1-1-2012

Ensuring the effectiveness of information security policy: the development and validation of an information security policy model

Vivid Vicki Chen

University at Albany, State University of New York, vicki.chen@ge.com

The University at Albany community has made this article openly available. Please share how this access benefits you.

Follow this and additional works at: https://scholarsarchive.library.albany.edu/legacy-etd

Part of the Computer Engineering Commons, and the Library and Information Science Commons

Recommended Citation


https://scholarsarchive.library.albany.edu/legacy-etd/519

This Dissertation is brought to you for free and open access by the The Graduate School at Scholars Archive. It has been accepted for inclusion in Legacy Theses & Dissertations (2009 - 2024) by an authorized administrator of Scholars Archive. Please see Terms of Use. For more information, please contact scholarsarchive@albany.edu.
Ensuring the Effectiveness of Information Security Policy: The Development and Validation of an Information Security Policy Model

By

Vivid Vicki Chen

A Dissertation
Submitted to the University at Albany, State University of New York
in Partial Fulfillment of
the Requirements for the Degree of
Doctor of Philosophy

College of Computing and Information
Information Science Program
2012
ABSTRACT

The purpose of this dissertation is to develop and test a conceptual model of an Information Security Policy (ISP) and to measure the benefits that accrue to organizations that implement and deploy such policies. As a result of rapid changes in technology, the importance of computer Information Security Policy (ISP) has increased dramatically. In recent decades, governments and private enterprises have increasingly come to store ever greater amounts of information on computers and on networks. Unfortunately, storing information in this manner not only makes firms engaged in cutting-edge technology vulnerable to hackers, but may also jeopardize customer / employee relations, product sales and R&D (Goel and Chen, 2005). Recent events at Martin Marietta illustrate the impact such intrusions can have on a nation's classified information. Protecting against these threats is critical in helping firms prevent the loss of physical and monetary assets, as well as intellectual property. It is also critical in helping firms defend their reputations.

An ISP constitutes a set of rules that regulate how an organization’s resources, assets, information and information systems are managed, protected and distributed within, as well as outside, the organization. An effective ISP should provide assurance that proper security functions are enforced. Unfortunately, there exists no comprehensive or readily agreed upon Information Security Policy model that clearly defines information security policy processes or provides concise guidelines or rules for managing such policies. In an attempt to develop such a model one must rely on either an extant theory or framework, or develop a new one. Fortunately, the information
systems development literature is extremely well developed and provides an analogous model that can be extended to the information security problem to help generate an effective ISP model.

The model discussed in this thesis is the result of a careful synthesis of the most widely referenced and validated information systems development models, including Choo’s Information Management Cycle Model (2002), Delone and McLean’s Information System Success Model (1992, 2003), Ives and Olson’s Descriptive Model (1984) and Davis’ Technology Acceptance Model (1989).
First of all, I would like to dedicate this dissertation to my family: my mother, Jane Lee-Chen; my uncle, Dr. S. C. Lee; and the rest of my family members and relatives, Dr. Charlotte Chen, Dr. Frank Luk, Dr. Jim Napolitano, Tom Callan, Rachel Callan, Sean Evanoff and June Evanoff. They have selflessly supported me despite the distance, time, and costs associated with research, publishing and travel. Their unconditional support has helped me overcome many difficulties in completing my Ph.D. I would like to thank my husband, Joseph Callan, without whose continuous support and self-sacrifice, I would not have been able to complete this study.

I would like to thank my dissertation committee members: Dr. Sanjay Goel (my chair), Dr. Salvatore Belardo, Dr. George Berg and Dr. Kevin Williams. They have provided me with expert knowledge and guidance. I am especially appreciative of Dr. Belardo’s dedication and Dr. Goel’s technical expertise in information security policy.

I am profoundly grateful to my colleagues and managers, Alan Walker, Dr. Roshan Chhabra, Chuck Nyberg, Gwen Cole, Edward Boudreau, James Bezner, Greg Blackburn, Kevin Leighton, Robert Conkey, Harold McEathron, Jim Stathopoulos, Alan DeTeso and Dr. ML Hsiao, and to my immediate supervisor Quinton Pierson. I would like to give special thanks to the members of my congregation, Harold McEathron, Lou Tomaino and John Capazza, who have dedicated their time to reading and critiquing my writing.

I thank my fellow students, John Zhang, Yuhui Chen, Xiao-Shui Yang, Julio Pontes, Sairam Chinnam and Willy Wang, for their support and continuous encouragement. I also extend my gratitude to those who have supported me in various other ways, including Dean Dr. Jennifer Goodall, Dr. Peter Bloniarz, Dr. Peter Duchessi, Dr. InduShobha Chengalur-Smith and Dr. Jagdish Gangolly.

Finally, I would like to share this achievement with my late father, Wilson Chen, who provided encouragement without condition and my late grandfather, Dr. C.L. Lee, who always pushed me to my limits. I wish they could see what I have accomplished.
# Table of Contents

ABSTRACT......................................................................................................................... ii

ACKNOWLEDGEMENTS ........................................................................................................ iv

LIST OF TABLES ......................................................................................................................... viii

LIST OF FIGURES ...................................................................................................................... ix

**Chapter 1: Introduction** ........................................................................................................ 1
  1.1. Background and Motivation .......................................................................................... 4
  1.2. Importance of Research .............................................................................................. 8
  1.3. Objective of the Study ................................................................................................ 12
  1.4. Study Structure .......................................................................................................... 14

**Chapter 2: Literature Review and Theoretical Framework** .............................................. 15
  2.1. Information Security Policy Scope ............................................................................. 16
    2.1.1. Information ........................................................................................................ 17
    2.1.2. Information Technology ..................................................................................... 17
    2.1.3. Information System ............................................................................................ 18
    2.1.4. Information Security Policy ............................................................................... 19
  2.2. Information Management Cycle Model (Choo 2002) .................................................. 20
  2.3. Information System Success Model (Delone and Mclean (1992, 2003)) .................. 22
    2.3.1. Origin of D&M IS Success Model (1992) ......................................................... 24
    2.3.2. Revised D&M IS Success Model (2003) ............................................................. 25
  2.4. Technology Acceptance Model (TAM) ...................................................................... 28
    2.4.1. TAM-Origin ...................................................................................................... 29
    2.4.2. TAM2 and UTAUT ............................................................................................ 30
    2.4.3. TAM3 ................................................................................................................ 31
    2.4.4. Conclusion of TAM .......................................................................................... 32
  2.5. Descriptive Model: Ives and Olson (1984) ................................................................ 34
    2.5.1. Involvement Roles ............................................................................................. 35
    2.5.2. Development Characteristics ........................................................................... 35
    2.5.3. User Involvement .............................................................................................. 36
      2.5.3.1. Facets of User Involvement ...................................................................... 38
      2.5.3.2. Outcomes of User Involvement ................................................................. 39
      2.5.3.3. System Quality, User Acceptance and System Usage .............................. 39
      2.5.3.4. Outcomes of User Involvement ................................................................. 39
    2.5.4. System Quality, User Acceptance and System Usage ........................................ 39
    2.5.5. Conclusion of Descriptive Model ...................................................................... 39

**Chapter 3: Development of ISP Conceptual Model** ...................................................... 41
  3.1. ISP Driver .................................................................................................................. 41
Chapter 8: Results of Testing the ISP Conceptual Model

8.1. Introduction
8.2. Data Collection and Demographics
8.3. Hypothesized ISP Model Assessment
  8.3.1. Handling Missing Data and Sample Size
  8.3.2. Validation Methods
    8.3.2.1. First Level Model Validation
    8.3.2.2. Second Level Model Validation
8.4. Testing the ISP Conceptual Model
  8.4.1. Data Collection
  8.4.2. Data Analysis
    8.4.2.1. r- Pearson Product-Moment Correlation Coefficient
    8.4.2.2. R Squared ($R^2$)
    8.4.2.3. Linear Regression
    8.4.2.4. A Trend Line
  8.4.3. Analyzing 2012 Security Breach Report
  8.4.4. Comparison of Firms with and without security breaches
  8.4.5. Comparison of B2B and B2C Firms
8.5. Conclusion of ISP Model Testing

Chapter 9: Discussion and Implication

Chapter 10: Limitation and Future study

REFERENCES

APPENDIX A: Sample of unapproved and validated ISP Checklists
APPENDIX B: 2010 ISP Organizational Defects Survey
APPENDIX C: Cover Letter for eMail based Survey
APPENDIX D: Cover Letter for Pilot Users Survey
APPENDIX E: SURVEY INSTRUMENT
LIST OF TABLES

Table 1 – IT Characteristics of a Priori Research Models
Table 2 – Research Time Line
Table 3 – Operationalization of ISP Deployment Value Constructs
Table 4 – Operationalization of User Perspective Constructs
Table 5 – Operationalization of Organizational Performance Constructs
Table 6 – Items Measure for the Information Security Policy
Table 7 – Recommendation Level of Goodness-of-Fit Cutoff Criteria
Table 8 – Covariance Matrix Table Error Message
Table 9 – User Perspective Testing Result
Table 10 – Goodness-of-Fit of User’s Perspective Construct
Table 11 – Goodness-of-Fit of Second Generation ISP Model Test Result
Table 12 – Summary of 2011 Security Breach Report
Table 13 – Summary of Significant Security Breaches
Table 14 – Reported and Unreported Security Breach Comparison
Table 15 – B2B and B2C Security Breach Comparison
LIST OF FIGURES

Figure 1 – ISACA Information Security Business Model 2010
Figure 2 – Information Security Policy Scope
Figure 3 – Four-Stage Model (Delone and McLean, 1992)
Figure 4 – Information Management Cycle Model (Choo, 2002)
Figure 5a – Information System Success Model: (Delone and McLean, 1992)
Figure 5b – Reformed IS Success Model: (Delone and McLean, 2003)
Figure 6 – Categories of I/S Success (Delone and McLean, 1992)
Figure 7 – Technology Acceptance Model: (Davis, 1989)
Figure 8 – Technology Acceptance Model 2 (TAM2)
Figure 9 – Technology Acceptance Model 3 (TAM3)
Figure 10 – Descriptive Model: (Ives and Olson, 1984)
Figure 11 – ISP conceptual Model Drivers
Figure 12 – Information Management Cycle Model’s ISP Value
Figure 13 – ISPCM Deployment Factors and Choo’s Model
Figure 14 – Searching for ISPCM Deployment Driver Value
Figure 15 – D&M IS Success Model ISP Value
Figure 16 – TAM’s ISP Value
Figure 17 – Original Delone and McLean Model Driver and Factors
Figure 18 – ISP Conceptual Model Deployment Factors and Qualities
Figure 19 – Combined TAM and D&M IS Success Model Variables
Figure 20 – ISP Deployment and Usage Driver Connection
Figure 21 – Relationship Between ISP Deployment and Usage
Figure 22 – ISP Conceptual Model and Descriptive Model
Figure 23 – Benefits of IT System in Olson’s Descriptive Model
Figure 24 – Olson’s Descriptive Model-Value/USE of IT
Figure 25a – ISP Conceptual Model Development Process: Step 1
Figure 25b – ISP Conceptual Model Development Process: Step 2
Figure 26 – ISP Conceptual Model Value, Usage and Benefit
Figure 27 – ISP Conceptual Model Stages
Figure 28 – ISP Proposed Conceptual Model Drivers and Factors
Figure 29 – Proposed ISP Conceptual Model Measurement
Figure 30 – Example of CFA Structural Model
Figure 31 – Proposed CFA Structural ISP Conceptual Model
Figure 32 – Participants’ Gender
Figure 33 – Participants’ Age
Figure 34 – Participants’ Job Function
Figure 35 – The Original Hypothesized ISP Model with Covariances
Figure 36 – User’s Perspective Model
Figure 37 – Second Generation ISP Conceptual Model
Figure 38 – Second Generation ISP Conceptual Model with Covariances
Figure 39a – B2B ISP Qualities / User’s Perspective (r, $R^2$)
Figure 39b – B2B ISP Qualities / Organizational Performance (r, $R^2$)
Figure 40a – B2C ISP Qualities / User’s Perspective (r, $R^2$)
Figure 40b – B2C ISP Qualities / Organizational Performance (r, $R^2$)
Figure 41a – B2C User’s Perspective / Organizational Performance (r, $R^2$)
Figure 41b – B2B User’s Perspective / Organizational Performance (r, $R^2$)
Figure 42a – B2B/B2C ISP Qualities and User’s Perspective
Figure 42b – B2B/B2C ISP Qualities and Organizational Performance
Figure 43a – Overall B2B and B2C ISP Qualities / User’s Perspective (r, $R^2$)
Figure 43b – Overall B2B and B2C ISP Qualities / Organizational Performance (r, $R^2$)
Chapter 1: Introduction

In a world in which hacking, the malicious spread of computer viruses and cyber-terrorism have become daily events, security has become a top priority for businesses, governments and private citizens (Sonnenreich et al., 2006). Information security breaches have a profound impact on organizational assets, both tangible and intangible. While it is extremely difficult to measure the monetary costs of Wikileaks’ exposure of classified government documents, the impact that these leaks have had on relationships between governments throughout the world is profound.

Other security breaches, in which valuable customer information was leaked from SONY’s online gaming systems and the Amazon Cloud, have resulted in considerable financial costs to these firms. The loss to SONY due to PlayStation Network downtime amounts to $171 million. While no fixed estimate of the losses incurred by Amazon in its attempt to resolve a cloud problem is readily available, the cost of bringing “all hands on deck” is surely substantial. As a result, protecting organizational assets must be considered one of the everyday costs of doing business. Yet, the benefits that can be derived from such investments are difficult to assess and the methods used to estimate the cost of information security solutions can vary greatly (Sonneri et al., 2006). I will argue that findings regarding IT/IS investments and systems success in organizations can provide a useful framework for helping develop an ISP model that will result in successful ISP implementation and use, thus leading to better organizational performance.
The value of information technology (IT) to modern organizations is undeniable (Byrd and Davidson, 2006). Both the academic and trade literature report that corporations use information technology (IT) for several reasons: to improve productivity (Byrd and Davidson, 2006); to enhance performance and reduce costs (Earl, 1989; King, 1998); to enable new ways of planning, organizing, and controlling (Earl, 1989); to support business strategies (Porter and Miller, 1985); to gain competitive advantage (Clemons and Row, 1991); and to improve customer service, enhance product and service quality, and integrate supplier and customer operations (Luftman, Lewis and Oldach, 1993).

A number of researchers have argued that it is difficult to assess the impact that IT/IS investments have on organizational performance (Loveman, 1988; Glazer, 1991; Brynjolfsson, 1993; Ragowsky et al., 1996; Salmela, 1997; Brynjolfsson and Hitt, 1998; Marchand et al., 2001; Brynjolfsson and Hitt, 1998, Gable et al., 2004). A separate group of researchers have made an effort to explain how organizations become successful and how information systems affect organizational success (Bailey and Pearson, 1983; Delone and McLean, 1992; Rai et al., 2002; Seddon, 1997). This branch of research provides the foundation upon which I will build a comprehensive ISP model that will enhance user acceptance and improve organizational performance.
An ISP includes processes, practices and technologies; it provides a set of rules which regulate how resources, assets, information systems, and information technology are managed, protected and distributed within an organization. There are numerous Information Security Policy models on which businesses or organizations can rely, including the ISACA Information Security Business Model 2010 (see Figure 1). Some organizations rely on templates or checklists\(^1\) (see Appendix A), but none of these have been thoroughly validated. Most of the research on the subject has focused on the costs associated with security breaches. There is no existing research that examines the factors required to ensure the successful deployment of ISP. Nor has there been research which validates the usage of ISP models or indicates whether or not usage leads to positive organizational performance.

![Figure 1: ISACA Information Security Business Model (2010)](image)

Figure 1: ISACA Information Security Business Model (2010)

In this study I will argue that an effective ISP will not only enhance the organization’s daily business procedures and transactions, but will also help ensure that much needed security measures are implemented effectively.

\(^1\) This checklist was provided by one participant’s company
The purpose of this dissertation is, therefore, to develop and test a conceptual model of an Information Security Policy (ISP) and to measure the proposed benefits that will accrue to the organization as a result of the implementation and deployment of such a policy.

1.1. Background and Motivation

In 2010, Gartner predicted that 3.3 trillion dollars would be spent on technology that year alone (Gartner, 2010); Gartner further predicted that, by 2015, information-smart businesses would increase IT spending per head by 60% and that tools and automation will eliminate 25% of labor hours associated with IT services (Gartner, 2011). Most organizations believe in Porter and Miller’s classic argument that IT investments can provide a competitive advantage (Porter & Miller, 1985). The current financial crisis, however, has had a huge impact on business investment and has resulted in increasing pressure to cut costs. Firms have been forced to substantially lower their investments in Information Technologies, Information Systems and ISPs. Before investing in technology to support organizational information security needs, decision-makers want to know if the investment is sound (Sonnereich et al., 2006). To do this, organizations need to understand what drives ISP (Petter, Delone and McLean, 2008).
Cutting IT costs will necessarily increase a firm’s information security vulnerabilities, giving hackers greater opportunity to invade an organization’s information and communications networks. Most firms continue to recognize the benefits provided by technology investment, especially in times of crisis. The publication “Gartner Predicts 2011” details the shifting role of IT, outlining how information technology has come to play a greater role in helping organizations ensure positive business outcomes (Gartner, 2011). However, along with growing technology needs, there has been an unfortunate increase in system failure, and a corresponding increase in disillusionment with these systems. Improving our understanding of how to successfully implement IT/IS and ensure its successful usage has thus become an important area of research (Chuttur, 2009). This thesis examines these issues as they relate to information security policies, processes, practices and technologies.

In order to survive in today’s economic environment and protect their information systems effectively, organizations have to implement a strategy in which “effective security is at odds with convenience” (Grygus and Beyond, 2003). The effectiveness of a security mechanism, however, depends on both users and technology “doing the right thing”. The usefulness of security mechanisms is not just a question of improving interfaces with security tools, but of designing security systems that will work with the real-world tasks that users perform (Sasse et al., 2001; McHugh and Deek, 2005).
It is incumbent on security managers to ask the following questions. How much security is enough? How can we get maximum benefits from a limited IT budget? It is important to note that the intangible benefits of Information Technology (IT) have not been appropriately measured because of the use of conventional productivity measurement techniques (Im et al., 2001). The same is true for ISP, making it all the more difficult for security managers to evaluate alternative security designs and to justify security technology investment decisions (Butler, 2002).

Information Technology (IT) and Information Systems (IS) are critical resources for creating organizational value (Kohli and Devaraj, 2004). Similarly, information security is an important business issue because of the role it plays in ensuring the effectiveness of these technologies. The goal of organizational information security policies, then, is to define the procedures, guidelines, practices and technologies required for configuring and managing information security in organizations. Information security policies can minimize organizational risks and, equally importantly, demonstrate to customers and shareholders that serious due diligence has been done to prevent and/or mitigate the effect of security breaches. An organization’s ISP should reflect its goals and objectives for information security, define the methods for Security Risk Assessment and agree upon a management strategy for securing information. Figure 2 outlines the scope of information security policy.
Information security is hardly a new concept. The need to protect valuable information is as old as mankind (Hoo, 2000). An Information Security Policy Model is the driver used to create information security policy, processes, practices and technologies. Information security policy, processes, practices and technologies are, in turn, used to create an information security system. An information security system provides the technology needed to protect valuable information. Employee use of information systems bolsters a firm’s information security policy (e.g., IS can be used to force a user into ISP through the use of a password policy). An information security policy model, meanwhile, allows an organization to measure its investment in Information Technology and Information Systems. As noted above, there is no standard model available to businesses or organizations wishing to implement an ISP.
Unfortunately, studies suggest that even if a firm has an information security policy in place, fully 91% of employees fail to adhere to it (Hinde, 2002). To tackle this situation, researchers have begun to study employee behavior, in particular, the inclination or disinclination to use the organization’s ISP. Such studies are designed to help ensure employee compliance with security policies and have identified some serious weaknesses in the existing approaches to this problem. Unfortunately, empirical evidence is lacking. Because practitioners need empirically validated information, it is extremely important that employees’ non-compliance with information security policies be studied using field research (Siponen, 2009).

1.2. Importance of Research

IT managers are asked to simultaneously minimize security costs and maximize security benefits (Buttler, 2006). Researchers, meanwhile, focus on estimating the direct impact of investments in security technologies (e.g. risk assessment, information system vulnerability and threats). The economic decision for or against investment is based on these estimates (Cavusoglu et al., 2004). Few researchers have paid attention to security policy per se. An ISP should be established before any information system is implemented. In short, information technology and information systems should be guided by ISP.
Since the purpose of an ISP is to protect an organization’s valuable information, it is important to estimate the value of this information (Ragowsky et al., 1996) and the methods designed to protect the information in order to determine the appropriate level of IT investment. Information is diffused through business activities, products and services (Orna, 1996). Information can improve an organization’s productivity and innovation rates (Koenig, 1992; Oppenheim et al., 2001), and is therefore a strategic resource (Buchanan and Gibb, 1998). Because information can act as a catalyst that may enhance productivity, it can increase the value of traditional resources (e.g., employees) (Oppenheim et al., 2001). Given that the value of information is determined by how it is used (Choo, 1998), IT systems are a critical element in distributing information and enhancing organizational performance (Glazer, 1991). Subsequently, in developing an ISP model to distribute and protect information, it is essential to consider just what sort of information or information technology is at stake.

An ISP model is clearly designed to protect valuable information. When thinking about the costs of developing and implementing an ISP Model, we should remember the words of President Dwight D. Eisenhower, who said that “We will bankrupt ourselves in the vain search for absolute security.” Finding the right mix of costs and benefits is critical, yet identifying these costs and benefits is easier said than done.

How then does a firm go about developing an effective ISP model, i.e., one that can help Information Security Officers address the complexity of information security
requirements while ensuring a balance between protecting the firm’s valuable information assets and minimizing the firm’s IS/IT investment? This research will focus on the relationship between the deployment of an ISP model, including processes, practices and technologies, and its use. It is assumed in the validated IS literature that usage of an ISP model will result in a positive impact on the organization and thereby increase the return on security investments (ROSI).

Developing an ISP or ISP model, however, is a difficult task. Bruce Schneier, founder and CTO of Counterpane Internet Security, Inc., provides a valuable insight as to how hard this is when he states: “Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches” (Schneir, 2011). This means that an organization cannot buy an “off-the-shelf” solution to meet its security needs. However, this is not to say that a general and comprehensive framework cannot be created from which organizations can develop an ISP that fits their unique business environment.

The development of a generic and comprehensive ISP model is derived from a number of models designed to help decision makers understand what is required in order to develop successful IT/IS. I begin by examining a widely accepted generic four stage model (Delone and McLean, 1992) which focuses on: investment, deployment, usage and
business value (see Figure 3). All investment decisions proceed through these stages. Ultimately, this will enhance organizational performance and increase the return on investment (ROI). For a more detailed discussion of the four-stage model see Chapter Two.

![Four-Stage Model (Delone and McLean, 1992)](image)

Information security can be viewed from a number of perspectives. There are organizations that have successfully implemented ISPs and experienced fewer security breaches. Other organizations have had the opposite experience. A third group has foregone ISPs for any number of reasons, including an inability to calculate the benefits that might result from investment therein. This can happen if a firm does not have the IT infrastructure to support an effective ISP and/or does not have the senior management support to ensure the successful development and implementation of such a policy. Nevertheless, all firms need to have a basic ISP even if it is nothing more than a simple checklist.

