publishers.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, 31*(4), 360-365.

Yuan, K. –H., Marshall, L. L., & Bentler, P. M. (2002). A unified approach to exploratory factor analysis with missing data, nonnormal data, and in the presence of outliers. *Psychometrika, 67*, 95-122.

Zainuddin, E., Bassellier, G., & Benbasat, I. (2010). *Outsourcing project success: The role of competence and leadership of the vendors and client project managers.* Proceedings of the Special Interest Group on Management Information Systems 48th annual Conference on Computer Personnel Research, New York, NY, USA.

Zarknekow, R., Brenner, W., & Pilgram, U. (2006*). Integrated information management: Applying successful industrial concepts in IT*. New York, NY: Spring.

Zhang, J., Borisov, N., Yurcik, W., Slagell, A. J., & Smith, M. (2006). *Future Internet security services enabled by sharing of anonymized logs.* Workshop on Security and Privacy in Future Business Services held in conjunction with International Conference on Emerging Trends in Information and Communication Security (ETRICS), University of Freiburg Germany.

Zhao, X., Xue, L., & Whinston, A. B. (2009). *Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling.* Proceedings of the Thirteenth International Conference on Information Systems, Phoenix, Arizona, 1-17.