In the following I will use widely accepted and richly cited IS success models to develop and test a generic ISP conceptual model that will be able to predict user
perspectives. This is intended to lead to successful ISP model deployment and to provide
guidance both to firms that have implemented ISPs yet failed to protect their assets, and
to firms that do not plan to invest in ISPs because of such concerns.

1.3. Objective of the Study

How can we define Information Security Policy model success? How can we make sure that an organization’s investment will have a net benefit? This research will use the Delone and McLean model as a practical analogy for the development of an effective ISP model. Unfortunately, the Delone and McLean IS Success Model does not provide a detailed account of how deployment factors such as service quality, system quality and information quality are related to IS system use (Koh et al., 2010) and, ultimately, organizational net benefits. Individuals’ technology use decisions are critical to the success of information technology in an organizational context (Cornell, Eining and Hu, 2011). One model that has been proposed to explain and predict the use of a system is the technology acceptance model (TAM) (Chuttur, 2009). The Delone and McLean IS Success Model and TAM are an ISP conceptual model’s solution for explaining how service quality, system quality and product quality can have a positive impact on an organization’s performance.

I began my research by conducting a survey, the purpose of which was to investigate users’ perceptions of the inefficiencies of information security policies among
startup, small, and medium-sized firms as well as large corporations. Seven firms participated in the study (see Chapter Four for details). The survey results point out that startups, small and medium-sized companies generally lack information security policy concepts, processes, practices and technologies. It also points out that: there was no clear guidance or enforcement when information security systems were deployed; there was often no access control regulation; and communication and operation management were deficient. The survey indicated that, in most cases, end users are required to use the IS without any formal means of assessing potential damages or harmful consequences, and that top management is reluctant to invest in an information security policy if there is no recognizable return on information security investment (ROISI).

The purpose of this dissertation is to develop and test a conceptual model of an Information Security Policy (ISP) and to measure the proposed benefits that will accrue to the organization as a result of the implementation and deployment thereof. A new, more comprehensive framework is required to investigate the interaction between Deployment Drivers of Information Security Policy and Usage Drivers of Information Security Policy. Such a framework will lead to improved organizational performance.

This study will focus on the primary question: “Can the Information Security Policy conceptual model be a good predictor of ISP success as measured from the end user’s perspective?”
1.4. Study Structure

The thesis is organized as follows. Chapter Two presents a literature review and an analysis of four different models that form the basis of the ISP conceptual model; it describes in detail and validates the D&M IS Success Model and TAM. In Chapter Three we develop the ISP model and examine the academic research, personal experience of IS/IT, and survey data function drivers critical to the success of ISP model development. In Chapter Four we describe an original study and a 2010 survey design. Chapter Five presents the research questions. Chapter Six delineates the research methodology. Chapter Seven describes our testing of the ISP conceptual model methods. Chapter Eight examines the results of these tests. Chapter Nine discusses the implications of the study. Chapter Ten discuss limitations and future study questions.
Chapter 2: Literature Review and Theoretical Framework

This chapter provides an overview of the literature related to conceptual models of Information Security Policy (ISP). The purpose of the following is to examine the prior models employed in building the ISP model. I intend to focus on the interaction between ISP deployment drivers and ISP usage drivers. The generic ISP model begins, as all investment decisions must, by paying attention to the four critical stages between managing investments and managing benefits. Following the example of Delone and McLean’s IS Success Model, I will focus on the deployment and usage stages (see Figure 3 in Chapter One). Based on a review of the literature and extensive survey data I will postulate a comprehensive and multidimensional ISP conceptual model (ISPCM).

The four theoretical models, the Information Management Cycle Model (Choo, 2002), the Information System Success Model (Delone and McLean, 1992, 2003), the Technology Acceptance Model (Davis, 1989) and the Descriptive Model (Ives and Olson, 1984), together help explain the value of IT/IS, the use of IT/IS, and the benefits derived from IT/IS. The values of the models in this study are summarized in Table 1. The category “Value of the IT System” is focused on the development, deployment, and quality of the IT system; the category “Use of the IT System” is focused on user behavior, the perceived usefulness of an IT system, the perceived ease of use of the IT system, user attitudes and the perceived consequences of using an IT system. The category “Benefit of the IT System” evaluates the usefulness and ease from the user’s perspective, and
describes how these relate to organizational performance. Table 1 also describes the factors underlying the value, use and benefit of the IT system, all of which are antecedents in developing a new ISP conceptual model.

<table>
<thead>
<tr>
<th>Models</th>
<th>Value of IT System</th>
<th>Usage of IT System</th>
<th>Organizational Benefit of IT System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptive Model of user Involvement</td>
<td>• System Quality</td>
<td>• System Acceptance</td>
<td>• Organizational Climate</td>
</tr>
<tr>
<td></td>
<td>• Development Characteristics</td>
<td>• User Characteristics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Involvement Role</td>
<td>• Involvement</td>
<td></td>
</tr>
<tr>
<td>IS Success Model</td>
<td>• Information Quality</td>
<td>• Use</td>
<td>• Net Benefit</td>
</tr>
<tr>
<td></td>
<td>• System Quality</td>
<td>• User Satisfaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service Quality</td>
<td>• Information Needs</td>
<td></td>
</tr>
<tr>
<td>Information Management Model</td>
<td>• Organization and Storage</td>
<td>• Information Acquisition</td>
<td>• Information Use</td>
</tr>
<tr>
<td></td>
<td>• Product/Service</td>
<td>• Information Distribution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Acquisition</td>
<td>• Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Distribution</td>
<td>• Information Use</td>
<td></td>
</tr>
<tr>
<td>Technology Acceptance Model</td>
<td>• Perceive Usefulness</td>
<td>• Attitude Toward Using</td>
<td>• Net Benefit</td>
</tr>
<tr>
<td></td>
<td>• Perceive Ease of USE</td>
<td>• Behavioral Intention to use</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Actual Use</td>
<td></td>
</tr>
<tr>
<td>ISP Model</td>
<td>Determine ISP Investment Drivers and Deployment Factors</td>
<td>Establish a positive link between deployment of Information Security Policy and Use of Information Security Policy</td>
<td>Demonstrate ISP model will lead to improve the organization performance</td>
</tr>
</tbody>
</table>

Table 1: IT Characteristics of Prior Research Models

The following sections describe the four IS models depicted above and focuses on the factors germane to the success of an ISP model.

2.1. Information Security Policy Scope

The scope of the information security policy is important because it helps us to clarify the precise meaning of Information Value, Information Technology, Information System, Information Security, and Computer Security.
2.1.1. Information

"Information is the new currency of business - a critical corporate asset whose value rises and falls at different times, and in different ways, depending on when, how, where and by whom it is placed into circulation as a medium of exchange" (Coopers, 2008). The word information is derived from the Latin “informare” which means "to give form to"; in the Oxford English Dictionary, we find the following definition: “knowledge communicated concerning some particular fact, subject or event; that of which one is apprised or told; intelligence, news.”

Information must be transformed by human cognitive processes into human knowledge in order for it to have value; in essence, information has no value unless it is used (Orna, 1996; Abell, 1993). The value of information, therefore, cannot be separated from the value of information system usage (Ahituv, 1989, 2008).

2.1.2. Information Technology

According to the Oxford English Dictionary, the term “Information Technology” first appeared in a 1958 article published in the Harvard Business Review, in which authors Leavitt and Whisler commented, "The new modern technology does not yet have
a single established name. We shall call it information technology (IT)” (Wikipedia IT, 2011).

The value of information technology (IT) to modern organizations is undeniable (Byrd and Davidson, 2006). Information technology (IT) makes possible the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by a microelectronics-based combination of computing and telecommunications (Adelman, 2000; Longley and Shain, 1985).

Information Technology has made it much easier to access many types of information (Davenport, 1997) and the level of Information Technology (IT) expenditure within organizations continues to increase as organizations seek to gain competitive advantage in their respective industries (Ghoneim, 2007).

2.1.3. Information System

An information system is composed of interrelated tasks, technologies, structures, and people (Gill and Bhattacherjee, 2007; Kelly et al., 1999; Pearson, 2009). As an academic or professional discipline, information systems research bridges the business and computer science fields and has generated a whole new area of scientific inquiry (Hoganson, 2001; Davis et al., 2004; Khazanchi et al., 2000). Information systems research is generally interdisciplinary and concerned with studying the effects of
information systems on the behaviour of individuals, groups, and organizations (Galliers et al., 2006; Ciborra, 2002).

Computer-based information systems are complementary networks of hardware/software that people and organizations use to collect, filter, process, create, and distribute data (Jessup, Leonard and Valacich, 2008). Within the computer science field information systems studies examine algorithmic processes, software and hardware design, the application of these, and their impact on society (Polack, 2009; Hayes and Sharma, 2003). The ultimate goal of information systems is to enhance the effectiveness of the transmission of information (Koh et al., 2010).

2.1.4. Information Security Policy

“Information Security Policy (ISP) is concerned with protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation” (NSTISSC, 2000). Information security is often conceptualized as the protection or preservation of four characteristics: availability, integrity, authenticity, and confidentiality (NSTISSC, 2000; Parker, 1998; Russell and Gangemi Sr., 1994; Howard, 1995)\(^2\). This dissertation is primarily concerned with four of these issues, namely:

- **Availability**: Timely, reliable access to data and information services,

\(^2\) NSTISSC (2000) defined the Information Security domain in terms of availability, integrity and confidentiality; Parker (1998) added Authenticity; similar definitions can be found in the work of Deborah Russell and G. T. Gangemi, Sr.,(1994) and John D. Howard (1995).
• **Confidentiality:** Assurance that information is not disclosed to unauthorized persons, processes or devices,

• **Integrity:** Completeness, wholeness, and readability of information, protection against unauthorized modification or destruction of data (and processes)

• **Authenticity:** Validity, conformance, and genuineness of information.

The terms information security, computer security and information assurance are used interchangeably and often incorrectly (Blyth and Kovacich, 2001). All three, however, are meant to protect the confidentiality, integrity and availability of information (Title 44\(^3\)). Information security applies to both computers and networks (Blyth and Kovacich, 2001). The objective of computer security is to protect information and property from theft, corruption, or natural disaster, while allowing it to remain accessible to its intended users (Blyth and Kovacich, 2001). Information assurance encompasses both computer and information security but focuses more on the strategic risk management of information systems rather than on security controls.

### 2.2. Information Management Cycle Model

One of the most well-known information management processes is Choo’s Information Management Cycle (Choo, 2002). Choo has defined information management as a continuous cycle (see Figure 4). From Choo’s perspective, the information management process serves as the basis for all business intelligence processes. Choo’s original model, presented in 1995, consists of six closely related

---

3 Title 44 outlines the role of public printing and documents in the United States Code.

Figure 4: Information Management Cycle Model

Choo’s model begins at phase 6 (Adaptive Behavior), at which stage information is created by an organization’s actions, or Adaptive Behavior. These actions interact with those of other organizations and systems to alter the environment and generate new messages and information. Eventually, adaptive behavior will cycle back to phase 1 (Information Needs).

1. Phase 1 (Information Needs): an organization’s members have to find out what kind of information is necessary to solve different problems and to make decisions successfully.
2. Phase 2 (Information Acquisition): there are many different sources of information both inside and outside an organization; acquisition is driven by the previous phase, Information Needs.

3. Phase 3 (Information Organization and Storage): information is collected, integrated, and stored. Choo explains that an organizational memory is created in Phase 3; the organizational memory is the active storehouse of an organization’s knowledge and know-how.

4. Phase 4 (Information Products/Services and Information Distribution): information acquired and information residing in the organizational memory are packaged into different levels of information products and services. These products and services are allocated according to an organization’s different user groups and information needs. In information distribution, the goal is to increase the sharing of information.

5. Phase 5 (Information Use): acquired knowledge is used enhance the decision-making processes.

2.3. Delone and McLean’s Information System Success Model

Choo’s model focuses on information and information management but does not offer any explanation of how the use of information systems leads to a net benefit. Choo also fails to discuss information security policy. The D&M IS Success Model is the most popular means of evaluating the success of an information system (Myers et al., 1998; Sedera and Gable, 2004); it has been widely acknowledged as a powerful and effective
explanation of the factors that contribute to successful Information Systems (Heo and Han, 2003; Myers, 1997). D&M IS is one of the most frequently cited models (Heo and Han, 2003) and has contributed greatly to the field of IS research by summarizing the key components of successful IS (Gable, Sedera and Chan, 2008). By 2002, there were over 285 papers in refereed journals and proceedings that had referenced and cited the model (Delone and McLean, 2003).

The measurement of information system (IS) success or effectiveness is critical to our understanding of the value and efficacy of IS management actions and IS investment decisions (Delone and McLean, 2003). Delone and McLean recognize the difficulty of directly measuring the benefits of a firm’s investment in technologies, programs, processes and systems (Delone and McLean, 1992). Prior to Delone and McLean’s work, IS success was often measured in isolation; their work was unique in allowing a better understanding of research as a whole.

Delone and McLean (1992) begin with a four-stage success model that includes Investment, Deployment, Utilization and Organizational Benefits (see Figure 3); this four-stage model is designed to measure the relationship between investment and IT value. In their model the authors predict that people will realize the benefits of using a technology, program and system if they perceive that it enhances their productivity.
2.3.1. Origin of D&M IS Success Model (1992)

In their original 1992 work, Delone and McLean (see Figure 5a) relied on Shannon and Weaver’s communications research (1963), Mason’s information "influence" theory (1978), and a host of theoretical and empirical IS studies conducted in the 1970s and 1980s (see Figure 6). From these they extracted 100 measures of “MIS-success” and developed a general and comprehensive definition of IS success called the D&M IS Success Model (Delone and McLean, 1992). They incorporated six different categories of IS success measures, including: “System Quality”, “Information Quality”, “Use”, “User Satisfaction”, “Individual Impact” and “Organizational Impact” (see Figure 5b).

Figure 5a: Delone and McLean (1992) IS Success Model (or D&M IS Success Model)
2.3.2. Revised D&M IS Success Model (2003)

In 2003 Delone and McLean revised their original model in response to criticism from various researchers who argued that its combination of the process model and other references was confusing. Critics complained that Delone and McLean had inappropriately conceptualized the notion of “use” (Seddon, 1997; Seddon et al., 1999). Pitt, Watson and Kavan (1995) observed that commonly used measures of IS
effectiveness focus on the products rather than the services of the IS function, thereby misconstruing IS effectiveness.

Other critics believed that service quality measurements should be considered part of IS success (Kettinger and Lee, 1995; Li, 1997; Wilkin and Hewitt, 1999) and suggested that service quality could be applied and tested using the “SERVQUAL” measurement instrument from marketing (Pitt, Watson and Kavan, 1995; Kettinger and Lee, 1995)

4. In 1995, Pitt and colleagues argued that, due to the increasing importance of relationships between users and IT departments, a service quality construct should be added to the model. There are, however, many ways to think of service quality. The work of Myers and Ishman (Myers et al., 1998; Ishman, 1998) focused on “workgroup impacts”. Clemons and colleagues (Clemons et al., 1993) focused on “Inter-organizational and industry impacts”. Hitt and Brynjolfsson (Hitt and Brynjolfsson, 1994; Brynjolfsson, 1996) focused on “consumer impacts” while Seddon (Seddon, 1997) focused on “societal impacts”.

In 2003, after eleven years of critique, validation, justification, and reproach, Delone and McLean revised their 1992 D&M IS success model and published it in an article titled “Information Systems Success Revisited” in the Proceedings of the 35th

4 This instrument uses the dimensions of tangibility, reliability, responsiveness, assurance, and empathy to measure service quality (DeLone and McLean 2003);
The original D&M IS Success Model of 1992 had four components: organizational investment, system-deployment, system-usage and the consequences of system use, i.e., benefit. Delone and McLean recognized that organizational benefits are often difficult to assess, and that user perceptions of system value and ease of use could be considered surrogates for organizational benefits given that users would not favor systems that did not facilitate or improve job performance (Delone and McLean, 2003). Seddon used the terms “consequences” and “net benefits” in assessing outcomes (Seddon, 1997). He argued that the nature and purpose of the system being evaluated will determine outcome measurements. Delone and McLean conceded that their 1993 success model used the assessment term IMPACT, which could be either positive or negative, thereby causing confusion. DeLone and McLean’s revised D&M IS success model of 2003 grouped impact measures into a single category called “net benefits”. Unfortunately, the term “net benefit” is still somewhat ambiguous given that no outcome is entirely positive or entirely negative.

In their paper “Information System Success Revisited”, Delone and McLean grouped the comments, suggestions and issues raised by critics of the IS Success Model into six categories: 1) “Process vs. Causal Models”; 2) “System Use as a
Success Measure”; 3) “Model Extensions-Service Quality”; 4) “Model Extensions-Impact”; 5) “Independent vs. Dependent Variables”; 6) “Role of Context” (Delone and McLean, 2003). They reformulated their original success model, adding Service Quality and IS impact measures and redefined the variables. In their revised model the main independent factors are System Quality, Information Quality and Service Quality and the main dependent factors are Net Benefits, Intention to Use, and User Satisfaction (see Figure 5b).

2.4. Technology Acceptance Model (TAM)

The independent factors identified by Delone and McLean, namely, service quality, system quality, and information quality are more easily assessed than the dependent factors, namely, net benefit, intention to use and user satisfaction. Predicting IT acceptance and use has been a key area of information systems research since the discipline’s inception (Jones and Hubona, 2005). Security managers often regard human behavior as a security liability, but they still need to accommodate it within their organization’s information security management procedures (Parkin et al., 2009). Of the many alternatives to the D&M IS Success Model, the Technology Acceptance Model (TAM) (Davis, 1989) has become the most influential and commonly employed theory in information systems (Lee et al., 2003). TAM is an information system theory that models how users come to accept and use a technology. The model demonstrates that, when users are presented with a new technology, a number of factors influence their decisions about how and when to use it (Davis, 1989).
2.4.1. TAM – Origins

Davis, Bagozzi, and Warshaw developed the Technology Acceptance Model (TAM) to predict the use of technology systems in the workplace (Davis, Bagozii and Warshaw, 1992). The origins of TAM can be traced to the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975). TRA is based on three general constructs: behavioral intention (BI), attitude (A), and subjective norm (SN). TRA suggests that a person's behavioral intention depends on his or her attitude about behavior and subjective norms (\( BI = A + SN \)). If a person decides upon a course of behavior, then it is likely that he or she will follow through with it. The TAM posits that attitudes toward system use are based on perceived usefulness and ease of use (see Figure 7). Usefulness and ease of use are, therefore, key determinants of Information Technology (IT) acceptance.

- Perceived usefulness (PU) is the degree to which a person believes that using a particular system will enhance his or her job performance (Davis, 1989).
- Perceived ease of use (PEOU) is the degree to which a person believes that using a particular system will be free of effort (Davis, 1989).

![Figure 7: Technology Acceptance Model: Davis (1989)](image)

Studies evaluating TAM show that perceived usefulness has been found to have a
significant impact on attitudes toward online retailers (Chen et al., 2002; Chen and Tan, 2004; Kim and Forsythe, 2007; Koufaris, 2002; Lee et al., 2006; Lin and Lu, 2000; O’Cass and Fenech, 2003; Vijayasarathy, 2004). Perceived ease of use, meanwhile, is an important determinant of the use of technology or systems in TAM (Davis, 1989; 1993; Davis et al., 1992; Mathieson, 1991). Both beliefs influence the user’s attitude, which, in turn, influences his or her intention to adopt the application or technology (Schepers and Wetzels, 2007). In addition, intention has been found to be a stable and strong predictor of system use (Taylor and Todd, 1995). TAM, therefore, provides a foundation for measuring beliefs and attitudes that may predict future behaviors (Hubona and Burton-Jones, 2002).

2.4.2. TAM2 and UTAUT

As with the D&M IS Success Model, TAM has also been modified and expanded, the two major upgrades being TAM 2 (Venkatesh and Davis, 2000; Venkatesh, 2000) and the Unified Theory of Acceptance and Use of Technology (or UTAUT, Venkatesh et al., 2003).

Venkatesh and Davis extended the original TAM model to explain perceived usefulness and usage intentions in terms of social influence and cognitive instrumental processes. Their extended model, TAM2 (see Figure 8), was tested in both voluntary and mandatory settings. The results strongly support TAM2 (Venkatesh and Davis, 2000).
In an attempt to integrate the main competing user acceptance models, Venkatesh and colleagues formulated the Unified Theory of Acceptance and Use of Technology (UTAUT) model. This model was found to outperform each of the individual models (Adjusted R squared of .69 or 69 percent) (Venkatesh et al., 2003).

Figure 8: Technology Acceptance Model 2 (TAM2)

2.4.3. TAM3

A third iteration, TAM 3, was proposed by Venkatesh and Bala in 2008; TAM3 adds to the existing body of knowledge by offering a comprehensive nomological network of the determinants of information technology adoption and use (Venkatesh and Bala, 2008) (see Figure 9).
2.4.4. Conclusion of TAM

Since its inception in the late 1980’s TAM has been applied and tested extensively (Venkatesh and Davis, 2000). Much of the attention has focused on the robustness and validity of the questionnaire instrument used by Davis (1989). Several researchers have replicated Davis’s original 1989 study to provide empirical evidence of the relationship between usefulness, ease of use and system use (Adams, Nelson and Todd, 1992; Davis,
TAM has been widely applied to studies investigating: web site use (Moon and Kim, 2001; Teo, Lim, and Lai, 1999); online shopping (Barkhi and Wallace, 2007; Chen, Gillenson, and Sherrell, 2002; Chen and Tan, 2004; Childers et al., 2001; Gefen and Straub, 1997; Koufaris, 2002; Lin and Lu, 2000; Liu et al., 2003; O’Cass and Fenech, 2003; Vijayasarathy, 2004); online retailing (Kim and Forsythe, 2007; Lee, et al., 2006); and use of mobile devices (Cheong and Park, 2005; Liao et al., 2007; Shin, 2007; Wang, Lin, and Luarn, 2006).

Although TAM has been widely used to predict an individual’s acceptance and usage of new technology, many scholars note that there has not been enough emphasis placed on individual-level factors (Agarwal and Prasad, 1999; Kwon and Chidambaram, 2000; Lee et al., 2006; Venkatesh and Davis, 2000). Despite efforts to refine and expand TAM, critics continue to question its heuristic value, its explanatory and predictive power, and practical value (Chuttur, 2009). TAM, these critics contend, has diverted researchers from more important issues and has created an illusion of progress in knowledge accumulation (Benbasat and Barki, 2007). Attempts to expand TAM so that it more closely conforms to the constantly changing IT environment, meanwhile, has led to a state of theoretical chaos and confusion (Benbasat and Barki, 2007).
In general, TAM focuses on the “individual user” and attempts to explain how he or she “perceives usefulness”. TAM, in essence, ignores the fundamentally social processes of information systems development as well as the social dimensions of information system use (Bagozzi, 2007).

2.5. Descriptive Model: Ives and Olson (1984)

It is almost an axiom of the MIS literature that user involvement is a necessary condition for successful development of computer-based information systems (CBIS) (Ives and Olson, 1984). Based on the Organizational Behavior literature, Ives and Olson proposed a descriptive model of user involvement, in which the dependent variables are system quality and system acceptance (Ives and Olson, 1984). The descriptive model’s primary focus, as seen in Figure 10, is the relationship between user involvement and two types of outcome variables: system quality and system acceptance. Ives and Olson (1984) proved user involvement has a positive impact on system quality and system acceptance.

Figure 10: Descriptive Model: Ives and Olson (1984)
2.5.1. Involvement Roles

Involvement roles describe who should be involved in the development of the system; three different levels have been suggested:

- Primary users of the system: those who use system output;
- Secondary users of the system: those who generate system inputs or run the system;

2.5.2. Development Characteristics

Development characteristics refer to the type of system being developed and where in the development process user involvement should take place. For example, user participation is critical during the definition stage but becomes less important in the installation stage.

Two classes of development characteristics may affect user involvement: the type of system being developed and the stage in the development process. Depending upon the type of system being developed there are four possible scenarios that will determine user involvement:

- User involvement is critical.
- User involvement is inappropriate because the system requires considerable technical
expertise.

- The product is invisible or unimportant to users.
- The system is highly structured and well-defined, so user involvement may not be important for improving system quality (although it may be important for system acceptance).

Depending upon the actual stage in the development process, user involvement is prescribed:

- For the definition stage, in which the project is justified and high level specifications are written.
- In the installation stage, in which participation is considered less important during the intervening stages of system design and physical development.

### 2.5.3. User Involvement

"User involvement" in information system development is generally considered an important mechanism for improving system quality and ensuring successful system implementation leading to system usage and/or information satisfaction (Baroudi, Ives and Olson 1986). Ives and Olson describe "user involvement" as participation in the system development process by representatives of the target user group. Two areas of this theory relevant to the current discussion are participative decision-making (PDM) and planned organizational change (Ives and Olson, 1984).
The goal of participative decision-making (PDM) is to increase inputs by subordinates into management decisions that affect their jobs (Ives and Olson, 1984). Locke and Schweiger found strong evidence relating PDM to higher job satisfaction as well as to increased acceptance of change (Locke and Schweiger, 1979). Users and system developers working together to increase the quality or acceptance of the system provide information for an accurate assessment of the requirements of the organization (Ives and Olson, 2004). In short, user involvement can be considered a special case of PDM in which users and system designers appear more as superiors than subordinates.

Ives and Olson describe how user participation may be related to user acceptance of the system. They report that user involvement develops realistic expectations of the system, provides grounds for conflict resolution between the development team and the users, decreases user resistance and increases system ownership by the users, which, in turn, commits users to the system. The "common wisdom" that user involvement should lead to improved chances of successful system implementation can be traced to theory and research in Organizational Behavior (Ives and Olson, 1984).

In the theory of planned organizational change implementation, success (i.e., acceptance and use of new models or information systems) is considered to be dependent on the quality of the implementation process (Ginzberg, 1979; Schultz and Slevin, 1975; Zand and Sorenson, 1975), so the planned change research assumes that change entails either a joint effort (Ginzberg, 1979) or negotiation (Zand and Sorenson, 1975) between
the manager and the change agent.

2.5.3.1. Facets of User Involvement

The type of participation may vary from direct, in which all parties affected by the system are involved, to indirect, in which employee representatives serve on committees (Ives and Olson, 1984). Ives and Olson proposed three dimensions of user involvement, ranging from least direct to most direct, namely: consultative, representative, and consensus.

1. Consultative: users provide the needs of the system but decisions are made by the development group.
2. Representative: users at all levels are represented on the system design team.
3. Consensus: consensus occurs when all users are consulted through the development process.

The degree of involvement refers to the amount of influence the user has over the final product. At one extreme, system designers make assumptions about requirements and ignore user input; at the other, users design systems and/or accept them on the basis of user-defined criteria of quality (Lucas, 1974).
2.5.3.2. Outcomes of User Involvement

Research on user involvement, PDM, and planned organizational change focuses on two classes of outcome variables: system quality and system acceptance. Those two variables act as "intervening mechanisms" between user involvement and two other factors: cognitive and motivational (Locke and Schweiger, 1979). Cognitive factors refer to improved understanding of the system, system needs, and improved evaluation of system features. The motivational factors that lead to system acceptance are increased ownership, decreased resistance to change, and increased commitment.

2.5.4. System Quality, User Acceptance and System Usage

Ives and Olson’s research provides little justification for user involvement. Boland and Gallagher, on the other hand, found evidence supporting a positive relationship between user involvement and system quality (Boland, 1978; Gallagher, 1974). Of six studies examining the relationship between user involvement and system usage, only one found a significant impact on system usage (Swanson 1974).

2.5.5. Conclusion of Descriptive Model

Ives and Olson studied 22 instances of user involvement and reached no firm conclusion in favor of it. In 8 instances they were able to discern a positive relationship
between user involvement and various measures of system success; 7 studies presented mixed results; the remaining 7 were negative. Although multiple studies operationalized user involvement, there is still a lack of consensus regarding the significance of operationalization per se. In Ives and Olson’s model there are two system success variables:

- System quality: a set of measures utilized to determine some aspect of the benefits of a system.
- System acceptance: system use, changes in behavior and attitude, and user satisfaction (King and Rodriquez, 1978; Lucas, 1975, 1976; Maish, 1979; Schewe 1976; Swanson, 1974).

NB: The significance of the above two systems success variables is somewhat controversial.
Chapter 3: Development of the ISP Conceptual Model

This chapter discusses the conceptualization and operationalization of the selected framework and describes how the ISP conceptual model (or ISPCM) maps onto prior research models. In the following chapter I will: 1) assess the relevance of prior models5 to identify the study constructs; 2) revisit relevant studies of user satisfaction, user involvement, net benefits and organizational impact constructs; 3) define a more expansive organizational impacts theory of the ISPCM; 4) describe the ISPCM itself; and 5) discuss the operationalization of the ISPCM.

3.1. ISP Drivers

The ISP conceptual model described below is based on a number of concepts and models that have migrated from the field of information system security. The four most highly cited models on which I will rely are the following: Choo’s Information Management Cycle (Choo, 2002); Delone and McLean’s IS Success Model (Delone and McLean, 1992, 2003); Ives and Olson’s Descriptive Model (Ives and Olson, 1984); and the Technology Acceptance Model (Davis, 1989; Venkatesh and Davis, 2000; Venkatesh and Bala, 2008). The values derived from the models that I will address are: “Value of IT Systems”; “Usage of IT Systems”; and, “Benefits of IT Systems” (see Table 1).

5 These models were discussed in Chapter 2
These four models are closely associated with the conceptionalization and operationalization of information systems, information security, and information security policy and provide the basis for the information security policy (ISP) conceptual model described below. The proposed ISP conceptual model includes the following drivers derived from the work of Delone and McLean: investment, deployment, usage and benefits (see Figure 11).

**Information Security Policy Drivers**

An ISP investment driver has five factors: supervision, technical, training, resources, and assets. An ISP deployment driver also has five factors: business, project rollout, technology, human factors, and product. As discussed in the preceding chapters, different types of firms need different types of ISP processes, practices and technologies; firms cannot buy an-off-the-shelf ISP model (Schneier, 2011) unless it is

---

6 These deployment factors can be regrouped as follows: Business (including human factors), Technology (including project rollout) and information (as part of the firm’s assets)
modified and/or adapted to meet the firm’s requirements\textsuperscript{7}. Ives and Olson demonstrated that user involvement and organizational climate are important factors in IS success (Ives and Olson, 1984). An ISP is a set of rules that regulates the IS environment. User involvement and organizational climate are, thus, crucial factors in successful ISP implementation. The main purpose of ISP is to protect the firm’s most valued assets; this requires contemporary hardware and software in order to detect and mitigate vulnerabilities and threats.

Usage drivers are designed to account for employees who do not follow information security policies and constitute a serious threat to the organization. What are the consequences of failing to follow security policies? A field study designed to assess deployment qualities, i.e., service quality, system quality, and product quality, and help employees comply with ISP processes, practices and technologies will serve to answer these questions. The usage drivers germane to this study are: consequences, perceived ease of use, perceived usefulness, user satisfaction and ISP efficiency.

Finally, there is a benefit driver in the ISP conceptual model development process. The purpose of the ISP conceptual model is to produce a positive impact on an organization. This includes: compliance with government and business regulations; upgrades to the organization’s current standards; increased employee acceptance of new policies, processes, practices and technologies; enhanced productivity; reduced clean-up

\textsuperscript{7} During face-to-face interviews in 2010, some of firms indicated that they had purchased an-off-the-shelf software or system and found it necessary to modify at least 25\% of the product in order to meet their needs.
costs and legal fees; and, ultimately, improved reputation and greater revenue stream. A benefit driver must, therefore, encompass compliance, modernization, adaptation, productivity, reputation, and revenue factors.

There have been numerous studies regarding IT productivity and business value, defined as the contribution of IT to corporate performance (Cron and Sobol, 1983; Turner, 1985; Bender, 1986; Loveman, 1994; Strassman, 1990; Harris and Katz, 1991; Weill, 1992; Brynjolfsson and Hitt, 1993; Lichtenberg, 1993; Markus and Soh, 1993; Brynjolfsson and Hitt, 1994). Unfortunately, these studies show little consensus regarding the actual nature of IT business value. None of these studies have examined the relationship between the value of IT and ISP. I will endeavor to demonstrate the intangible benefits that accrue to organizations that invest in, develop and use ISPs.

3.2. ISP Conceptual Model and Choo’s Model

In the 1990s, researchers first began to pay attention to information management (Davenport, 1993, McGee and Prusak, 1993). One of the most well-known information management processes to emerge from this literature was Choo’s Information management Cycle (Choo, 2002).

Choo defines information management as a continuous cycle involving constant interaction between organizations and systems (see Figure 4). The process begins at the right-end of the cycle; here, information is created by an organization’s actions, or
Adaptive Behavior. The cycle proceeds from Adaptive Behavior to Information Needs, Information Acquisition, Information Organization and Storage, Information Products/Services and Information Distribution, and Information Use, before circling back to Adaptive Behavior. All six phases are linked to the use of IT systems.

Information Acquisition, Information Organization and Storage, Information and Products/Services and Information Distribution are all related to information technology and constitute the “Value of the IT System”. Information Use and Adaptive Behavior relate to how information behavior leads to information use: these constitute the “Usage of the IT System”. Finally, Information Use, Information Organization and Storage, and Information Products/Services and Information Distribution constitute the “Benefit of the IT System”. In Figure 12:

- The dotted blue line represents the Value of the IT system,
- The dotted green line represents the Use of the IT system,
- The dotted red line represents the Benefit of the IT system

![Diagram of Information Management Cycle Model’s ISP Value](image)

**Figure 12: Information Management Cycle Model’s ISP Value**
The deployment drivers of ISPCM from Figure 11 can be regrouped into three factors: business (including human factors), technology (combined with project rollout) and information (part of assets). Each factor connects to Choo’s Information Management Cycle. See Figure 13 to understand how Choo’s model fits into the ISPCM deployment factors.

![Figure 13 – ISPCM Deployment Factors and Choo’s Model](image)

### 3.3. Gap in CHOO’s model

As noted above, ISPCM’s deployment factors are derived from Choo’s Information Management Cycle Model: however, Choo’s model is missing a crucial element, namely inspiration for users to move from phase 1 (Information Needs) through phase 4 (Information Distribution) to the phase 5 (Information Use). The question is: why do we use information? The same question applies to the ISPCM. (See Figure 14)
Choo’s Information Management Cycle Model does not explain how Information Needs, Information Acquisition, Information Organization/Storage, Information Products/Services and Information Distribution relate to Information Use. In addition, Choo’s Information Management Cycle model misses the relationship between Investment and IT Value. The Delone and McLean IS Success Model measures IT value on the basis of IT investment, IT deployment, and IT usage (see Figure 3). TAM (1989) measures external variables and actual system use (see Figure 7). The ISP conceptual model described in this dissertation adopts the generic framework of the Delone and McLean IS Success Model and the TAM, but customizes it to focus on the relationship between ISP deployment and ISP usage.
3.4. ISP Conceptual Model and D&M IS Success Model

The ISP conceptual model uses both versions of the D&M IS Success Model but relies more heavily on the 2003 model. Unlike the 1992 model, the 2003 model was developed to help assess internet-based systems (Halonen, 2009, Delone and McLean, 2004). Secondly, the 2003 model combines “Individual Impact” and “Organizational Impact” under the heading “Net Benefit” (see Figures 5a and 5b). The 2003 D&M IS Success Model represented by Figure 15 identifies the value, use and benefit of the IT system as follows:

- The dotted blue line represents the Value of the IT system,
- The dotted green line represents the Use of the IT system,
- The dotted red line represents the Benefit of the IT system.

Figure 15: D&M IS Success Model’s ISP Value
In 1998, Smithson and Hirschheim proposed a conceptual framework for IS evaluation and demonstrated its “usefulness” by applying the framework to an outsourcing situation. Delone and McLean argued, "While most studies that follow D&M replace the Use box with ‘Usefulness’ . . . we prefer to maintain Use as in the original work” (Delone and McLean, 2003). The term “ease of use” was used in several studies that evaluated the relationship between “system quality” and “individual impacts” in the D&M IS Success Model (Elezadi-Amoli et al., 1989; Goodhue, 1985; Seddon, et al., 1994; Teo et al., 1998; Wilson et al., 2001). These studies concluded that the D&M IS Success Model was missing two measurement variables: perceived ease of use and perceived usefulness. By merging the D&M IS Success Model with TAM, they were able to correct this deficiency.

3.5. ISP Conceptual Model and TAM

As previously noted, the Technology Acceptance Model (TAM), developed by Davis in 1989, is extremely useful in research examining the determinants of information technology acceptance and use. TAM’s “perceived ease of use” (PEOU), and “perceived usefulness” (PU) are the two most important factors in explaining the use of new technology. In terms of ISP usage, PEOU and PU are the important drivers that determine the IT system’s value (see Figure 16).
In the original TAM model (1989), the “external variables” can be replaced by the D&M IS Success Model’s System Quality, Service Quality, and Information Quality or by Olson and Ives’ User Characteristics, Organizational Climate, and User Involvement (see chapter 2). In the TAM model cited below in Figure 16, Attitude toward Using and Behavioral Intention to Use constitute the value of IT system usage. In Figure 16:

- The dotted blue line represents the Value of the IT system,
- The dotted green line represents the Use of the IT system,
- The dotted red line represents the Benefit of the IT system

Figure 16: TAM’s ISP Value

3.6. Combined TAM and D&M IS Success Model

Since 1999, researchers estimate that the total annual worldwide expenditure on information technology (IT) has exceeded one trillion US dollars per year and is growing at an annual rate of 10% (Seddon et al., 1999). At the same time, information systems
have infiltrated almost all aspects of human life. In light of these facts is it crucial to determine just how effective these investments actually are (livari, 2005).

In the early stages of my research, I conducted face-to-face interviews with the CEOs of a number of startup and small-sized companies, all of whom had the same concerns. How do we measure IT investment? How do we develop IS systems that will satisfy government regulations? How do we prevent hacking? How do we maximize the positive Return on Information System Investment?

The original D&M IS Success Model has four IT related drivers: IT investment, IT Deployment, IT usage and IT value. The deployment driver and usage driver, meanwhile, constitute the critical path of the D&M IS Success Model (Delone and McLean, 1992). The deployment driver factors generate IS qualities, while the usage drivers are perceived as those qualities that lead to User Satisfaction and IT Use. Figure 17 summarizes the D&M IS Success Model’s concepts, drivers, and factors. The same concept was used to develop the ISP Conceptual model, which, as Figure 18 indicates, covers IT/IS regulation but expands the scope of the D&M IS Success Model.
Figure 17: Original Delone and McLean Model Driver and Factors

Figure 18: ISP Conceptual Model Deployment Factors and Qualities
In ISP the deployment driver consists of three factors: Business, Technology, and Information. The Business Factors are: Environment, Governing, Leadership/IT team, Awareness and Assets. The Technology Factors are: Secure, User-friendly, Reactive, Maintenance and Bug-free. The information factors are: Correctness, Suitability, Clear, Fullness and Up-to-Date. These factors are key points in the implementation of ISP processes, practices and technologies. However, it’s very hard for users to translate these factors into perceived consequences, perceived ease of use and perceived usefulness.

What will motivate employees to use the ISPCM? The D&M IS Success Model (2003) and TAM (1989) can translate deployment factors into qualities allowing users to observe consequences, ease of use and usefulness. These qualities form the bridge between the deployment and usage drivers (see Figure 18 and 20). We, therefore, need to replace the TAM model “External Variables” with the D&M IS Success Model’s Qualities in order to construct our ISP conceptual model. Figure 19 demonstrates the flow of TAM and D&M IS Success Model variables. Here, Information Quality, System Quality, and Service Quality replace the TAM model’s external variables; the TAM model’s Perceived Ease of Use, Perceived Usefulness and Attitude Toward Using constitute antecedents to Behavioral Intention to Use and User Satisfaction. Figure 20 represents the ISP conceptual model, which combines the TAM and D&M IS Success Model.
As previously noted, an ISP is a set of rules or guidelines for employees covering such factors as organizational resources, access to information, IS design and
maintenance, environmental safety and health policies. A successful ISP needs to be able to translate these factors into qualities that can be understood and appreciated by employees. Translating the relevant D&M IS Success Model and TAM factors into ISP factors yields the following: ISP Business Factors correspond to Service Quality; ISP Technology Factors correspond to System Quality; and ISP Information Factors correspond to Product Quality.

Next, we translate deployment factors into qualities: the Business Factors correspond to Service Quality; Technological Factors correspond to System Quality; Informational Factors correspond to Product Quality. The correspondence of factors and qualities suggests a number of conclusions: governing ensures reliability (e.g., reduce IS downtime); awareness ensures that employees are responsive; reactivity ensures quick system response time; maintenance ensures that information systems are easy to modify and monitor; correct information guarantees an accurate product; suitable information guarantees a relevant product.

After combining the TAM and D&M IS success models, the ISP conceptual model deployment and usage drivers can easily be connected. Figures 20 and 21 show the ISP conceptual model’s connection between deployment and usage drivers.
Figure 21: Relationship Between ISP Deployment and Usage

After connecting the ISP model’s deployment drivers to their usage drivers, the following aspects of the D&M IS Success Model (2003) and TAM (1989) should be clarified:

- Delone and McLean measured Information Quality in terms of accuracy, timeliness, completeness, relevance, and consistency. They measured Individual Impact in terms of decision-making performance, job effectiveness, and quality of work. Not all applications of IT involve production information for decision making. The ISP conceptual model focuses on accuracy, completeness, relevance, and consistency.

- In the ISP conceptual model Product Quality becomes Information Quality.

- For Delone and McLean, System Quality relates to the safety and reliability of the system, the consistency of the user interface, ease of use, quality of documentation,
and sometimes, the quality of the program code. In the ISP conceptual model System Quality relates to Information Needs and Information Acquisition.

- Service Quality relates to: whether the IS has up to date hardware and software (tangible) and is reliable; whether IS employees give prompt service to users (responsiveness); whether IS employees have the knowledge to do their job well (assurance); and whether IS employees have the user’s best interests at heart (empathy).

- Intention to Use is an attitude; Use is a behavior.

- Use and User Satisfaction are interrelated. Use must precede User Satisfaction in a process sense, but use will also lead to greater user satisfaction in a causal sense. Similarly, increased user satisfaction will lead to increased intention to use. User Satisfaction remains an important means of measuring individual success and organizational performance. Use or usage covers all aspects of information security policy. Figure 21 shows how deployment qualities lead to usage.

- Perceived consequences lead employees to follow ISP rules. For example, password sharing could result in disciplinary action; entering a manufacturing area without safety glasses or shoes may result in physical harm.

- Perceived ease of use – “the degree to which a person believes that using a particular system would be free of effort” (Davis, 1989).

- Perceived usefulness – “the degree to which a person believes that using a particular system would enhance his or her job performance” (Davis, 1989).
Net Benefits consist of three categories: strategic, informational and transactional. Strategic benefits include competitive advantage, alignment, and customer relations benefits. Informational benefits include information access and information flexibility. Transactional benefits include communications efficiency, systems development efficiency, and business efficiency. These are the most important success measures as they capture the balance of positive and negative impacts on an organization. The ISP conceptual model incorporates these concepts.

3.7. Perceived Consequences

There are two approaches in a perceived consequence environment: “mandatory use” and “voluntary use.” In mandatory use, users are required to use a specific technology or system in order to perform their jobs (Brown, Massey, Montoya-Weiss, and Burkman, 2002). The user must use the system, regardless of any anticipated benefit. Mandatory use was considered a probable cause of mixed findings in TAM studies (Hartwick and Barki, 1994; Mathieson 1991; Taylor and Todd, 1995; Venkatesh and Davis, 2000). If a user is required to use a system, his or her intention is irrelevant (Brown et al., 2002). If a user is obligated to follow the information security policy, his intention to use ISP directly affects his or her perspective.

Some researchers have used the same model to study both mandatory and voluntary systems (e.g., Brown et al., 2002; Venkatesh and Davis, 2000; Venkatesh et al.,
One such study modeled voluntariness as a moderator of the relationship between intention *per se* and determinants of intention (Venkatesh et al., 2003).

A fundamental difference between a mandatory and a voluntary system are the organizational consequences that system use carries for the user. For the former, system use is mandated based on the organization’s aims and objectives. Users are obliged to use the system because that is the only way of accomplishing a given task (Adamson and Shine, 2003). Performance considerations are the user’s main concern (Taylor and Todd, 1995). System use can lead to reward or punishment. Hence, a user’s attitude toward use depends on whether he or she believes that such use will enhance his or her job performance or future promotion (Adamson and Shine, 2003) or result in punishment if he or she is reluctant to use the systems.

### 3.8. Gap in D&M IS Success Model and TAM

As previously noted, the ISP conceptual model adopts three D&M IS Success Model qualities: Service Quality, System Quality and Information Quality (see Figure 21). Business Factors create Service Quality at the organization level. Technology Factors create System Quality and Information Factors create Product Quality. All three qualities directly impact perceived consequences, perceived ease of use, perceived usefulness, intention to use and user satisfaction. However, in general, TAM and the D&M IS Success Model focus on the individual “user”; these models introduce additional factors
to explain how a user “perceives usefulness,” but ignore the essentially social processes of IS development and implementation (Bagozzi, 2007). Olson and Ives’ descriptive model is used to compensate for shortcomings in the D&M IS Success Model and TAM. Figure 22 indicates how Olson and Ives’ descriptive model factors are incorporated into the ISP conceptual model.

**Figure 22: ISP Conceptual Model and Descriptive Model**

In order to develop a comprehensive measurement model/instrument for a particular context, the constructs and measures should be systematically selected considering contingency variables, such as organizational structure, size, technology, and the individual characteristics of the system (Gable et al., 2003). To address these needs, Ives and Olson’s “Descriptive Model” evaluates “User Characteristics” and “Organizational Climate”. These two factors are incorporated into the ISP Conceptual Model.
To assess the validity of my ISP conceptual model I will use the Descriptive Model, which measures end-user satisfaction with information technology (IT) and has been widely accepted as an indicator of IT success (Gable et al., 2009). In the Descriptive Model, organizational climate and development characteristics constitute elements of the ISPCM’s Business Factors; these are considered to be a benefit of the IT system along with system quality and system acceptance (Figure 23). User characteristics, and user involvement are results of the usage of any IT system; system quality and system acceptance constitute the Value of IT (Figure 24). In Figures 23 and 24,

- The dotted blue line represents the Value of the IT system,
- The dotted green line represents the Use of the IT system,
- The dotted red line represents the Benefit of the IT system.

Figure 23: Benefits of the IT System in Olson’s Descriptive Model
3.9. Proposed ISP Conceptual Model

Figure 25a presents the conceptualization and operationalization of the ISP conceptual model development and figure 25b shows the final version of my proposed ISP conceptual model. Both figures involve a combination of the following concepts:

- Choo’s Adaptive Behavior (Information Needs, Information Acquisition, Information Products/Services, Information Distribution and Information Use) is applied to ISPCM’s Deployment and Information Usage Behavior Drivers (Figure 18).
- Delone and McLean’s System Quality, Information Quality and Service Quality are used to connect the ISPCM’s Information Usage Drivers and Information Deployment Drivers (see Figure 21).

ISPCM activates the following models for operationalization:
• Ives and Olson’s Descriptive Model’s (1984): User Characteristics and Organizational Climate are used to improve System Quality and System Acceptance.

• Davis’s TAM model (1989) and Delone and McLean’s IS Success Model are used to measure the ISPCM’s User Satisfaction and Organizational Net Benefit (see Figure 25).

Figure 25a: ISP Conceptual Model Development Process: Step 1

Figure 25b: ISP Conceptual Model Development Process: Step 2
Figures 25a and 25b present the ISP Model development process. Figure 26 shows the value of ISP, use of ISP and benefit of ISP. The dotted blue line is the Value of the IT System; the dotted green line is the Use of the IT System and the dotted red line is the Benefit of the IT System. Figure 26 shows the completed proposed ISP conceptual model with drivers. Figures 26 and 27 represent the completion of the proposed ISP conceptual model and its stages.

Figure 26: ISP Conceptual Model Value, Usage and Benefit

Figure 27: ISP Conceptual Model Stages
3.10. Conclusion of ISP Conceptual Model Development

The study described in this chapter represents an important step forward in the creation of a new model, the Information Security Policy Conceptual Model (ISPCM), and in the study of user perspectives and their impact on information satisfaction and ISPCM usage. My next step was to survey several hundred employees from two different types of companies: those with few or no security breaches; and those with numerous such breaches. A well-designed study will allow me to conclude that carefully considered ISP qualities will lead to increased user satisfaction, increased system usage and increased organizational performance.
Chapter 4: 2010 Research

This study investigates organizational ISP defects and describes what needs to be done to increase employee productivity and corporate return on security investment. Chapter four describes my survey of corporate ISP and my findings.

4.1.  2010 Survey Design

The goal of the survey was to identify firms that had either chosen or failed to implement ISPs and document their security records. Surveys were sent to 200 participants in five countries: Austria, Australia, Germany, Taiwan and the USA. The seven companies participating in the survey included start-up, small, medium and large corporations; participants were CEOs, Managers, Security Officers, IS developers and end users. Before sending out the survey, I met face-to-face with the IT Security Officers or CEOs of all seven companies to obtain their support.

4.2.  Research Questions

The first survey questions were designed to assess the return on security investment. They focus information security policy strengths and weaknesses. My goal was to determine whether demonstrating the flaws or weaknesses in a given company’s
Information Security Policy would motivate it to revise its policies in order to realize a
Return on Security Investment.

4.3. Sample and Data Collection

I surveyed 7 different companies on 4 continents. The companies ranged in size
from 50 employees to more than 40,000. I conducted face-to-face interviews with the
various company’s IT security officers or CEOs prior to sending out the surveys; of the
200 survey recipients, 146 replied. 33 respondents were not on the original email list.
The survey consisted of 60 questions (see Appendix B), in 16 different categories, under
5 different headings: Organization, Assets, Access, Systems and Operation.

4.4. Instrumentation and Results

The first part of the study focused on the organization rather than the individual.
The goal was to measure each company’s Information Security Policy in terms of
financial value. These questions did not ask whether nor not the individual actually used
an ISP.
The questions were based on personal experience and interviews with corporate IT security officers. The survey results indicated that the 50% of respondents in start-up, small and mid-sized firms did not know what a security policy was or how it functioned.

4.5. Conclusion

In response to the unsatisfactory results revealed by the survey, I decided to develop and test a conceptual model of an Information Security Policy (ISP) and to measure the proposed benefits that would accrue to organizations that implement and deploy such policies. A new, more comprehensive framework was required to investigate the interaction between the Deployment of an Information Security Policy and the Usage of an Information Security Policy and to assess whether these would lead to positive changes in organizational behavior.
The purpose of this study is to develop and test a conceptual model of an Information Security Policy (ISP), including processes, practices and technologies, and to measure the benefits that will accrue to the organization as a result of implementation and deployment (see Figure 28). A new, more comprehensive framework is required to investigate the interaction between deployment and usage behavior of information security policy drivers and determine whether this will lead to improved performance. As previously noted, ISP Value (service, system and product quality) has a profound influence on perceived ease of use (PEOU), perceived usefulness (PU) and perceived consequences (PC) and may ultimately lead to enhanced organizational performance benefit (see Figure 28).
This goal of this study is to evaluate the ISP conceptual model. The study concentrates on the ISP conceptual model’s deployment and usage drivers in order to answer the question: “Can the Information Security Policy Conceptual Model be a good predictor of ISP success as measured from the end user’s perspective?” In order to address this issue it is necessary to ask three additional questions:
1. What are the determinants of organizational performance benefit?

ISP Value (hereafter, ISPV) mediates between perceived consequences (PC), perceived ease of use (PEOU), and the perceived usefulness (PU) of the ISP. ISPV affects the user’s perspective (UP) of ISP use and leads to a positive organizational performance benefit (OPB). (ISPV -> US -> OPB)

- Is ISP service quality associated with organizational performance?
- Is ISP system quality associated with organizational performance?
- Is ISP product quality associated with organizational performance?

2. Do ISP conceptual model deployment drivers (including factors and qualities) define the successful value of ISP processes, practices and technologies in the user’s perspective?

- Does ISP Value affect perceived consequences? (ISPV -> PC)
- Does ISP Value affect individual Perceived Ease of Use and Perceived Usefulness? (ISPV -> PEOU/PU)
- Does ISP Value affect User Satisfaction? (ISPV -> US)

3. What are the determinants of User Satisfaction and ISP Use?

- Do Perceived Consequences affect User Satisfaction and ISP Use? (PC -> US)
- Does Perceived Ease of Use/Perceived Usefulness affect User Satisfaction and ISP Use? (PEOU/PU -> US)
• Does Perceived Ease of Use/Perceived Usefulness mediate the relationship between Perceived Consequences and User Satisfaction and ISP Use?

(PEOU/PU->PC->US)

Figure 29 – Proposed ISP Conceptual Model Measurement.

5.2. Research Propositions

Well-designed questions will help researchers address the right issues (Yin, 2003). This study seeks to demonstrate how user satisfaction with the ISP conceptual model will lead to organizational performance benefit (OPB). With regard to strategy and methodology, several propositions must be examined.

Proposition 1: Organizational Performance Benefit (OPB) can be achieved if adequate ISP value (ISPV) has been deployed. (ISPV -> OPB)

Rival proposition 1: ISPV does not have any positive impact on performance.
Proposition 2: User Satisfaction with ISP will occur if the Perceived Consequences (PC) of ISP use are significant (ISPV -> PC).

Rival proposition 2: User satisfaction with ISP will not occur if the Perceived Consequences of ISP are irrelevant.

Proposition 3: User Satisfaction with ISP will occur if the Perceived Ease of Use (PEOP) and the Perceived Usefulness (PU) of ISP are high (PEOU/PU -> US).

Rival proposition 3: User Satisfaction with ISP will not occur if the Perceived Ease of Use (PEOP) and the Perceived Usefulness (PU) of ISP are low.

Proposition 4: Organizational Performance Benefit will occur if ISP User Satisfaction is high (US -> OPB).

Rival proposition 4: Organizational Performance Benefit will not occur if ISP User Satisfaction is low.

5.3. Summary of Research Questions

The research questions can be summarized according to the following hypotheses:

H1: ISP Value affects Perceived Consequences. (ISPV -> PC)
    Perceived Consequences affect User Satisfaction. (PC -> US)
H2: ISP Value affects Perceived Ease of Use/Perceived Usefulness. (ISPV->PEOU/PU)

Perceived Ease of Use/Perceived Usefulness affects User satisfaction. (PEOU/PU -> US)

H3: ISP Value affects User satisfaction. (ISPV -> PEOU/PU)

Perceived Consequences mediate between Perceived Ease of Use/Perceived Usefulness and User Satisfaction. (PEOU/PU -> PC -> US) (e.g., if usage is mandated, Perceived Ease of Use/Perceived Usefulness is low; however, use may be motivated by fear of the consequences of not using the ISP; User Satisfaction will be low.)

H4: ISP Value affects User satisfaction. (ISPV -> US)

User Satisfaction directly affects Organization Performance Benefit. (US -> OPB)

Figure 29 demonstrates the operation of these hypotheses.
Chapter 6: RESEARCH METHODOLOGY

In the modern internet age, computer-based information changes constantly and dramatically and new threats arise on a daily basis. An ISP is one means of preventing or at least anticipating these threats. Ideally, an ISP should be perceived as providing a vital competitive edge to an organization. An ISP provides a secure way to share information among employees and protects organizations against hackers.

An Information Security Policy Model is, in essence, an information system (IS). However, the success of an ISP largely depends on user behavior. The IS literature reveals some of the factors affecting IS use, including: perceived information quality, system quality and service quality (Delone and McLean, 2003); user characteristics and organizational climate (Ives and Olson, 1984); and perceived usefulness and perceived ease of use (Technology Acceptance Model (TAM)) (Davis, 1989).

This study focuses on such constructs as perceived ISP Value (e.g., service, system, and information quality), Perceived Ease of Use (e.g., the ISP ensures that work objectives are clearly understood.), Perceived Usefulness (e.g., ISP products provide some tangible benefit), and Perceived Consequences (e.g., the ISP can prevent security breaches). These constructs are used to verify User Satisfaction and to evaluate the Organizational Benefits of ISP (e.g., improved productivity). An integrated ISP conceptual model was created to test the effect of the constructs described above on employee satisfaction, and to explore the relationship between the perceived ISP value
and User Satisfaction (see Chapter 3, Figure 14, and Figure 27 below). Figure 28 presents the ISP Conceptual Model’s drivers and factors, and Figure 29 shows the ISP Conceptual Model’s Measurement.

6.1. Rationale for Selecting the Research Methods

The scientific methods available for the research study include case studies, surveys, content analyses, and grounded theories. The present study relies on the survey method, which has been used extensively in Information Systems (IS) research (Ives and Olson, 1986). The following paragraphs discuss our rationale for selecting this method.

Surveys are used extensively in such fields as marketing, business, education, psychology, political science, sociology, social work, and library and information science (Powell, 1997). The academic study of management information systems (MIS) relies heavily on the careful application of these methods to answer research questions and test research hypotheses (Kraemer, 1991). Pinsonneault and Kraemer argue that survey data is collected from only a small fraction of the study population, but that it is collected in such a way that the findings can be generalized (Pinsonneault and Kramer, 1991). The targets of the survey may include service or manufacturing organizations, line or staff work groups, MIS departments, or various users of information systems such as managers,
professional workers, and clerical workers. Usually, the sample is large enough to allow extensive statistical analysis.

The survey approach encompasses both quantitative and qualitative analysis; data is collected by way of letters, email, web-based questionnaires, telephone interviews, and published statistics; the data is then analyzed using statistical techniques (Craemer et al., 1991; Gable, 1994; Goel and Chen, 2005). By studying a representative sample, the survey approach seeks to discover relationships that are common across organizations and, hence, to provide generalizable statements about the object of study (Craemer et al., 1991; Gable, 1994).

Yet, for a survey to succeed in explaining causal relationships or even in providing descriptive statistics, it must contain the right questions asked in the right manner (Gable, 1994). The researcher should, therefore, have a very good idea of the answers he or she anticipates before starting a survey (Kaplan and Duchon, 1988). Unfortunately, once the survey is underway, there is little one can do to correct omissions or to compensate for questions that are ambiguous or misunderstood (Gable, 1994). In order to avoid such pitfalls, the survey discussed here was pre-tested with IT professionals, managers and end users.
Traditional surveys normally consist of a methodology of verification rather than discovery (Gable, 1994). As noted above, this study focused on several constructs, including perceived ISP value (service, system, and information quality), Perceived Usefulness, and Perceived Ease of Use, to verify their effects on employee intentions to use ISP and to evaluate Organizational Benefit. The survey method was selected because survey research constitutes verification rather than discovery (Locke, 1989; Gable, 1994).

6.2 Binding the Case

One of the common problems associated with surveys is a tendency to ask questions that are too broad (Baxter and Jack, 2008). In order to avoid this, several authors have suggested placing strict boundaries on the scope of the study (Yin, 2003; Stake, 1995). A given study might be bound by: time and place (Creswell, 2003); time and activity (Stake, 1995); or definition and context (Miles and Huberman, 1994). Binding the scope of the study will ensure that the research remains reasonable and relevant.

In this study, we evaluated ISP value based on the user’s perspective. The scope of the study was bound by collecting data from small e-business companies only.
6.3 Time Table

The original purpose of this research was to identify the strengths and weaknesses of information security policy (ISP) for varying sizes and types of companies. The research was designed to address the following questions:

1. If the Enterprise reviews its Information Security Policy, finds flaws and implements a new strategy, will this lead to increased Return on Security Investment (ROSI)?

2. If the Enterprise implements an effective Information Security Policy, will this lead to increased Return on Security Investment (ROSI)?

The 2010 survey was designed to identify ISP defects and inefficiencies at the organizational level. Unfortunately, many participants could not adequately answer questions related to service and system quality. Question 1 asked whether “There is an information security policy, which is approved by the management, published and communicated as appropriate to all employees.” Question 53 asked whether “The business requirements for access control have been defined and documented.” Question 54 asked whether “The Access control policy….address[es] the rules and rights for each user or… group of users.” Responses were scored on the following 10 point scale:

1. Does not apply

2. Under review

3. Reviewed/Initial planning is under way
4. Only partially implemented

5. Minimal implementation and compliance

6. Room to improve

7. Full implementation and compliance

8. Satisfactory

9. Production running well

10. Best: no improvement required

More than 90% of participants responded to questions 1, 53 and 54 by choosing response 1: Does not apply. Hence, the results indicate that many of the companies surveyed do not have an effective ISP in place. Such companies may have a very basic policy such as a firewall, or rules governing intranet and internet practices, but, by and large, the study indicated that the ISP was either defective or deficient and that, consequently, ROSI is either low or non-existent. These results indicated that more research was needed and that an improved research protocol should focus on ISP value and user perceptions rather than cataloguing ISP defects.

This survey seeks to explain the relationship between ISP value, user acceptance, and behavioral intentions. Figure 29 presents the revised framework. Our objectives are to:
1. Focus on the ISP value of our ISP conceptual model.

2. Verify the proposed model, and empirically demonstrate how Perceived Consequences, Perceived Usefulness and Perceived Ease of Use influence the relationship between user perspectives and ISP Value.

This empirically integrated model will be useful to future research designed to test and develop ISP. The Table 2 presents our research time line.

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarter</td>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>Phase 1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Phase 2</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Phase 3</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase #</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>1 Research on ISP Inefficiency Issues in organizations</td>
</tr>
<tr>
<td></td>
<td>2 Literature Review</td>
</tr>
<tr>
<td></td>
<td>3 Survey – Original ISP Survey</td>
</tr>
<tr>
<td></td>
<td>4 Analysis 1st Survey and identified the problem</td>
</tr>
<tr>
<td>Phase 2</td>
<td>5 Literature Review for IS/IP model (process and practice)</td>
</tr>
<tr>
<td></td>
<td>6 ISPCM Development (including process and practice)</td>
</tr>
<tr>
<td></td>
<td>7 Pilot User testing ISPCM</td>
</tr>
<tr>
<td></td>
<td>8 Survey to find the degree of ISPCM process and practical impacts</td>
</tr>
<tr>
<td>Phase 3</td>
<td>9 Data collection</td>
</tr>
<tr>
<td></td>
<td>10 Data analysis</td>
</tr>
<tr>
<td></td>
<td>11 Finalize Results</td>
</tr>
</tbody>
</table>

Table 2: Research Time Line
6.4 Research Design

6.4.1 Data Selection

Our sample contains data provided by several hundred e-business users from a variety of companies. The participants were selected from two different types of companies: those with few security breaches and those with many. This controlled environment variable serves to validate the notion that acceptance and use of ISP will have a significant impact on organizational performance.

Data relating to publicly reported security breaches has been available in the US since 2005. These records document 536 million security breaches at 2677 different organizations, including government agencies, corporations, hospitals and educational institutions. Amongst these 2677 organizations, we decided to focus on firms that had reported security breaches in 2011 and could therefore provide recent data. A total of 399 firms reported security breaches in 2011. Next, we eliminated firms whose security breaches were not clearly described. Third, firms were ranked from high to low based on the severity of the breach. Fourth, we separated firms into two groups: high security

---

8 The list of 2677 firms was provided by Professor Goel.
breach and low security breach. Fifth, we either googled these firms in order to find a contact person or used the snowball\textsuperscript{9} method to find potential participants.

We anticipated that the low security breach group would display greater enthusiasm for such ISP qualities as Perceived Ease of Use, Perceived Usefulness, Perceived Consequences and User Satisfaction. We anticipated that the high security breach group would have a less favorable view of these.

6.4.2 Survey Instrument

The survey instrument is based on previous research, personal experience, IT expertise, and input from dissertation committee members. The purpose of a survey instrument is to measure the value of ISP processes, practices, and technologies and to capture end-user perceptions of ISP acceptance and utility.

In this study, constructs are used to rate the importance of each item. The measures shown in Appendix E were mainly adapted from relevant prior studies. The degree of scale is based on the Job Satisfaction Survey Method created by Paul E.

\textsuperscript{9} Snowball sampling (snowball) is a non-probability sampling technique in which existing study subjects recruit future subjects from among their acquaintances. Thus the sample group appears to grow like a rolling snowball. As the sample builds up, enough data is gathered to be useful for research. This sampling technique is often used in hidden populations which are difficult for researchers to access.
Spector (Spector, 1985). Spector developed the survey method that asks respondents to place their answers somewhere on a 6 point scale ranging from 1 (“Disagree very much”) to 6 (“Agree very much”).

Assessments of Perceived Ease of Use (PEOU), Perceived Usefulness (PU) and Behavioral Intent (BI) are adapted from the work of Davis (1989) Venkatesh and Davis (2000) and Ong and Lai (2007). The items relating to ISP value are adapted from the measurements defined by Delone and McLean (1992), and Ong and Lai (2007). An additional nominal scales questionnaire was used to collect basic information about respondents, including gender, age, education, and ISP experience. To ascertain the validity of research measures of ISP, a pilot test was conducted in order to assess the semantic content and readability of the questionnaire. Chapter seven discusses all multi-item scales, problems and difficulties, such as ambiguous wording, misunderstanding of technical terms, model–fit and required modifications.

6.4.3. Constructs of ISP value

As mentioned in the Chapter 3, the research model includes: an ISP value (service, system and product quality), which is part of a deployment driver; and a set of three antecedent variables (Perceived Ease of Use/ Perceived Usefulness (PEOU/PU) and Perceived Consequences (PC)) that are expected to influence ISP user satisfaction in the ISP Conceptual Model framework (see Figure 29).
6.4.3.1. Perceived ISP value

As discussed earlier, ISP value includes Service, System and Product Quality. Service Quality derives from Business Factors – environment, governing, leadership/IT teams, awareness and assets; System Quality derives from Technology Factors – secure, user-friendly, reactive, maintenance and bug-free; Product Quality derives from Information Factors – correctness, suitability, clear, fullness and up-to-date (Delone and McLean, 1992, 2003; Choo, 2002; Davis, 1989) (see Figure 14). Service, System and Product Quality are the bridges between Deployment Factors and Usage Drivers.

Perceived ISP value is obvious in an e-business or web-based information system’s overall performance and can be measured by user perceptions of ISP value in the ISP conceptual model. In such instances, ISP value may be defined in terms of the desired characteristics of ISP processes, practices and technologies. The support functions of an ISP value (Service, System and Information Quality) are the qualities valued by IS users (Delone and McLean, 2003; Ong and Lai, 2007).

The operationalized constructs of ISP value (Service Quality, System Quality and Product Quality) are presented in Table 3. The corresponding survey can be found in Appendix E.
6.4.3.2. Constructs of Service Quality

Service Quality is concerned with whether the IS has up-to-date hardware and software (e.g., assets), whether the ISP is dependable (e.g., reliability), whether ISP employees, IT teams or management give prompt service to users (e.g., responsiveness), whether ISP employees have the knowledge to do their job well (e.g., awareness), whether ISP provides a secure environment for employees (e.g., assurance), and whether IT teams and management have the user’s best interests at heart (e.g., empathy). Service Quality is composed of such constructs as: tangible, contemporary, reliability, responsiveness, assurance and empathy (see Figure 14 and Table 3).
6.4.3.3. Constructs of System Quality

Delone and McLean argued that System Quality is concerned with whether or not there are bugs in the system, the consistency of the user interface, ease of use, quality of documentation, and sometimes, the quality and maintainability of the program code. System Quality is measured in terms of ease-of-use, functionality, reliability, flexibility, data quality, portability, integration, and importance (Delone and McLean, 2004). System Quality consists of five constructs: simplicity (user friendly), security (secure), speed (reactive), scalability (maintenance) and efficiency (bug-free systems) (see Figure 14 and Table 3).

6.4.3.4. Constructs of Product Quality

As mentioned earlier, information is produced by system and services; Product Quality, therefore, is Information Quality. According to Delone and McLean (2003), Product Quality is concerned with such issues as relevance, timeliness, and accuracy. Information Quality measures include accuracy, relevance, understandability, completeness, current, dynamism, personalization, and variety (D’Ambra, 2001; Molla, 2001; Palmer, 2002). Researchers are strongly encouraged to include Information Quality measures as a critical dimension of their success measurement constructs (Petter et al., 2009). In this ISP study, Product Quality consists of five constructs: accuracy, relevance, understandability, completeness and current. A number of studies have found
these constructs to be suitable to this type of analysis (Goel and Chen, 2005; Delone and McLean, 2004; D'Ambra, 2001; Molla, 2001; Palmer, 2002) (see Figure 14 and Table 3). Table 3 presents the operationalization of ISP construct values. The survey questionnaire can be found in Appendix E, section B.

6.4.4. Constructs of the ISP User’s Perspective

Several empirical studies indicate that Service Quality, System Quality and Product/Information Quality positively affect Perceived Usefulness (PU) (Delone and McLean, 1992; Seddon, 1997), Perceived Ease of Use (PEOU) (Lin and Lu, 2000) and Perceived Consequences (PC). The research model postulates that the ISP Conceptual Model is affected by ISP value and, therefore, measures PC, PEOU, PU and User Satisfaction.

An individual generally adopts a new technology based on its functionality (Davis 1989). In TAM, PEOU is antecedent to PU. Several studies have indicated that PEOU has a positive effect on PU in online contexts (Chen et al., 2002; Davis et al., 1989; Lin and Lu, 2000; Lu et al., 2007; Shih, 2004). We contend that if ISP procedures are easy to follow, users will consider information systems beneficial. The ISP Conceptual Model incorporates these assumptions.
Perceived consequences may be determined by organizational ISPs that have a direct impact on employee behavior. Failure to adhere to such policies may have harmful consequences and cause an employee to adhere to an ISP out of fear. Compliance with such policies, on the other hand, may lead to recognition or promotion. A positive experience will undoubtedly lead to improved Perceptions of Usefulness and Ease of Use (PU/PEOU). These assumptions are incorporated into the ISP Conceptual Model.

Table 4 demonstrates User Satisfaction with ISP value. The ISP value is measured on the basis of Perceived Consequences, Perceived Ease of Use, and Perceived Usefulness. The questionnaire relating to this table may be found in Appendix E, section B.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Factors</th>
<th>Operationalized Measure</th>
<th>Survey questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Behavior Intention</td>
<td>Perceived Consequence</td>
<td>To what degree of consequence for using ISP</td>
<td>App E, Section B. (Q17/18)</td>
</tr>
<tr>
<td>(Adapted from Goel &amp; Chen 2008, Davis et al. 1989, 2000; 2003)</td>
<td>Perceived Ease of Use</td>
<td>To what degree of ISP can provide IS to improve my performance</td>
<td>App E, Section B. (Q19/20)</td>
</tr>
<tr>
<td></td>
<td>Perceived usefulness</td>
<td>To what degree of ISP is helpful to my work.</td>
<td>App E, Section B. (Q21/23)</td>
</tr>
<tr>
<td></td>
<td>User Intention to use</td>
<td>To what degree of ISP you will use in the future</td>
<td>App E, Section B. (Q23/24)</td>
</tr>
</tbody>
</table>

**Table 4: Operationalization of User Perspective Constructs**

### 6.4.5. Constructs of Organizational Performance

The challenge for the researcher is to clearly define the stakeholders amongst whom and the context in which organizational net benefits are to be measured (Delone
and McLean, 2002). In this study the organizational performance construct is adopted from research conducted by Goel and Chen, Buyter, Tallon and Arumugam (Goel and Chen, 2005; Buyter et al., 2001; Tallon et al., 2000; Arumugam et al., 2011). Organizational performance is measured on the basis of compliance, modernization, adaptation, productivity, reputation and revenue. Table 5 represents the operationalization of the organizational performance construct. The questionnaire relevant to this table may be found in Appendix E, section F.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Factors</th>
<th>Operationalized Measure</th>
<th>Survey questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>To what level of reducing firm's security breaches</td>
<td>App E, Section B. (Q25)</td>
<td></td>
</tr>
<tr>
<td>Modernization</td>
<td>To what level of firm's IS modernization is provided</td>
<td>App E, Section B. (Q26)</td>
<td></td>
</tr>
<tr>
<td>Adaptation</td>
<td>To what level of employees' adaptation acceptance of tight security rules</td>
<td>App E, Section B. (Q27)</td>
<td></td>
</tr>
<tr>
<td>Productivity</td>
<td>To what level of organization's productivity is increased and computer downtime decreased</td>
<td>App E, Section B. (Q28)</td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>To what level of firm's reputation is improved</td>
<td>App E, Section B. (Q29)</td>
<td></td>
</tr>
<tr>
<td>Revenue</td>
<td>To what level of firm's revenue is increased</td>
<td>App E, Section B. (Q30)</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Operationalization of Organizational Performance Constructs
Chapter 7: Testing ISP Conceptual Model Methods

In order to test the ISP Conceptual Model and all individual hypotheses, I will rely on Structural Equation Modeling (SEM), using an Analysis of Moment Structures (AMOS) program. Structural Equation Modeling (SEM), also known as analysis of covariance structures, or casual modeling (Byrne, 2001), has a number of practical advantages, including multiple regression, path analysis and analysis of variance (ANOVA), and has proven useful across a wide range of disciplines (Smith et al., 2004).

The major limitations of multiple regression analysis are as follows: (1) there is one dependent variable and a number of independent (explanatory) variables; (2) multiple regression analysis assumes that all constructs are free of measurement error. The analysis path assumes a unidirectional flow of relations between variables (Maruyama, 1998) and does not formally adjust the coefficient of each independent variable for estimated measurement error. SEM, on the other hand, conceptualizes a variety of relations between a range of variables. SEM can account for estimated measurement error in latent variables (including those associated with interaction terms) and can provide measures of fit to assess an entire model (Smith et al., 2004). SEM also

---

10 AMOS (Analysis of Moment Structures) is an easy-to-use program for visual SEM. With AMOS, you can quickly specify, view, and modify your model graphically using simple drawing tools. Then you can assess your model’s fit, make any modifications, and print out a publication-quality graphic of your final model.
encompasses a number of well-known conventional techniques, including the general linear model and common factor analysis (Smith et al., 2004).

The content validity of this research should be acceptable given that the questionnaire was adapted from validated models, as discussed in chapters 2 and 3.

7.1. Structure Equation Modeling (SEM)

In recent years, structural equation modeling (SEM) has become one of the most commonly used multivariate data analysis techniques in Information Systems (IS) research (Henriksen et al., 2007). SEM allows for the simultaneous analysis of a series of structural equations (Smith, 2004). Hoyle defines SEM as “a comprehensive statistical approach to testing hypotheses about relations among observed and latent variables” (Hoyle, 1995). Model fit criteria include goodness-of-fit indicators, modification indices, error variances, significance of loadings and residual indices (Kline, 2004). The purpose of SEM is to estimate the scale and significance of each path, and provide an indication of the overall ability of the proposed model to fit the sample data (Tallon et al., 1999). SEM is particularly useful in analyzing complex designs since it can identify multiple and interrelated dependence relationships between unobserved concepts like latent variables (Segars et al., 2005) as well as relations between observed and unobserved latent variables (Tomarken et al., 2005).
In addition to estimating multiple and interrelated dependent relationships between variables, SEM may also be used to represent a latent variable in these relationships while accounting for errors associated with imperfect measurement of variables (Hair et al., 1995). Each construct or latent variable may be conceptualized by the use of measured indicators.

7.2. **Confirmatory Factor Analysis (CFA) and Exploratory Factor Analysis (EFA)**

This study evaluated two factor analysis methods, Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA), and determined that CFA was the better fit.

EFA is appropriate in situations in which the links between observed and latent variables are unknown or uncertain (Byrne, 2001). It does not encompass high-order factors or multidimensionality and is, therefore, inapplicable to our study (Rubio et al., 2001). We will rely, instead, on Confirmatory Factor Analysis (CFA) in order to verify the proposed factor structure and determine whether any significant modifications are needed (Hair et al., 1998). CFA uses a set of factors to account for covariance among a set of observed variables (Bollen, 1989; Sorbom et al., 1989) and provides plausible alternative models that can be tested using new data. Confirmatory studies serve to provide more precise model specifications and to increase confidence in the measures used in making decisions and testing substantive hypotheses (Chang et al., 2004). Given
that the ISP Conceptual Model contains high-order factors, we employed confirmatory factor analysis to evaluate construct validities.

7.3 Assessment of Measurement Model

Figure 30 represents a CFA structural model. By convention, squares or rectangles represent observed variables, circles or ellipses represent factors or latent variables, uni-directional arrows(->) represent regressions or residuals, and bi-directional arrows (<->) represent correlations or covariances between pairs of variables. Researchers use these symbols within the framework of four basic configurations:

- Path coefficient for regression of an observed variable onto an unobserved latent variable (or factor).
- Path coefficient for regression of one factor onto other factors.
- Measurement error associated with an observed variable.
- Residual error in the prediction of an unobserved factor.

The factor analysis model expresses the variation and covariation in a set of observed continuous variables $y$ ($j = 1$ to $p$) as a function of factors $\eta$ ($k = 1$ to $m$) and residuals $\epsilon$ ($j = 1$ to $p$).

For person $i$,

$$y_{i1} = v_1 + \lambda_{11} \eta_{i1} + \lambda_{12} \eta_{i2} + \ldots + \lambda_{1k} \eta_{ik} + \ldots + \lambda_{1m} \eta_{im} + \epsilon_{i1}$$

$$\ldots$$

$$y_{ij} = v_j + \lambda_{j1} \eta_{i1} + \lambda_{j2} \eta_{i2} + \ldots + \lambda_{jk} \eta_{ik} + \ldots + \lambda_{jm} \eta_{im} + \epsilon_{ij}$$
\[ y_{ip} = \nu_p + \lambda p_1 \eta_{i1} + \lambda p_2 \eta_{i2} + \ldots + \lambda p_k \eta_{ik} + \ldots + \lambda p_m \eta_{im} + \epsilon_{ip} \]

where \( \nu_j \) are intercepts
\( \lambda_{jk} \) are factor loadings
\( \eta_{ik} \) are factor values
\( \epsilon_{ij} \) are residuals with zero means and correlations of zero with the factors

In matrix form, \( y_i = \nu + \Lambda \eta + \epsilon_i \),

Where \( \nu \) is the vector of intercepts \( \nu_j \),
\( \Lambda \) is the matrix of factor loadings \( \lambda_{jk} \),
\( \Psi \) is the matrix of factor variances/covariances, and
\( \Theta \) is the matrix of residual variances/covariances

with the population covariance matrix of observed variables \( \Sigma \),
\[ \Sigma = \Lambda \Psi \Lambda' + \Theta. \]

Formulas for The Path Diagram:
\[ y_{i1} = v_1 + \lambda_{11} f_{i1} + 0 f_{i2} + \epsilon_{i1} \]
\[ y_{i2} = v_2 + \lambda_{21} f_{i1} + 0 f_{i2} + \epsilon_{i2} \]
\[ y_{i3} = v_3 + \lambda_{31} f_{i1} + 0 f_{i2} + \epsilon_{i3} \]
\[ y_{i4} = v_4 + 0 f_{i1} + \lambda_{42} f_{i2} + \epsilon_{i4} \]
\[ y_{i5} = v_5 + 0 f_{i1} + \lambda_{52} f_{i2} + \epsilon_{i5} \]
\[ y_{i6} = v_6 + 0 f_{i1} + \lambda_{62} f_{i2} + \epsilon_{i6} \]

Elements of \( \Sigma = \Lambda \Psi \Lambda' + \Theta \):

Variance of \( y_1 = \sigma_{11} = \lambda_{11} \)
\[ 2 \psi_{11} + \theta_{11} \]
Covariance of \( y_1, y_2 = \sigma_{21} = \lambda_{11} \psi_{11} \lambda_{21} \)
Covariance of \( y_1, y_4 = \sigma_{41} = \lambda_{11} \psi_{21} \lambda_{42} \)
Figure 30: Example of CFA Structural Model

Figure 31 represents the proposed CFA Structural ISP Conceptual Model; the proposed model hypothesizes 30 observed variables and 8 latent variables. Rectangles indicate observed variables, which are linked to their corresponding latent variables by arrows; arrows signify that observed indicators provide a measure of latent variables (Smith et al., 2004). Each observed indicator is associated with an error term (e₁, e₂, or e₃), indicating the degree of error associated with measurement of the observed indicators. Items such as SRQ1, STQ1, PDQ1 are observed variables that may be directly measured by survey items (Smith et al., 2004). There is a further error term associated with each endogenous latent variable, which indicates the prediction error associated with each dependent variable (d₁, d₂)\(^\text{11}\) (Smith et al., 2004). Latent variables are unobserved

\(^\text{11}\) This is residual error in the prediction of an unobserved factor.
variables and are represented by circles (Smith et al., 2004). In this study, latent variables include such constructs as Service Quality, System Quality, Information Quality, User Perspectives and Organizational Performance Benefits. Table 6 aligns the 30 observed variables with the constructs used in the survey questions. The confirmatory factor analysis in AMOS software is used to analyze construct validities.

Figure 31: The Proposed CFA Structural ISP Conceptual Model
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SRQ1</strong></td>
<td>My company’s Information Security Policy provides a highly secure information environment.</td>
</tr>
<tr>
<td><strong>SRQ2</strong></td>
<td>My company’s Information Security Policy provides a reliable IT Team including helpdesk.</td>
</tr>
<tr>
<td><strong>SRQ3</strong></td>
<td>My company’s Information Security Policy rules and regulations takes into account the interests and needs of the users.</td>
</tr>
<tr>
<td><strong>SRQ4</strong></td>
<td>My company’s Information Security Policy regulates that IT helpdesk responds to request in a timely manner.</td>
</tr>
<tr>
<td><strong>SRQ5</strong></td>
<td>My company’s Information Security Policy provides up-to-date equipment (e.g., Hardware, Software)</td>
</tr>
<tr>
<td><strong>STQ1</strong></td>
<td>My company’s Information Security Policy has adequate security protection against internal unauthorized access and external hackers.</td>
</tr>
<tr>
<td><strong>STQ2</strong></td>
<td>My company’s Information Security Policy regulated information systems, making them simple to use by containing user-friendly features.</td>
</tr>
<tr>
<td><strong>STQ3</strong></td>
<td>My company’s Information Security Policy creates excessive delays in information systems response time.</td>
</tr>
<tr>
<td><strong>STQ4</strong></td>
<td>My company’s Information Security Policy ensures that the information systems are easy to maintain and to modify.</td>
</tr>
<tr>
<td><strong>STQ5</strong></td>
<td>My company’s Information Security Policy ensures that the information systems are highly stable.</td>
</tr>
<tr>
<td><strong>PDQ1</strong></td>
<td>My company’s Information Security Policy is free of technical and information errors.</td>
</tr>
<tr>
<td><strong>PDQ2</strong></td>
<td>My company’s Information Security Policy does not include unnecessary information.</td>
</tr>
<tr>
<td><strong>PDQ3</strong></td>
<td>My company’s Information Security Policy does not include unnecessary information.</td>
</tr>
<tr>
<td><strong>PDQ4</strong></td>
<td>My company’s Information Security Policy is easy to read and comprehend.</td>
</tr>
<tr>
<td><strong>PDQ5</strong></td>
<td>My company’s Information Security Policy is current with information technology (e.g., Latest hacker’s threats and current equipment.)</td>
</tr>
<tr>
<td></td>
<td>Item Code</td>
</tr>
<tr>
<td>---</td>
<td>-----------</td>
</tr>
<tr>
<td>15</td>
<td>DQ6</td>
</tr>
<tr>
<td>17</td>
<td>PC1</td>
</tr>
<tr>
<td>18</td>
<td>PC2</td>
</tr>
<tr>
<td>19</td>
<td>PEOU3</td>
</tr>
<tr>
<td>20</td>
<td>PEOU4</td>
</tr>
<tr>
<td>21</td>
<td>PU5</td>
</tr>
<tr>
<td>22</td>
<td>PU6</td>
</tr>
<tr>
<td>23</td>
<td>US7</td>
</tr>
<tr>
<td>24</td>
<td>US8</td>
</tr>
<tr>
<td>25</td>
<td>OPB1</td>
</tr>
<tr>
<td>26</td>
<td>OPB2</td>
</tr>
<tr>
<td>27</td>
<td>OPB3</td>
</tr>
<tr>
<td>28</td>
<td>OPB4</td>
</tr>
<tr>
<td>29</td>
<td>OPB5</td>
</tr>
<tr>
<td>30</td>
<td>OPB6</td>
</tr>
</tbody>
</table>

Table 6: Items Measure for the Information Security Policy
7.3.1. Assessment of Methods and Sample Size

Maximum-likelihood estimation (MLE) may be applied to a given data set or statistical model in order to estimate the model's parameters. Maximum Likelihood (ML) is the preferred method for selecting and evaluating models (Hu et al., 1995; Hoyle et al., 1995; Smith et al., 2004) and is relatively unbiased (Shah et al., 2005).

Suppose there is a sample $X_1, X_2…X_n$ of $n$ independent and identically distributed random variables (iid), coming from a distribution with an unknown probability density function (pdf) $f_0(\cdot)$. It is, however, surmised that the function $f_0$ belongs to a certain family of distributions $\{ f(\cdot|\theta), \theta \in \Theta \}$, called the parametric model, so that $f_0 = f(\cdot|\theta_0)$. The value $\theta_0$ is unknown and is referred to as the "true value" of the parameter. It is desirable to find some estimator which would be as close to the true value $\theta_0$ as possible. Both the observed variables $x_i$ and the parameter $\theta$ can be vectors (Aldrich, 1997; Basu, 1998).

To use the method of maximum likelihood, one first specifies the joint density function for all observations. For an iid sample this joint density function will be

$$f(x_1, x_2, \ldots, x_n \mid \theta) = f(x_1 \mid \theta) \cdot f(x_2 \mid \theta) \cdot \ldots \cdot f(x_n \mid \theta).$$

Now we look at this function from a different perspective by considering the observed values

$x_1, x_2…x_n$ to be fixed "parameters" of this function, whereas $\theta$ will be the function's
variable and is allowed to vary freely. From this point of view this distribution function will be called the likelihood:

\[ \mathcal{L}(\theta | x_1, \ldots, x_n) = f(x_1, x_2, \ldots, x_n | \theta) = \prod_{i=1}^{n} f(x_i | \theta). \]

In practice it is often more convenient to work with the logarithm of the likelihood function, called the log-likelihood:

\[ \ln \mathcal{L}(\theta | x_1, \ldots, x_n) = \sum_{i=1}^{n} \ln f(x_i | \theta), \]

or its scaled version, called the average log-likelihood

\[ \hat{\ell} = \frac{1}{n} \ln \mathcal{L}. \]

The hat over \( \ell \) indicates that it is akin to some estimator. Indeed, \( \hat{\ell} \) estimates the expected log-likelihood of a single observation in the model.

The method of maximum likelihood estimates \( \theta_0 \) by finding a value of \( \theta \) that maximizes

\[ \hat{\ell}(\theta | x). \] This method of estimation is a maximum likelihood estimator (MLE) of \( \theta_0 \):

\[ \hat{\theta}_{\text{MLE}} = \arg \max_{\theta \in \theta} \hat{\ell}(\theta | x_1, \ldots, x_n). \]

ML performs considerably well with a small sample size (i.e., no more than 200) (Alstöm and Olsson, 2000). This research will use Maximum Likelihood (ML) since the research sample is going to have sample size \( 100 < n < 200 \).
A suggested rule of thumb for SEM is a minimum sample size of 100 (Medsker et al., 1994; Boomsma, 1982; Russell, 2002; Mak et al., 2001). If the sample size is smaller than 100 the “bootstrapping” method (West et al., 1995; Yung and Bentler, 1996) can be used to compensate for the small sample size (Smith et al., 2004). Bootstrapping is a resampling procedure in which the researcher’s data set is treated as a population. Cases from the original data set are randomly selected to create other data sets with the same number of observations as the original (Kline, 1998). In this study the sample size will meet both the SEM and ML boundaries.

In AMOS, the maximum likelihood estimation (MLE) value uses a default setting: the required information is conveyed to the program by selecting the “Estimation” tab in the “Analysis Properties” dialogue box and then checking off the estimation procedure desired.

7.3.2. Data Screening

The problems associated with missing scores and the inability of software packages to deal with incomplete data are critical issues in SEM (Byrne, 2001). However, when conducting a survey, there will always be incomplete data. Data screening is the precursor to SEM analysis (Hair et al., 1998). Missing data will result in convergence failures, biased parameter estimates, and inflated fit indices (Brown, 1994; Muthen et al., 1987). Because incomplete data can seriously bias conclusions drawn
from an empirical study, this issue needs to be addressed (Byrne, 2001). The extent to which such conclusions will be biased depends on both the amount and the pattern of the missing values. Widely cited guidelines relating to the pattern of incomplete data have been derived from the seminal work of Rubin, Allsion and Little (Rubin, 1976; Allison, 1987; and Little and Rubin, 1987).

A number of model estimation methods are based on the assumption of normality. As a result, non-normal data may result in inflated goodness-of-fit statistics and underestimated standard errors (MacCallum, 1995). The Expectation-Maximization (EM) algorithm is commonly used to manage missing data (Shah et al., 2005) and reduce the effect of incomplete data on reliability (Hair et al., 1998; Enders, 2003).

The following section examines the Expectation–Maximization (EM) algorithm (Gupta and Chen, 2010). In statistics, an Expectation–Maximization (EM) algorithm is an iterative method for finding maximum likelihood (ML) or maximum a posteriori (MAP) estimates of parameters in statistical models, where the model depends on unobserved latent variables. The EM iteration alternates between performing an expectation (E) step, which computes the expectation of the log-likelihood evaluated using the current estimate for the parameters, and a maximization (M) step, which computes parameters maximizing the expected log-likelihood found on the (E) step.
These parameter-estimates are then used to determine the distribution of the latent variables in the next (E) step.

Given a statistical model consisting of a set $X$ of observed data, a set of unobserved latent data or missing values $Z$, and a vector of unknown parameters $\theta$, along with a likelihood function

$$L(\theta; X, Z) = p(X, Z | \theta),$$

the maximum likelihood estimate (MLE) of the unknown parameters is determined by the marginal likelihood of the observed data:

$$L(\theta; X) = p(X | \theta) = \sum_Z p(X, Z | \theta)$$

However, this quantity is often intractable.

The EM algorithm seeks to find the MLE of the marginal likelihood by iteratively applying the following two steps: (1). Expectation step (E step): calculate the expected value of the log likelihood function, with respect to the conditional distribution of $Z$ given $X$ under the current estimate of the parameters $\theta^{(t)}$:

$$Q(\theta | \theta^{(t)}) = E_{Z|X,\theta^{(t)}} [\log L(\theta; X, Z)]$$

Maximization step (M step): find the parameter that maximizes this quantity:
In typical models to which EM is applied:

1. The observed data points $X$ may be discrete (taking values in a finite or countably infinite set) or continuous (taking values in an uncountably infinite set). There may in fact be a vector of observations associated with each data point.

2. The missing values (aka latent variables) $Z$ are discrete, drawn from a fixed number of values, and there is one latent variable per observed data point.

3. The parameters are continuous and are of two kinds: parameters that are associated with all data points; parameters that are associated with a particular value of a latent variable (i.e., associated with all data points whose corresponding latent variable has a particular value).

AMOS assumes that missing data is a random event, yet, it is difficult to determine whether this assumption is valid or what it means in practice (Rubin, 1976). AMOS recognizes missing data in many formats, e.g., ASCII, and provides several advanced methods for handling missing data.

### 7.3.3. Treatment of Non-normal Data
One critically important assumption associated with the SEM methodology is that the data has a multivariate normal distribution. Violation of this assumption can seriously invalidate statistical hypothesis-testing such that the normal theory test statistics may not reflect an adequate evaluation of the model under study (Hu, Bentler, and Kano, 1992; West, Finch, and Curran, 1995). One approach to dealing with multivariate non-normal data is to use the “bootstrapping” approach described in section 7.3.1 (West et al., 1995; Yung and Bentler, 1996).

7.2.4 Model Fit Methods

Of primary interest in SEM is the extent to which a hypothesized model “fits,” or adequately describes, the sample data (Byrne, 2010). The model-fitting process can be summarized as follows:

\[ \text{Data} = \text{Model} + \text{Residual} \]

where Data represent score measurements related to observed variables derived from persons comprising the sample, Model represents the hypothesized structure linking observed variables to latent variables (and in some models, linking particular latent variables to one another), and Residual represents the discrepancy between the hypothesized model and observed data (Byrne, 2001).
Ideally, the evaluation of model fit should derive from a variety of perspectives and be based on such criteria as the adequacy of the model as a whole and parameter estimates (Byrne, 2001). Assessing model fit is one of the more complicated tasks performed by SEM (Smith et al., 2004; Shah et al., 2005). In SEM models, the latent variable model represents the structural model fit, and generally, the hypotheses of interest (Shah et al., 2005). Researchers must provide a clear definition of each index (Hoyle and Panter, 1995) and should utilize the following statistical methods to measure model fit: the Comparative Fit Index (CFI); the Goodness-of-Fit Index (GFI); the Tucker-Lewis Index (TLI); the Root Mean Square Error of Approximation (RMSEA); the Standardized Root Mean Square Residual (SRMR); and $\chi^2$/df (Smith et al., 2004).

Statistical tests for indicators of model fit are problematic, insofar as their power is dependent on sample size (Hox et al., 1998). Chi-square ($\chi^2$) tests may not be good indicators of model fit due to sensitivity with regard to sample size (Russel, 2002; Hu and Bentler, 1995; Bentler, 1990; Schumaker and Lomax, 1996; Fan et al., 1999; Jackson, 2003; Mak et al., 2001; Etezadi-Amoli et al., 1996). Chi-square ($\chi^2$) tests are reliable for sample sizes between 100 and 200 (Hair et al., 1995). If the sample size is not between 100 and 200, then the $\chi^2$/df ratio can replace Chi-square ($\chi^2$) tests. A $\chi^2$/df ratio yielding a value of five or less indicates a reasonable model fit (Adams et al., 1992; Doll et al., 1994). Some researchers maintain that a $\chi^2$/df ratio of less than 3 is a more reliable indicator of good fit (Hayduk, 1987; Pituch and Lee, 2004; Moore, 2000). We concur and will adopt a cutoff value of 3 in our study.
Related indices include the Normed Fit Index (NFI) and the Comparative Fit Index (CFI) (Bentler and Bonett, 1980; Bentler, 1990). The Comparative Fit Index (CFI) is a normed relative non-centrality index and is less affected by sample size (Russel, 2002; Hu and Bentler, 1995, Tallon et al., 1999; Fan et al., 1999). It estimates each non-centrality parameter by the difference between its T statistic and corresponding degrees of freedom (Deng et al., 2003); it is less biased than NFI (Bentler, 1990) or the Chi-square test (Kline, 1998). A CFI index value exceeding 0.90 represents a good fit (Hagger et al., 2004; Bentler, 1990).

The Goodness of Fit Index (GFI), meanwhile, measures the relative amount of observed variance and covariance in the model (Hoyle and Panter, 1995). GFI is moderately dependent on sample size (Anderson and Gerbing, 1984; Fan et al., 1999; Hoyle and Panter, 1995) and provides a meaningful interpretation (Hoyle and Panter, 1995) of the observed variances and covariance.

The Root Mean Square Error of Approximation (RMSEA) is used to evaluate the approximate fit of the model (Kaplan, 2000). RMSEA is minimally influenced by sample size (Fan et al., 1999). A RMSEA value less than 0.08 provides some support for the proposed model (Hair et al., 1995; Browne and Cudeck, 1993) yet the RMSEA value must be equal to or less than 0.06 to indicate a truly close fit (Hu and Bentler, 1999).
Residual values represent the discrepancy between elements in the sample and those in the restricted variance and covariance matrices; one residual represents each pair of observed variables. In a well-fitting model, these values will be close to zero and evenly distributed among all observed variables; large residuals associated with particular parameters indicate misspecification, thereby affecting overall model fit (Byrne, 2001).

The Standardized Root Mean Square Residual (SRMR) provides an overall average of the size of residuals. A combined RMSEA of 0.06 and SRMR of 0.08 indicate a good fit (Loehlin, 2004). A SRMR value less than or equal to 0.08 indicates a better fit (Hu and Bentler, 1999; Hagger et al., 2004). A GFI greater than 0.08 combined with a SRMR approaching 0.05 would also indicate a good fit (Etezadi-Amoli and Farhoomand, 1996).

Of the models discussed in the preceding, the Chi-Square Index, the Comparative Fit Index (CFI), the Root Mean Square Error of Approximation (RMSEA) and the Tucker and Lewis Index (TLI) are the most suitable for one-time analysis (Schreiber et al., 2006). Table 7 summarizes the application of the cutoff criteria generated by these indices to our ISP Conceptual Model (Schreiber et al., 2006).
Table 7: The Recommendation Level of Goodness-of-Fit Test Cutoff Criteria

<table>
<thead>
<tr>
<th>Goodness-of-fit test Indexes</th>
<th>Shorthand</th>
<th>Recommendation level</th>
<th>Categorical data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-square</td>
<td>$\chi^2$</td>
<td>$\chi^2/df &lt; 2$ or $3$</td>
<td></td>
</tr>
<tr>
<td>Comparative Fit Index</td>
<td>CFI</td>
<td>$&gt; = .95$ for acceptance</td>
<td>0.95</td>
</tr>
<tr>
<td>Comparative fit index</td>
<td></td>
<td>$&gt; = .95$ for acceptance</td>
<td>0.96</td>
</tr>
<tr>
<td>Tucker-Lewis Index</td>
<td>TLI</td>
<td>1 &lt; TLI &lt; 0 for acceptance</td>
<td></td>
</tr>
<tr>
<td>Root Mean Square Error of Approximation</td>
<td>RMSEA</td>
<td>$&lt; .06$ to $.08$ with confidence interval</td>
<td>$\leq 0.06$</td>
</tr>
</tbody>
</table>

7.4. Analysis Test of the Proposed ISP Conceptual Model

The preceding section discussed the initial analysis of proposed model testing and fit criteria. Following survey and data analysis, the next step is to determine whether the proposed model is a good fit. If index values meet the recommendation levels indicated in Table 6, the proposed model is a good fit. AMOS provides standard residuals and modification indices (MI) to help identify which positions in the model may impact model fit.
7.5 Model Modification

When a model is not a good fit, the Modification Index (MI) may be used to rectify the situation (Hoyle, 1995). When test results indicate misspecification, such as an inadequate fit between the sample and the restricted variance and covariance matrices, it is necessary to determine the source of the problem (Byrne, 2001). Assessments of model adequacy focus on two types of information: residuals and modification indices (Byrne, 2001); high residuals between items suggest that inter-correlations are not well modeled (MacCallun, 1986; Anderson and Gerbing, 1984). In such instances, AMOS may be used to help compute MI and assist in the modification process (Hox and Becher, 1998).

7.6 Discussion and Implications

This study is designed to evaluate a new, comprehensive ISP Conceptual Model and uses the paradigm of security breaches reported in 2011 to validate the proposed model. ISP value, which includes Service Quality, System Quality and Information Quality, is the determinant of organizational performance and acts as the bridge between Deployment Drivers and Usage Drivers (see Figure 31). One of the chief contributions of this study is the ability to demonstrate the impact that ISP Value has on Organizational Performance. The conceptual model is comprised of three constructs: ISP Deployment Constructs (includes ISP Service Quality, System Quality and Information Quality), Usage Constructs, and Organizational Performance Constructs.
This study synthesizes and expands upon well established theories and models in the Information Systems (IS) literature in order to construct and validate the ISP Conceptual Model. To our knowledge, this is the first time that a research approach has been used to implement and evaluate Information Security Policy (ISP) process, practice and technology values at the organizational level. The goal of this study is to demonstrate the benefits that will accrue to an organization that implements an effective ISP. Determining how users perceive of ISP Service Quality, System Quality and Information Quality will lead to increased productivity and Organizational Performance Benefits.

This study is intended to confirm the assumption that ISP Deployment Drivers and Usage Drivers have a positive impact on Organizational Performance Benefits and lead to a direct return on ISP investment.

If survey results indicate that such ISP values as Perceived Consequences, Perceived Ease of Use, Perceived Usefulness and User Satisfaction are high, organizational performance should be as well. Conversely, low ISP values will indicate low expectations of organizational performance. The survey is designed to show that the ISP Conceptual Model is a valuable and positive model.
If the survey reveals high ISP values in combination with low organizational performance or low ISP values in combination with high organizational performance the study will have failed to demonstrate the anticipated value of the ISP Conceptual Model. Further research will be required in order to explain these counterintuitive results.
Chapter 8: Results of Testing the ISP Conceptual Model

8.1. Introduction

In the age of information it is impossible for an organization to succeed if it does not have some form of Information Security Policy (ISP). One of the goals of this dissertation is to identify the factors that must be considered in order to develop and implement an ISP that is valuable, useful and beneficial.

In the present study, our objective is to develop and test a conceptual model of an Information Security Policy (ISP) and to measure the benefits that accrue to organizations as a result of the implementation and deployment of such a policy. If the ISP Conceptual Model performs as expected, the study may be considered successful. The present chapter will discuss the validity of the model to determine whether or not we have met our research goals.

8.2. Data Collection and Demographics

In order to validate the proposed ISP model, a research survey instrument was created and delivered to potential participants in late 2011 by way of email or personal delivery (see Appendix E). Statistical data analysis followed receipt of the survey documents (see Chapter 7).
A total of 303 surveys were sent out\textsuperscript{12}. In January, 2012, 133 surveys were returned; 40 of these had missing data; after revising the flawed documents with known participants, a total of 120 sets of data were completed and deemed usable. Figures 32, 33 and 34 indicate participants’ gender, age and job function. We did not discern any meaningful correlation between gender, age and ISP quality scores. Job function, on the other hand, correlated with higher ISP quality scores. 101 out of 120 (84\%) participants were information users; 92 (77\%) were male; 10 out of 120 (8\%) worked in IT as programmers, security workers or decision makers; all participants were private sector employees.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{gender.png}
\caption{Participants’ Gender}
\end{figure}

\textsuperscript{12} The participants were selected from one North American company.
8.3. Hypothesized ISP Model Assessment

The proposed CFA structural ISP Conceptual Model (see figure 31 on page 99) hypothesizes 30 observed variables and 8 latent variables. Table 7 (see pages 100-101) aligns the 30 observed variables with the constructs identified in
the survey questions. Confirmatory factor analysis, using AMOS software (V20), was employed to analyze and validate the ISP conceptual model. See chapter 7 for a detailed discussion of data analysis.

8.3.1. Handling Missing Data and Sample Size

“How many observations does a good SEM model require?” Many potential users shy away from SEM because they believe that large sample sizes are required (Iacobucci, 2010). While it is generally true that “bigger is always better” when it comes to sample size, smaller samples will suffice if the variables are reliable, the effects are strong and the model is not overly complex (Bearden, Sharma and Teel, 1982; Bollen, 1990).

A total of 17 surveys were incomplete. AMOS uses the Modification Index (MI) in order to achieve a good fit in confirmatory factor analysis (CFA) (Byrne, 2001). Unfortunately, MI cannot be used if the data set is incomplete. The SPSS function Expectation-Maximization (EM) can be used to replace incomplete data (Enders, 2003; Shah, 2005) but, in the current study, 120 complete data sets were deemed sufficient for SEM analysis; we were able, therefore, to dispense with the 17 incomplete sets without having to resort to the EM method.
8.3.2. Validation Methods

Chapter 7 described our test method and criteria; Table 6 presented goodness-of-fit cutoff criteria. However, given that the main purpose of this study is to analyze security breaches in order to prove the research hypotheses we will present only the most basic concepts of model goodness-of-fit.

8.3.2.1. First Level Model Validation

It is rare that a model fits well during the initial stages of development; modification is usually required (Hoyle, 1995; Hu et al., 1992; Hox et al., 1998; Hu and Bentler, 1999; Whittaker, 2012). I began by analyzing the proposed model using AMOS tool; covariances were subsequently added (see Figure 35).

When I used AMOS to validate the proposed model, the following error message appeared: “The following covariance matrix is not positive definite.” Table 8 presents the negative covariance matrix. The error message pointed out that Perceived Consequences, Perceived Ease of Use, Perceived Usefulness and User Satisfaction were not properly defined. As indicated in Figure 35, d4 represents Perceived Consequences, d5 represents Perceived Ease of Use, d6 represents Perceived Usefulness, and d7 represents User Satisfaction.
The question, therefore, is: why is the above matrix not positive definite, and what can be done about this? Put another way, why does the matrix contain zero or negative eigenvalues? While it is possible to sidestep the issue, doing so
could prove extremely costly. In order to find a solution to this problem, a number of possibilities were considered (Jöreskog and Yang, 1996).

**Error Reading the Data**

It is necessary to ensure that the program has read your data correctly because an empty covariance matrix (with no variables in it) is always not positive definite. I tried to read the data using MINITAB, which would allow me to validate the covariance matrix estimated by the SEM program. I did not find any error in the data.

**Typo Error**

Whenever a covariance matrix is created, there is always a chance of typos. I double-checked for typos.

**Starting Values**

---

13 There are many ways to sidestep this problem without actually trying to discern its cause. Besides simply compelling the program to proceed with analysis, researchers can make a ridge adjustment to the covariance or correlation matrix. This involves adding some quantity to the diagonal elements of the matrix. This addition has the effect of attenuating the estimated relations between variables. A large enough addition is sure to result in a positive definite matrix. The price of this adjustment, however, is bias in the parameter estimates, standard errors, and fit indices.
The model-implied Sigma matrix is computed from the model's parameter estimates. Before iterations begin, these estimates may be such that Sigma is not positive definite. If this is the case, it is necessary to make sure that the model has been specified correctly and contains no syntax errors. If the proposed model is "unusual," then the starting value routines incorporated into most SEM programs may fail. It is then up to the researcher to supply likely starting values.

**Sampling Variation**

When sample size is small, a sample covariance or correlation matrix may not be positive definite merely due to sampling fluctuation. In our case, the sample size satisfied the minimum requirements.

**Missing Data**

Large amounts of missing data can lead to a covariance or correlation matrix that may not be positive definite. In simple replacement schemes, the replacement value may be at fault. With pairwise deletion, a problem may arise because each element of the covariance matrix is computed from a different subset of cases (Arbuckle, 1996). In this study, the missing data had been already deleted.
Variable as a Constant?

Sometimes, due to a data reading error or deletion of cases, a variable may only have a single value. In other words, one of the variables is actually a constant. This variable will then have zero variance, and the covariance matrix will not be positive definite. Simple tabulation of the data should prevent this. If this problem persists, the researcher must either choose a different missing-data strategy or delete the variable. We did not encounter this problem in our study.

No Error Variance

A zero here implies no measurement error. While it may seem unlikely that any latent variable could be measured without error, this may occur if the construct has only a single measure. Single measures often lead to identification problems, and analysts may leave the default parameter fixed at zero. This did not occur in our study.

Negative Error Variance

Negative values on the diagonal are another matter. Since the diagonal elements of these matrices are variance terms, negative values are unacceptable. Further, since these error variances represent the "left-over" part of some variable,
a negative error variance suggests that the regression has somehow explained more than 100 percent of the variance. This was not the case in our study.

**Linear Dependency**

An input covariance matrix that is not positive definite may signal a perfect linear dependency of one variable on another. For example, if a plant researcher had data on corn (maize) stalks, and two of the variables in the covariance matrix were "plant height" and "plant weight," the linear correlation between the two would be nearly perfect, and the covariance matrix would not be positive definite within sampling error. It may be easier to detect such relationships by sight in a correlation matrix rather than a covariance matrix, but often these relationships are logically obvious. Multivariate dependencies, where several variables perfectly predict another variable, may not be visually obvious. In these instances, I used sequential analysis of the covariance matrix, i.e., adding one variable at a time and computing the determinant, to isolate the problem.

Dealing with this kind of problem involves changing the set of variables included in the covariance matrix. If two variables are perfectly correlated with each other, then one may be deleted. Alternatively, principal components may be used to replace a set of collinear variables with one or more orthogonal components.
With regard to the asymptotic weight matrix, linear dependency does not exist between variables, but between elements of the moments (the means and variances and covariances or the correlations) that are being analyzed. This can occur in connection with modeling “multiplicative interaction relationships” between latent variables. Jöreskog and Yang show how moments of the interaction construct are linear functions of moments of the "main effect" constructs. Their work explores alternative approaches for estimating these models (Jöreskog and Yang, 1996).

After exhaustive reviews and repeated use of Jöreskog and Yang’s alternative approaches method, we determined that Perceived Consequences, Perceived Ease of Use, Perceived Usefulness and User Satisfaction should be combined in the same construct. The new latent variable “User’s Perspective” (see Figure 36) was created to measure these four variables. Table 9 shows the results of model validation. Table 10 demonstrates that the “User’s Perspective” model meets the goodness-of-fit test.
Figure 36: User’s Perspective Model

Table 9: User’s Perspective Testing Result

<table>
<thead>
<tr>
<th>Computation of degrees of freedom (Default model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of distinct sample moments:</td>
</tr>
<tr>
<td>44</td>
</tr>
<tr>
<td>Number of distinct parameters to be estimated:</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>Degrees of freedom (44 - 24):</td>
</tr>
<tr>
<td>20</td>
</tr>
</tbody>
</table>

**Result (Default model)**

- Minimum was achieved
- Chi-square = 32.981
- Degrees of freedom = 20
- Probability level = .034
Next, the ISP Conceptual Model must be updated to incorporate the new User’s Perspective construct. Figure 37 represents the second generation ISP Conceptual Model, which will be analyzed in the following section. Note that Service Quality, System Quality, Product Quality and User’s Perspective have a direct impact on Organization Performance Benefit.

Table 10: Goodness-of-fit of User’s Perspective Construct

<table>
<thead>
<tr>
<th>Goodness-of-fit test</th>
<th>Recommendation</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-square ($\chi^2$)</td>
<td>$\chi^2/df &lt; 3$</td>
<td>32.981/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$=1.649$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$p=0.34$</td>
</tr>
<tr>
<td>Comparative Fit Index (CFI)</td>
<td>$&gt; 0.9$</td>
<td>0.954</td>
</tr>
<tr>
<td>Tucker-Lewis Index (TLI)</td>
<td>$&gt; 0.9$</td>
<td>0.936</td>
</tr>
<tr>
<td>Root Mean Square Error of Approximation (RMSEA)</td>
<td>$\leq 0.06$</td>
<td>0.058</td>
</tr>
</tbody>
</table>
8.3.2.2. Second Level Model Validation

In order to evaluate the second generation hypothesized ISP Model we need to add factor covariances\textsuperscript{14} before performing the same test. Table 11 summarizes the goodness-of-fit statistics associated with fully constrained multiple models. As this table indicates, the $\chi^2$/df (ratio of the statistic to its

\textsuperscript{14}In probability theory and statistics, covariance is a measure of how much two random variables change together.
degree of freedom) value of 2.076 and the Standardized Root Mean Square Error of Approximation (RMSEA) value of 0.054 both satisfy goodness-of-fit recommendation levels.

Figure 38: Second Generation ISP Conceptual Model with Covariances
When the ISP Conceptual Model was tested using the Comparative Fit Index (CFI) and the Tucker-Lewis Index (TLI), the values generated did not satisfy the recommendation levels established by the SEM goodness-of-fit test (Schreiber et al., 2006). A first generation regression model (Pearson Product-Moment Correlation Coefficient) was used to validate the model and associated hypotheses.

8.4. Testing the ISP Conceptual Model

In order to test the second generation ISP model to validate our research hypotheses, we performed empirical testing. Our goal was to prove that organizations with effective Information Security Policies (ISPs) enjoy an Organization Performance Benefit. Two types of companies were selected: business-to-business (B2B) and business-to-customer (B2C).
8.4.1. Data Collection

Test data for the second generation ISP Conceptual Model was derived from the 2011 security breach report described above. Of the 397 companies that had experienced a security breach, 72 reported an actual dollar loss, theft or other negative consequence. We sent 83 emails to this group of 72 companies but received only 5 replies. Representatives of three companies completed the survey but, citing security policy, indicated that they could not forward employee email addresses or ask their employees to complete the survey. Two companies indicated that their security policies did not allow them to participate in research of any sort, that their employees’ email addresses are considered personal information, and asked me “Not to email or contact them again.”

In order to test the third generation ISP model, the snowball method was used. Using Facebook and LinkedIn, I contacted 15 companies and collected 115 surveys. Six of these companies were identified in the 2011 security breach report described above; nine were not. 4 of the 15 companies are business-to-business; 11 are companies are business-to-customer (see Table 12).
8.4.2. Data Analysis

In order to test the ISP Conceptual Model we used the r- Pearson Product-Moment Correlation Coefficient, $R^2$ (R squared), Simple Linear Regression and a Trend line.

8.4.2.1. $r$- Pearson Product-Moment Correlation Coefficient

The Pearson Product-Moment Correlation Coefficient ($r$), or correlation coefficient for short, is a measure of the degree of linear relationship between two variables, usually X and Y. In regression, the emphasis is on predicting one variable from the other; in correlation, the emphasis is on the degree to which a linear model may describe the relationship between two variables. In regression, the interest is directional: one variable is predicted and the other is the predictor. In correlation, the interest is non-directional; the relationship is the critical aspect.
The correlation coefficient may take on any value between plus and minus one.

\[-1.00 \leq r \leq +1.00\]

The sign of the correlation coefficient (+, -) defines the direction of the relationship; this is either positive or negative. A positive correlation coefficient means that, as the value of one variable increases, the value of the other variable increases; as one decreases, the other decreases. A negative correlation coefficient indicates that as one variable increases, the other decreases, and vice-versa. Please note that correlation does not imply causation (Stockburger, 1996).

The absolute value of the correlation coefficient indicates the strength of the relationship. A correlation coefficient of \( r = 0.50 \) indicates a stronger degree of linear relationship than one in which \( r = 0.40 \). A correlation coefficient of zero (\( r = 0.0 \)) indicates the absence of a linear relationship and correlation coefficients of \( r = +1.0 \) and \( r = -1.0 \) indicate a perfect linear relationship (Stockburger, 1996).

**8.4.2.2. R Squared \( (R^2) \)**

The squared correlation coefficient \( (R^2) \) is the proportion of variance in \( Y \) that can be accounted for by knowing \( X \). Conversely, the proportion of variance in \( X \) can be accounted for by knowing \( Y \).
The squared correlation coefficient is also known as the coefficient of
determination. It is one of the best means available for evaluating the strength of a
relationship. For example, we know that the correlation between height and weight is
approximately \( r = 0.70 \). If we square this number to find the coefficient of determination, \( r^2 = 0.49 \). Thus, 49 percent of one's weight can be directly accounted for by one's
height and vice versa (Stockburger, 1996).

8.4.2.3. Linear Regression

In statistics, linear regression is an approach used to model the relationship
between a scalar variable \( y \) and one or more explanatory variables denoted by \( X \). One
explanatory variable is called simple regression. More than one explanatory variable is
multiple regression (Pedhazur, 1982). Linear regression was the first type of regression
analysis to be subjected to rigorous testing and is used extensively in practical
applications. This is because models that depend linearly on their unknown parameters
are easier to fit than models that depend non-linearly on their parameters and because the
statistical properties of the resulting estimates are easier to determine (Pedhazur, 1982).

Most of the time, linear regression refers to a model in which the conditional
mean of \( y \) given the value of \( X \) is an affine function of \( X \). Less commonly, linear
regression may refer to a model in which the median is expressed as a linear function of
\( X \). Like all forms of regression analysis, linear regression focuses on the conditional
probability distribution of $y$ given $X$, rather than on the joint probability distribution of $y$ and $X$, which is the domain of multivariate analysis (Pedhazur, 1982).

Linear regression has many practical uses. The most basic case of a single scalar predictor variable $x$ and a single scalar response variable $y$ is known as “simple linear regression.” The extension to multiple and/or vector-valued predictor variables (denoted with a capital $X$) is known as “multiple linear regression.” Nearly all real-world regression models involve multiple predictors, and basic descriptions of linear regression are often phrased in terms of the multiple regression model (Pedhazur, 1982).

Most applications of linear regressions are devoted to prediction or forecasting. Linear regression can be used to fit a predictive model to an observed set of data $y$ and $X$ values. After developing such a model, if an additional value of $X$ is given without its accompanying value of $y$, the model can be used to make a prediction of the value of $y$.

Given a variable $y$ and a number of variables $X_1...X_j$ that may be related to $y$, linear regression analysis can be applied to quantify the strength of the relationship between $y$ and $X_j$, to assess whether $X_j$ has a relationship with $y$, and to identify which subsets of $X_j$ contain redundant information about $y$. 
8.4.2.4. A Trend Line

A trend line represents the long-term movement in time series data after other components have been accounted for. A trend line indicates whether a particular data set (say GDP, oil prices or stock prices) has increased or decreased over a given period of time. A trend line may simply be drawn by hand through a set of data points. More often, position and slope are calculated using statistical techniques like linear regression. Trend lines are typically straight lines, although some variations use higher degree polynomials depending on the degree of curvature desired (Pedhazur, 1982; Kaw et al., 2008).

Trend lines are sometimes often used in business analytics to show changes in data over time. These are often quite simple. Trend lines are also used to argue that a particular action or event (such as training, or an advertising campaign) may cause observable changes at a certain point in time. This is a simple technique and does not require a control group, experimental design, or sophisticated analysis. However, such results may lack scientific validity in cases in which other potential changes can affect the data (Pedhazur, 1982; Kaw et al., 2008).

8.4.3. Analyzing the 2011 Security Breach Report
Our first path in analyzing the 2011 security breach report involved dividing the breaches into two categories; those caused by hackers and those caused by employees. Our second path was to categorize the type of company involved, i.e., business to business (B2B) or business to customer (B2C). Table 13 lists the firms that reported security breaches in 2011 and indicates the type of breach and type of firm. As the table indicates, 9% were B2B companies and 91% were B2C companies; in 295 out of 397 cases (74%) the security breaches were caused by employees.

Table 14 lists the 72 companies that experienced security breaches in 2011 and reported dollar loss, theft or some other negative impact. As the table indicates, 17 out of 72 (24%) were B2B companies; 55 out of 72 (76%) were B2C companies. Overall, 44 of the 72 (61%) reported breaches were caused by employees; among B2B companies, only 4 of the 17 (22%) breaches were caused by employees. These findings strongly suggest that B2B firms have better security policies than B2C firms.
<table>
<thead>
<tr>
<th>Type</th>
<th>TOT#</th>
<th>Example of some of the Company names in the Report</th>
<th>% of firms of 397</th>
<th>Number of Security Breaches contributed by Employees</th>
<th>% of Security Breaches caused by Hackers</th>
<th>% Security Breaches caused by Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Reported</td>
<td>397</td>
<td>Example of some of the Company names in the Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Significant Cost/Record of impact</td>
<td>72</td>
<td>Example of some of the Company names in the Report</td>
<td>18%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Reported</td>
<td>397</td>
<td>Example of some of the Company names in the Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizations /Gov. Agents (B2B)</td>
<td>36</td>
<td>BP Oil, Toshiba, SONY, Lockheed Martin</td>
<td>9%</td>
<td>102</td>
<td>295</td>
<td>26%</td>
</tr>
<tr>
<td>Restaurants (B2C)</td>
<td>28</td>
<td>TGI Friday, Taco Bell</td>
<td>6%</td>
<td>29</td>
<td>20</td>
<td>13%</td>
</tr>
<tr>
<td>Health/Insurance (B2C)</td>
<td>176</td>
<td>Blue Cross, Hartford Ins.</td>
<td>44%</td>
<td>17</td>
<td>159</td>
<td>10%</td>
</tr>
<tr>
<td>Bank/Finance Institute (B2C)</td>
<td>38</td>
<td>Book exchange, Campus Apt.</td>
<td>10%</td>
<td>7</td>
<td>32</td>
<td>18%</td>
</tr>
<tr>
<td>Others</td>
<td>128</td>
<td>computer service, airline, stores</td>
<td>31%</td>
<td>46</td>
<td>77</td>
<td>37%</td>
</tr>
<tr>
<td>Total B2C</td>
<td>361</td>
<td>91%</td>
<td>73</td>
<td>238</td>
<td>20%</td>
<td>80%</td>
</tr>
</tbody>
</table>

Table 13: Summary of 2011 Security Breach Report

<table>
<thead>
<tr>
<th>Type</th>
<th>TOT#</th>
<th>Example of some of the Company names in the Report</th>
<th>% of firms of 397</th>
<th>No. of Security Breaches caused by Emps.</th>
<th>% of Security Breaches caused by Hackers</th>
<th>% Security Breaches caused by Emps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Reported</td>
<td>397</td>
<td>Example of some of the Company names in the Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Significant Cost/Record</td>
<td>72</td>
<td>BP Oil, Toshiba, SONY, Lockheed Martin</td>
<td>24%</td>
<td>13</td>
<td>4</td>
<td>22%</td>
</tr>
<tr>
<td>Bank/Finance/credit card (B2C)</td>
<td>10</td>
<td>Chase bank, Morgan Stanley, Shell, Chevron</td>
<td>26%</td>
<td>4</td>
<td>15</td>
<td>79%</td>
</tr>
<tr>
<td>Restaurants (B2C)</td>
<td>12</td>
<td>TGI Friday, Taco Bell</td>
<td>17%</td>
<td>3</td>
<td>9</td>
<td>75%</td>
</tr>
<tr>
<td>Health/Insurance (B2C)</td>
<td>9</td>
<td>Blue Cross, Hartford Ins.</td>
<td>13%</td>
<td>2</td>
<td>7</td>
<td>78%</td>
</tr>
<tr>
<td>University (B2C)</td>
<td>4</td>
<td>Book exchange, Campus Apt.</td>
<td>6%</td>
<td>2</td>
<td>2</td>
<td>50%</td>
</tr>
<tr>
<td>Computer Security (B2C)</td>
<td>6</td>
<td>Bethesda Softworks</td>
<td>8%</td>
<td>3</td>
<td>3</td>
<td>50%</td>
</tr>
<tr>
<td>Entertainment /Publishing (B2C)</td>
<td>3</td>
<td>Broadcast, publishing</td>
<td>4%</td>
<td>1</td>
<td>2</td>
<td>67%</td>
</tr>
<tr>
<td>Airline (B2C)</td>
<td>2</td>
<td>Airport, AA airline</td>
<td>3%</td>
<td>0</td>
<td>2</td>
<td>100%</td>
</tr>
<tr>
<td>Total B2C</td>
<td>55</td>
<td>76%</td>
<td>15</td>
<td>40</td>
<td>55%</td>
<td></td>
</tr>
</tbody>
</table>

Table 14: Summary of Significant Security Breach Firms

137
8.4.4. Comparison of Firms With and Without Security Breaches

Of the 15 companies that we contacted to test the third generation ISP model using the snowball method, 4 were B2B and 2 were included in the list of companies that had experienced security breaches in 2011. 11 of these were B2C companies, 4 of whom were on the list. 55 surveys were collected from B2B companies; 18 were on the security breach list (see Table 12). These results indicate that there was no significant difference in ISP effectiveness or Organization Performance Benefit between those B2B companies that had experienced security breaches and those that had not.

A total of 60 surveys were collected from B2C companies; 11 surveys were collected from 4 firms on the security breach list; 49 surveys were collected from 7 firms that were not on the list (see Table 12). The results indicate that there was no significant difference in ISP Quality, User Perspective or Organizational Performance between those B2C firms that had experienced security breaches and those that had not (see Table 15).

<table>
<thead>
<tr>
<th>ISP Constructs</th>
<th>RPT vs. Not RPT Firms</th>
<th>RPT Firms User’s Perspective</th>
<th>NOT RPT Firms User’s Perspective</th>
<th>RPT Firms Organizational Performance Benefit</th>
<th>NOT RPT Firms Organizational Performance Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Quality</td>
<td>RPT MEAN  4.63</td>
<td>4.03</td>
<td>0.59</td>
<td>0.33</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>Not RPT MEAN</td>
<td>4.03</td>
<td>0.58</td>
<td>0.33</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td>correlation coefficient</td>
<td>r</td>
<td>0.38</td>
<td>0.33</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td>R Squared</td>
<td></td>
<td>0.38</td>
<td>0.33</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.62</td>
<td>0.39</td>
<td>0.41</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.41</td>
<td>0.18</td>
</tr>
<tr>
<td>System Quality</td>
<td>RPT MEAN  4.14</td>
<td>3.79</td>
<td>0.83</td>
<td>0.69</td>
<td>0.76</td>
</tr>
<tr>
<td></td>
<td>Not RPT MEAN</td>
<td>3.79</td>
<td>0.83</td>
<td>0.69</td>
<td>0.76</td>
</tr>
<tr>
<td></td>
<td>correlation coefficient</td>
<td>r</td>
<td>0.69</td>
<td>0.76</td>
<td>0.58</td>
</tr>
<tr>
<td></td>
<td>R Squared</td>
<td></td>
<td>0.86</td>
<td>0.73</td>
<td>0.81</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.81</td>
<td>0.63</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.63</td>
<td>0.40</td>
<td>0.63</td>
</tr>
<tr>
<td>Product Quality</td>
<td>RPT MEAN  4.20</td>
<td>3.85</td>
<td>0.74</td>
<td>0.55</td>
<td>0.70</td>
</tr>
<tr>
<td></td>
<td>Not RPT MEAN</td>
<td>3.85</td>
<td>0.74</td>
<td>0.55</td>
<td>0.70</td>
</tr>
<tr>
<td></td>
<td>correlation coefficient</td>
<td>r</td>
<td>0.55</td>
<td>0.70</td>
<td>0.50</td>
</tr>
<tr>
<td></td>
<td>R Squared</td>
<td></td>
<td>0.74</td>
<td>0.70</td>
<td>0.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.74</td>
<td>0.70</td>
<td>0.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.55</td>
<td>0.70</td>
<td>0.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.63</td>
<td>0.40</td>
<td>0.63</td>
</tr>
<tr>
<td>User’s Perspective</td>
<td>RPT MEAN  4.71</td>
<td>4.15</td>
<td>0.93</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td>Not RPT MEAN</td>
<td>4.15</td>
<td>0.93</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td>correlation coefficient</td>
<td>r</td>
<td>0.93</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td>R Squared</td>
<td></td>
<td>0.93</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.93</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.86</td>
<td>0.86</td>
</tr>
<tr>
<td>Organizational Performance Benefits</td>
<td>RPT MEAN  4.66</td>
<td>4.44</td>
<td>0.93</td>
<td>0.86</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td>Not RPT MEAN</td>
<td>4.44</td>
<td>0.93</td>
<td>0.86</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td>correlation coefficient</td>
<td>r</td>
<td>0.93</td>
<td>0.86</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td>R Squared</td>
<td></td>
<td>0.93</td>
<td>0.86</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.93</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.88</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.88</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.88</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.88</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.88</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.86</td>
<td>0.88</td>
<td>0.88</td>
</tr>
</tbody>
</table>

Table 15: Reported and Not Reported Security Breach Comparison
8.4.5. Comparison of B2B and B2C Firms

A comparison of B2B and B2C survey results, indicate that B2B employees award high scores to both their ISPs and Organizational Performance while B2C employees awarded lower scores to both. These results are summarized in table 23, which includes a mean, r-coefficient correlation, R squared between Service Quality, System Quality, and Product Quality with User’s Perspective and Organizational Performance Benefits.

Table 16: B2B and B2C Security Breach Comparison

As Table 16 indicates, there is a significant difference in the ISP Quality and Organizational Performance between B2B and B2C companies. In general, B2B companies have better ISPs, and higher User Perspectives and Organizational Performance Benefits. B2C companies, meanwhile, have room to improve. Figures 39a and Figure 39b show the r and R squared ($R^2$) value of B2B companies.
During the survey collection process, B2C participants discussed the impracticality of imposing a rigorous ISP. B2C employees require instant access to personal customer information; easy access entails a greatly increased risk of security
breaches. The survey results indicated that, among B2C companies, Service Quality has a negative association with User Perspectives and Organizational Performance Benefits (see Figures 40a, 40b and Table 15). Figures 40a and 40b indicate that better customer service impairs security, yet B2C firms cannot function without easy access to sensitive personal data. Amongst B2B companies this sort of information is limited to key personal who do not share it with general employees. For B2B companies, therefore, service quality has a positive association with User Perspectives and Organizational Performance Benefits (see Figure 39a, 39b and Table 14).

Figure 40a: B2C ISP Qualities / User’s Perspective ($r$, $R^2$)
Figures 41a and Figure 41b show r and R squared ($R^2$) values for User Perspectives and Organizational Performance Benefits of B2B and B2C companies. These figures show that User Perspectives have a positive impact on Organizational Performance Benefits for both B2B and B2C companies but are more significant for the former.

Figure 41a: B2C User’s Perspective / Organizational Performance (r, $R^2$)
8.5. Conclusion of ISP Model Testing

The survey results allowed me to confirm that if the company has a high quality ISP and high User Satisfaction, it will also have high Organizational Performance from the employees’ point of view. Figures 42a and 42b compare the B2B and B2C survey results, indicating that B2B companies score higher than B2C companies in terms of Service Quality, System Quality, and Product Quality correlated with User Satisfaction and Organizational Performance.
Figure 42a: B2B/B2C ISP Quality and User’s Perspective

Figure 42b: B2B/B2C ISP Quality and Organizational Performance
Of the 4 B2B companies that we surveyed, two had reported security breaches and two had not. Two companies are US government contractors; one of these had reported a security breach yet employees of both companies expressed satisfaction with their security policies and had survey scores in the same range. Most employees indicated that they are not allowed to log on to the internet outside the corporate firewall when they are at work. They cannot log on to the corporate internet outside the workplace; they cannot bring computers, cell phones, cameras, iPads, books or papers into or out of the workplace. There is zero tolerance of security violations perhaps because these types of facilities are frequently targeted by hackers looking to obtain classified government documents.

Figures 43a and 43b demonstrate that, when B2B and B2C survey results are combined, Service Quality, System Quality and Product Quality have a positive impact on User Perspectives and Organizational Performance Benefits. Figures 40a and 40b demonstrate that, among B2C companies, System Quality and Product Quality have positive impacts, while Service Quality has a negative impact on User Perspectives and Organizational Performance Benefits. B2B company employees, by contrast, have a favorable opinion of Service Quality; this has a positive impact on User Perspectives and Organizational Performance Benefits.
Figure 43a: Overall B2B and B2C ISP qualities / User’s Perspective (r, $R^2$)

Figure 43b: Overall B2B and B2C ISP qualities / Organizational Performance (r, $R^2$)
Chapter 9: Discussion and Implications

The ISP Conceptual Model that I have analyzed in this dissertation is unique in combining the Delone and McLean IS Success Model (1994, 2003) with the Technology Acceptance Model (TAM) (1989). This conceptual model enables researchers to study employee behavior and intention to use Information Security Policies (ISPs) and to evaluate the benefits that accrue from deployment of ISPs at the organizational level.

The study proves that Service Quality, System Quality and Product Quality are critical to overall ISP Quality and have a direct positive impact on Organizational Performance. The study also demonstrates that the relationship between Perceived Consequences, Perceived Ease of Use, Perceived Usefulness, and User Satisfaction are complementary rather than independent. The study thus satisfied our primary research goals, which were to:

1. Demonstrate that Information Security Policy (ISP) values have a positive impact on User Perspectives and Organizational Performance Benefits;

2. Determine the extent to which Perceived Consequences, Perceived Usefulness and Perceived Ease of Use affect the value of Information Security Policies and the extent to which these enhance Organizational Performance.
In their study of the Delone and McLean IS Success Model, Petter and colleagues argued that there was insufficient empirical evidence to evaluate the majority of relationships at the organizational level (Petter et al., 2008). The ISP Conceptual Model presented in this dissertation builds on prior models evaluating Information Technology (IT) investment, Information Quality, System Quality, Service Quality, User Perspectives and Organizational Performance Benefits. Our research makes an operational and a methodological contribution by employing Structural Equation Modeling (Chapter 8). Our research demonstrated that Service Quality, System Quality and Product Quality constitute the bridge between Deployment Drivers and Usage Drivers (Figures 18 and 20 in Chapter 3) and that the value of these qualities have a direct impact on Perceived Consequences, Perceived Ease of Use, Perceived Usefulness, and User Satisfaction, thereby generating Positive Organizational Benefit (Figure 28 in Chapter 5).

In Chapter 8 we demonstrated that the ISP Conceptual Model is a good predictor of ISP success as measured from the end User’s Perspective and in relation to Organizational Performance. This demonstrates the importance of ISP value to Organizational Performance.

Corporate security officers must determine how much security is required and how they can obtain optimal benefit from a limited IT budget. Our research demonstrates
that determining the value of ISP will assist security officers in evaluating just how much they need to invest in IT.

This study analyzed security breaches that occurred in 2011 at two different types of companies: Business-to-Business (B2B) and Business-to-Customer (B2C). Our findings indicated that the type of business had a direct impact on how employees perceived of the value of ISPs and that these perceptions would influence how much a firm would invest in Information Technology (IT), Information System (IS), or Information Security Policy (ISP) proper.

Empirical studies have indicated that Information Quality, Service Quality and System Quality have a positive impact on four constructs: Perceived Usefulness (PU) (Delone and McLean, 1992; Seddon, 1997), Perceived Ease of Use (PEOU) (Lin and Lu, 2000), Perceived Consequences and User Satisfaction (Davis, 1989). The results of our study indicate that these four constructs are statistically significant.

The four constructs used to measure Organizational Performance are: Compliance, Modernization, Adaptation and Revenue (see Table 16) (Goel and Chen, 2005; Buyter et al., 2001; Tallon et al., 2000; Arumugam et al., 2011). By assessing these aspects of ISP, an organization will be able to: provide better systems, services and products to users; enhance organizational competitiveness and strategic benefit; and, increase revenue by minimizing security breaches.

149
Chapter 10: Limitations and Future study

The participants used to help validate the ISP Conceptual Model were all employed by the same company. Future studies should involve participants from a wider variety of businesses and should, ideally, be international in scope. It is conceivable that a larger sample size will lead to more generalizable results. It is also conceivable that a different set of samples will result in a better fit of the second generation model. Unfortunately, as we discovered, many companies were unwilling to share information or allow employees to take part in surveys or academic research. This made it difficult to test the ISP Conceptual Model.

The security breaches report concluded that the majority of breaches that occurred at B2C companies were caused by employees, either intentionally or unintentionally. Future research should examine individual breaches in relations to the ISPs employed by the affected companies. Surveys should be combined with face-to-face interviews, which tend to generate more useful information but may be time consuming. Future studies of B2B companies should determine how much they spend on ISPs to prevent hacking and cybercrime.

We employed the snowball method in order to augment the number of survey participants. The snowball method was effective, given our sample size, and yielded
consistent results (Bailey, 1994; Bernard, 1999). Using this method may, however, have limited the ability to generalize our findings (Bernard, 1999).

In this study, we dispensed with incomplete data sets. In future studies, the Expectation Maximization (EM) algorithm may be used to replace missing data (Tomarken et al., 2005). The EM algorithm may, however, produce biased and inefficient estimates or inaccurate standard errors (Tomarken et al., 2005).

Future research should also seek to determine the actual costs associated with implementing IT and fixing security breaches. Cyber-attacks, such as the one that took place at Strategy Forecasts in Austin, Texas, in November 2011, result in losses of revenue and reputation, and customer loyalty.
References


Chang, J., Torkzadeh, G. & Dhillon, G. (2004). Re-examining the measurement models of Success for Internet Commerce. *Information and Management. 41*, 577-584


Gartner 2011. Retrieved from

http://www.interdynartis.com/SiteCollectionDocuments/Predicts2011_IT_Transparency.pdf)

Gartner 2011 Predicts. Retrieved from

http://www.gartner.com/technology/research/predicts/


Office of the Chief Information Officer, OCIO 2011. Retrieved at
http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Security/DEV01_003883

development, purification, and initial test. Computers in Human Behavior, 23(3), 1329-1346.

http://dictionary.oed.com/, retrieved 20 November 2010

Research, 13(2), 151-167.

Information. New York: John Wiley & Sons, Inc.

Human-Behavioural Implications. Published in the Proceedings of the 2nd International
Conference on Security of Information and Networks (SIN’09), October 6–10, 2009,

Pearson Custom Publishing & West Chester University, “Custom Program for Computer


model: An examination of IS success at the individual level. Information & Management,
46, 159–166

dimensions, measures, and interrelationships. European Journal of Information Systems,
17(3), 236-263.


Sciences in Colleges, 25(2), 100–106. ISSN 1937-4771

Business Review, 63(4), 149–160.


Stockburger, D. “*INTRODUCTORY STATISTICS: CONCEPTS, MODELS, AND APPLICATIONS.*” WWW Version 1.0 First Published 7/15/96, Revised 2/19/98


APPENDIX A: Unapproved and validated Information Security Policy Checklist

<table>
<thead>
<tr>
<th>Policy Checklist</th>
<th>Required</th>
<th>Published</th>
<th>Appraised</th>
<th>Accepted</th>
<th>Communicated</th>
<th>Training</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Management</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin/Special Access</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Training</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Licensing</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus Protection</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for networked environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for networked environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portable Computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for organizations supporting laptops, PDA, or other portable devices.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for networked environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Hardening</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for environments with servers.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for environments where software is developed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required for environments where access to or from entities external to organization is required. Outsourced maintenance, management, and network services must be considered.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## APPENDIX B: 2010 Survey Example

### A. Risk Assessment

#### Information Security Policy

<table>
<thead>
<tr>
<th></th>
<th>Is there an information security policy, which is approved by the management, published and communicated as appropriate to all employees?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Ans:**

1. Does not apply  
2. Under Review  
3. Reviewed /Initial planning is under way  
4. Only Partial implemented  
5. Minimum implemented and compliance  
6. Room to improve  
7. Fully implemented and compliance  
8. Satisfactory  
9. Production running well  
10. Best - No improvement is required

<table>
<thead>
<tr>
<th></th>
<th>The management is committed and set out the organizational approach to managing information security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Ans:**

1. Does not apply  
2. Under Review  
3. Reviewed /Initial planning is under way  
4. Only Partial implemented  
5. Minimum implemented and compliance  
6. Room to improve  
7. Fully implemented and compliance  
8. Satisfactory  
9. Production running well  
10. Best - No improvement is required

<table>
<thead>
<tr>
<th></th>
<th>Security policy has an owner who is responsible for its maintenance and review according to a defined review process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

**Ans:**

1. Does not apply  
2. Under Review  
3. Reviewed /Initial planning is under way  
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

| 4 | Information security process ensures that a review takes place in response to any changes affecting the basis of the original assessment, for example: significant security incidents, new vulnerabilities, or changes to organizational or technical structure. |

| 5 | There is a formal or informal agreement between the organizations for exchange of information and software. (This will save the software cost.) |

<p>| 6 | There are policies, procedures or controls in place to protect the exchange of information through the use of voice, facsimile and video communication facilities. |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does not apply</td>
<td>2</td>
<td>Under Review</td>
<td>3</td>
<td>Reviewed /Initial planning is under way</td>
<td>4</td>
<td>Only Partial implemented</td>
<td>5</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6</td>
<td>Room to improve</td>
<td>7</td>
<td>Fully implemented and compliance</td>
<td>8</td>
<td>Satisfactory</td>
<td>9</td>
<td>Production running well</td>
<td>10</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

**7**

Are responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined? - Allocation of information security responsibilities

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does not apply</td>
<td>2</td>
<td>Under Review</td>
<td>3</td>
<td>Reviewed /Initial planning is under way</td>
<td>4</td>
<td>Only Partial implemented</td>
<td>5</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6</td>
<td>Room to improve</td>
<td>7</td>
<td>Fully implemented and compliance</td>
<td>8</td>
<td>Satisfactory</td>
<td>9</td>
<td>Production running well</td>
<td>10</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

**8**

Are the appropriate contacts with law enforcement authorities, regulatory bodies, utility providers, information service providers and telecommunication operators maintained to ensure that appropriate action can be quickly taken and advice obtained in the event of an incident? - Co-operation between organizations

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does not apply</td>
<td>2</td>
<td>Under Review</td>
<td>3</td>
<td>Reviewed /Initial planning is under way</td>
<td>4</td>
<td>Only Partial implemented</td>
<td>5</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6</td>
<td>Room to improve</td>
<td>7</td>
<td>Fully implemented and compliance</td>
<td>8</td>
<td>Satisfactory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. Production running well
10. Best - No improvement is required

### 9
Is the implementation of security policy reviewed independently on regular basis? This is to provide assurance that organizational practices properly reflect the policy and that it is feasible and effective. - Independent review of information security.

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

### 10
Does the Security Policy identify operating procedures such as back-up, equipment maintenance, etc.

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

### Asset classification and control

11
Is there a maintained inventory or register of the important assets associated with each information system? - Inventory of assets

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

<table>
<thead>
<tr>
<th>12</th>
<th>Is there a Strategic Software Asset Management?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
<tr>
<td></td>
<td>10. Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13</th>
<th>Is there a strategy to reduce the license cost and lower the risk and cost of audits?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
<tr>
<td></td>
<td>10. Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14</th>
<th>Does a formal reporting procedure exist to report un-needed tools through appropriate management channels as quickly as possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
</tbody>
</table>

172
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

<table>
<thead>
<tr>
<th>15</th>
<th>Does a formal audit policy exist to audit the software in the user’s computer regularly?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2</td>
<td>Under Review</td>
</tr>
<tr>
<td>3</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9</td>
<td>Production running well</td>
</tr>
<tr>
<td>10</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16</th>
<th>Software usage will report periodically.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2</td>
<td>Under Review</td>
</tr>
<tr>
<td>3</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9</td>
<td>Production running well</td>
</tr>
<tr>
<td>10</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17</th>
<th>Illegal usage of software will report periodically.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2</td>
<td>Under Review</td>
</tr>
<tr>
<td>3</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7</td>
<td>Fully implemented and compliance</td>
</tr>
</tbody>
</table>
8. Satisfactory
9. Production running well
10. Best - No improvement is required

**Information classification**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Is there an information classification scheme or guideline in place which will assist in determining how the information is to be handled and protected?</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

**Personnel security**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Are security roles and responsibilities as placed in organization's information security policy documented where appropriate? Does this include general responsibilities for implementing or maintaining security policy as well as specific responsibilities for protection of particular assets, or for extension of particular security processes or activities? - Responsibilities</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>
Do employees sign confidentiality or non-disclosure agreements as a part of their initial terms and conditions of the employment and annually thereafter? - Confidentiality

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Do the terms and conditions of the employment cover the employee's responsibility for user training information security? Where appropriate, these responsibilities might continue for a defined period after the end of the employment.

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Security of third party access

Are risks from third party access identified and appropriate security controls implemented?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
<table>
<thead>
<tr>
<th>23</th>
<th>Are the types of accesses identified, classified and reasons for access justified?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>24</th>
<th>Are security risks with third-party contractors working onsite identified and appropriate controls implemented?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>25</th>
<th>Is there a formal contract containing or referring to all the security requirements to ensure compliance with the organization's security policies and standards?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
</tbody>
</table>
Outsourcing

Are security requirements addressed in the contract with the third party, when the organization has outsourced the management and control of all or some of its information systems, networks and/or desktop environments?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Does the contract address how the legal requirements are to be met, how the security of the organization's assets are maintained and tested, and the right of audit, physical security issues and how the availability of the services is to be maintained in the event of disaster?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

User Training
<table>
<thead>
<tr>
<th>28</th>
<th>Do all employees of the organization, the third party users (where relevant), and outsourcing employees (where relevant) receive appropriate information security training and regular updates in organizational policies and procedures?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does not apply</td>
<td></td>
</tr>
<tr>
<td>2. Under Review</td>
<td></td>
</tr>
<tr>
<td>3. Reviewed /Initial planning is under way</td>
<td></td>
</tr>
<tr>
<td>4. Only Partial implemented</td>
<td></td>
</tr>
<tr>
<td>5. Minimum implemented and compliance</td>
<td></td>
</tr>
<tr>
<td>6. Room to improve</td>
<td></td>
</tr>
<tr>
<td>7. Fully implemented and compliance</td>
<td></td>
</tr>
<tr>
<td>8. Satisfactory</td>
<td></td>
</tr>
<tr>
<td>9. Production running well</td>
<td></td>
</tr>
<tr>
<td>10. Best - No improvement is required</td>
<td></td>
</tr>
</tbody>
</table>

**Security/threat incidents**

<table>
<thead>
<tr>
<th>29</th>
<th>Does a formal reporting procedure exist to report security/threat incidents through appropriate management channels as quickly as possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does not apply</td>
<td></td>
</tr>
<tr>
<td>2. Under Review</td>
<td></td>
</tr>
<tr>
<td>3. Reviewed /Initial planning is under way</td>
<td></td>
</tr>
<tr>
<td>4. Only Partial implemented</td>
<td></td>
</tr>
<tr>
<td>5. Minimum implemented and compliance</td>
<td></td>
</tr>
<tr>
<td>6. Room to improve</td>
<td></td>
</tr>
<tr>
<td>7. Fully implemented and compliance</td>
<td></td>
</tr>
<tr>
<td>8. Satisfactory</td>
<td></td>
</tr>
<tr>
<td>9. Production running well</td>
<td></td>
</tr>
<tr>
<td>10. Best - No improvement is required</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>30</th>
<th>Does a formal reporting procedure or guideline exist for users to report security weakness in, or threats to, systems or services?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does not apply</td>
<td></td>
</tr>
<tr>
<td>2. Under Review</td>
<td></td>
</tr>
<tr>
<td>3. Reviewed /Initial planning is under way</td>
<td></td>
</tr>
<tr>
<td>4. Only Partial implemented</td>
<td></td>
</tr>
<tr>
<td>5. Minimum implemented and compliance</td>
<td></td>
</tr>
<tr>
<td>6. Room to improve</td>
<td></td>
</tr>
</tbody>
</table>
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

**Equipment(hardware) Security**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>31</strong></td>
<td>Are items requiring special protection isolated to reduce the general level of protection required?</td>
</tr>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>32</strong></td>
<td>Are controls adopted to minimize risk from potential threats such as theft, fire, explosives, smoke, water, dist, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, and flood?</td>
</tr>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>33</strong></td>
<td>Is the equipment protected from power failures by using redundant power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator, etc.?</td>
</tr>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
</tbody>
</table>
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

<table>
<thead>
<tr>
<th>34</th>
<th>Is maintenance carried out only by authorized personnel? (Including third party)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
<tr>
<td></td>
<td>10. Best - No improvement is required</td>
</tr>
</tbody>
</table>

**Insurance Policy**

<table>
<thead>
<tr>
<th>35</th>
<th>Is the equipment covered by insurance, and are the insurance requirements satisfied?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
<tr>
<td></td>
<td>10. Best - No improvement is required</td>
</tr>
</tbody>
</table>

**Offsite Equipment**

| 36 | Does any equipment usage outside an organization's premises for information processing have to be authorized by the management? |
1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Is the security provided for equipment while outside the premises equal to or more than the security provided inside the premises?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Disposal or re-use of equipment

Are storage devices containing sensitive information either physically destroyed or securely over written?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Security Management
<table>
<thead>
<tr>
<th>39</th>
<th>There is an incident management procedure to handle security/threat incidents.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
<tr>
<td></td>
<td>10. Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40</th>
<th>Does the security management procedure address the incident management responsibilities with an orderly and quick response to security/threat incidents?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
<tr>
<td></td>
<td>10. Best - No improvement is required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>41</th>
<th>Does the security management procedure address different types of incidents ranging from denial of service to breach of confidentiality etc.?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Does not apply</td>
</tr>
<tr>
<td></td>
<td>2. Under Review</td>
</tr>
<tr>
<td></td>
<td>3. Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td></td>
<td>4. Only Partial implemented</td>
</tr>
<tr>
<td></td>
<td>5. Minimum implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>6. Room to improve</td>
</tr>
<tr>
<td></td>
<td>7. Fully implemented and compliance</td>
</tr>
<tr>
<td></td>
<td>8. Satisfactory</td>
</tr>
<tr>
<td></td>
<td>9. Production running well</td>
</tr>
</tbody>
</table>
10. Best - No improvement is required

<table>
<thead>
<tr>
<th></th>
<th>Does the security management procedure address the way to handle different types of security incidents?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

43 The audit trails and logs relating to the incidents are maintained and proactive action taken in a way so that the incident doesn’t reoccur.

<table>
<thead>
<tr>
<th></th>
<th>The audit trails and logs relating to the incidents are maintained and proactive action taken in a way so that the incident doesn’t reoccur.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
<tr>
<td>8.</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>9.</td>
<td>Production running well</td>
</tr>
<tr>
<td>10.</td>
<td>Best - No improvement is required</td>
</tr>
</tbody>
</table>

44 When the Information processing facilities managed by an external company or contractor (third party), is there a policy of computer/information security for the third party?

<table>
<thead>
<tr>
<th></th>
<th>When the Information processing facilities managed by an external company or contractor (third party), is there a policy of computer/information security for the third party?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does not apply</td>
</tr>
<tr>
<td>2.</td>
<td>Under Review</td>
</tr>
<tr>
<td>3.</td>
<td>Reviewed /Initial planning is under way</td>
</tr>
<tr>
<td>4.</td>
<td>Only Partial implemented</td>
</tr>
<tr>
<td>5.</td>
<td>Minimum implemented and compliance</td>
</tr>
<tr>
<td>6.</td>
<td>Room to improve</td>
</tr>
<tr>
<td>7.</td>
<td>Fully implemented and compliance</td>
</tr>
</tbody>
</table>

183
8. Satisfactory
9. Production running well
10. Best - No improvement is required

<table>
<thead>
<tr>
<th>45</th>
<th>Are the risks associated with security management identified in advance and discussed with the third party with appropriate controls incorporated into the contract?</th>
</tr>
</thead>
</table>
1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

<table>
<thead>
<tr>
<th>46</th>
<th>Does any equipment usage outside an organization's premises for information processing have to be authorized by the management?</th>
</tr>
</thead>
</table>
1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

<table>
<thead>
<tr>
<th>47</th>
<th>Is the security provided for equipment while outside the premises equal to or more than the security provided inside the premises?</th>
</tr>
</thead>
</table>
1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

48  Is there a policy when storage devices are containing sensitive information either physically destroyed or securely overwritten?
1. Does not apply
2. Under Review
3. Reviewed/Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

49  Is the equipment covered by insurance, and are the insurance requirements satisfied?
1. Does not apply
2. Under Review
3. Reviewed/Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

Controls
50  Can equipment, information, or software be taken offsite without appropriate authorization?
1. Does not apply
2. Under Review
3. Reviewed/Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

51 Are spot checks or regular audits conducted to detect unauthorized removal of property?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

52 Are individuals notified and aware of these types of spot checks or regular audits?

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

**Access Controls**

53 The business requirements for access control have been defined and documented.

1. Does not apply
2. Under Review
3. Reviewed /Initial planning is under way
4. Only Partial implemented
5. Minimum implemented and compliance
6. Room to improve
7. Fully implemented and compliance
8. Satisfactory
9. Production running well
10. Best - No improvement is required

54 The Access control policy address the rules and rights for each user or a group of users.

55 Have the users and service providers been given a clear statement of the business requirement to be met by access controls?

56 Has a formal policy been adopted that takes into account the risks of working with computing facilities such as notebooks, palm pilots, etc., especially in unprotected environments?
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>Was training arranged for staff that use mobile computing facilities to raise their awareness on the additional risks resulting from this way of working and controls that need to be implemented to mitigate the risks?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>58</td>
<td>Are there any policies, procedures, and/or standards to control telecommuting activities? This should be consistent with organization's security policy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

188
<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
</tr>
</thead>
</table>
| Is suitable protection of telecommuting site in place against threats   | 1. Does not apply  
2. Under Review  
3. Reviewed /Initial planning is under way  
4. Only Partial implemented  
5. Minimum implemented and compliance  
6. Room to improve  
7. Fully implemented and compliance  
8. Satisfactory  
9. Production running well  
10. Best - No improvement is required |

<table>
<thead>
<tr>
<th>Are there any policies, procedures and/ or standards to control telecommuting activities?</th>
<th>Options</th>
</tr>
</thead>
</table>
| This should be consistent with organization's security policy?                              | 1. Does not apply  
2. Under Review  
3. Reviewed /Initial planning is under way  
4. Only Partial implemented  
5. Minimum implemented and compliance  
6. Room to improve  
7. Fully implemented and compliance  
8. Satisfactory  
9. Production running well  
10. Best - No improvement is required |
APPENDIX C: Cover Letter for eMail based Survey

Date:

Name:
Company:
Address:
City, State, Zip code:

Dear Name:

My name is Vick Chen and I am a Ph.D. Candidate in Information Science at State University New York Business School at Albany. I could certainly use your help in conducting a survey that I will be used to gather the data for my dissertation.

In my dissertation I hope to determine the factors that are critical to ensuring the success of information security policies. Using an a priori model from the domain of information system as an analog I have developed a comprehensive model that I believe will help determine whether an ISP will be successful. So with the IS success model, my model will also seek to understand success from the user’s perspective.

This attached survey is completely voluntary, confidential and only for research purpose there are no anticipated risks in your participation. However, your participation is extremely valued and appreciated.

The survey should take between 15 to 20 minutes to complete. If you have any questions or concerns about this research, please feel free to contact me at Email: vc5830@albany.edu or Vicki.chen@ps.ge.com.

Thank you for your attention.

Sincerely,

Vicki Chen
Business School of Information Science and Policy
University at Albany (SUNY)
135 Western Avenue
Albany, NY 12203
APPENDIX D: Cover Letter for Pilot users Survey

Date:

Dear Colleagues:

My name is Vick Chen and I am a Ph.D. Candidate in Information Science at State University New York Business School at Albany. I could certainly use your help in pilot testing a survey that will be used to gather the data for my dissertation.

In my dissertation I hope to determine the factors that are critical to ensuring the success of information security policies. Using an a priori model from the domain of information system as an analog, I have developed a comprehensive model that I believe will help determine whether an ISP will be successful. So with the IS success model, my model will also seek to understand success from the user’s perspective.

This survey is completely voluntary, confidential and only for research purpose there are no anticipated risks in your participation. It’s not related to the work, and your name is not required. However, your participation is extremely valued and appreciated.

The survey should take between 15 to 20 minutes to complete. If you have any questions or concerns about this research, please feel free to contact me at Email: vc5830@albany.edu or Vicki.chen@ps.ge.com.

Thank you for your attention.

Sincerely,

Vicki Chen
Business School of Information Science and Policy
University at Albany (SUNY)
135 Western Avenue
Albany, NY 12203
APPENDIX E: Survey Instrument

SECTION A. DEMOGRAPHIC INFORMATION

Company Name: (Option)_____________________________________

1. Gender a). Male  b). Female

2. Education – highest level attained
   a) Less than high School
   b) High School deployment or equivalent
   c) Associates’ degree
   d) Bachelors’ degree
   e) Masters’ degree
   f) Doctorate degree

3. Age (Circle one)
   a) Under 20
   b) 20-30
   c) 31-40
   d) 41-50
   e) 50-60
   f) 60+

4. Is your organization public or privately held?
   a) Public – Federal, State or Local Government
   b) Private sector

5. Which of the following best describes your job title? (check all that apply)
   a) Company CEO/Direct/Manager of Information Technology
   b) Direct/Manager of Information Security Technology
   c) Chief Information Officer(CIO) or Chief Technology Officer (CTO)
   d) Computer Consultant, Software Programmer, Hardware Engineer
   e) Security Officer
   f) Administrative / Policy Management
   g) Reviewer or decision maker for Information Security Management System
   h) IT Project Management
   i) IT Development
   j) Business/Operations management
   k) Business/Operations Support
   l) Information Users
   m) Other – specify: ___________________________________________

*** CONTINUE ON TO NEXT PAGE ***
6. Do your job duties include any of the following (check all that apply);
   a) Decisions Regarding Information Security
   b) Decisions regarding handling of employee policy violations
   c) Investigations of cybercrimes
   d) Decision regarding firm’s physical security
   e) Audit reporting concerning fraud or cybercrime
   f) None of the

7. Are you personally involved in any of the following at your organization?
   a) Decisions regarding information security
   b) Decisions regarding handling of employee policy violations
   c) Investigations of cybercrimes
   d) Decisions regarding firm’s physical security (e.g., grant access to restricted area)
   e) Audit reporting concerning fraud or cybercrime
   f) None of the above

8. Years of IT experience (e.g. system design, analysis, programmer)
   a) Entry level - less than 1 year
   b) 1-5 years
   c) 5-10 years
   d) More than 10 years
   e) None

*** CONTINUE ON TO NEXT SECTION ***
SECTION B. This section examines the Service Quality (questions 1-5), System Quality (questions 6-10), Information Quality (questions 11-16), User’s Perspective (questions 17-24) and Organizational Performance Benefits (questions 25-30) from your perspective in your company’s Information Security Policy which could include process, practice, procedure and technology.

<table>
<thead>
<tr>
<th>Number</th>
<th>Question</th>
<th>Description</th>
<th>Rating Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SRQ1 My company’s Information Security Policy provides a highly secure</td>
<td>Information environment.</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>information environment.</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td>2</td>
<td>SRQ2 My company’s Information Security Policy provides a reliable IT</td>
<td>Team including helpdesk.</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>policy provides a reliable IT Team including helpdesk.</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td>3</td>
<td>SRQ3 My company’s Information Security Policy rules and regulations takes</td>
<td>into account the interests and needs of the users.</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>account the interests and needs of the users.</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td>4</td>
<td>SRQ4 My company’s Information Security Policy regulates that IT helpdesk</td>
<td>responds to request in a timely manner.</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>responds to request in a timely manner.</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td>5</td>
<td>SRQ5 My company’s Information Security Policy provides up-to-date</td>
<td>equipment. (e.g., Hardware, Software)</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>equipment. (e.g., Hardware, Software)</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Question</th>
<th>Description</th>
<th>Rating Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>STQ1 My company’s Information Security Policy has adequate security</td>
<td>protection against internal unauthorized access and external hackers.</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>protection against internal unauthorized access and external hackers.</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td>7</td>
<td>STQ2 My company’s Information Security Policy regulated information</td>
<td>systems, making them simple to use by containing user-friendly features.</td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td>systems, making them simple to use by containing user-friendly features.</td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td>8</td>
<td>STQ3 My company’s Information Security Policy creates</td>
<td></td>
<td>Disagree very much, Disagree moderately, Disagree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>slightly, Agree slightly, Agree moderately, Agree</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>very much</td>
</tr>
<tr>
<td></td>
<td></td>
<td>excessive delays in information systems response time.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>STQ4</td>
<td>My company’s Information Security Policy ensures that the information systems are easy to maintain and to modify.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>STQ5</td>
<td>My company’s Information Security Policy ensures that the information systems are highly stable.</td>
<td></td>
</tr>
</tbody>
</table>

**Information Security Policy**

**Information PRODUCT QUALITY SURVEY**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>PDQ1</td>
<td>My company’s Information Security Policy is free of technical and information errors.</td>
</tr>
<tr>
<td>12</td>
<td>PDQ2</td>
<td>My company’s Information Security Policy does not include unnecessary information.</td>
</tr>
<tr>
<td>13</td>
<td>PDQ3</td>
<td>My company’s Information Security Policy allows appropriate access to all relevant data.</td>
</tr>
<tr>
<td>14</td>
<td>PDQ4</td>
<td>My company’s Information Security Policy is easy to read and comprehend.</td>
</tr>
<tr>
<td>15</td>
<td>PDQ5</td>
<td>My company’s Information Security Policy is current with information technology. (e.g., Warning for the latest hacker’s threats and current equipment.)</td>
</tr>
<tr>
<td>16</td>
<td>PDQ6</td>
<td>My company’s Information Security Policy comprehensively addresses all critical security issues within the company.</td>
</tr>
</tbody>
</table>

**USER’S PERSPECTIVE OF Information Security Policy SURVEY**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>PC1</td>
<td>I am confident that our company’s Information Security Policy will prevent security breaches from occurring.</td>
</tr>
<tr>
<td>18</td>
<td>PC2</td>
<td>Employees are rewarded for following company’s Information Security Policy. (you don’t cause the security breach for your company.)</td>
</tr>
<tr>
<td>19</td>
<td>PEOU1</td>
<td>My company’s Information Security Policy is easy to use.</td>
</tr>
<tr>
<td>20</td>
<td>PEOU2</td>
<td>The goals of my company’s Information Security Policy are clear.</td>
</tr>
<tr>
<td>21</td>
<td>PU1</td>
<td>My company’s Information Security Policy is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>22</td>
<td>PU2</td>
<td>My company’s Information Security Policy can increase my work effectiveness.</td>
</tr>
<tr>
<td>23</td>
<td>US1</td>
<td>I follow my company’s Information Security Policy on a regular basis.</td>
</tr>
<tr>
<td>24</td>
<td>US2</td>
<td>I strongly recommend others to use my company’s Information Security Policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ORGANIZATIONAL PERFORMANCE BENEFIT SURVEY</td>
</tr>
<tr>
<td>25</td>
<td>OPB1</td>
<td>My company’s Information Security helps in reducing the number of security breaches.</td>
</tr>
<tr>
<td>26</td>
<td>OPB2</td>
<td>My company’s Information Security Policy ensures that The company’s IT systems are up-to-date.</td>
</tr>
<tr>
<td>27</td>
<td>OPB3</td>
<td>My company’s Information Security Policy makes easy for workers to adapt to changes in regulations.</td>
</tr>
<tr>
<td>28</td>
<td>OPB4</td>
<td>My company’s Information Security Policy increases company’s productivity.</td>
</tr>
<tr>
<td>29</td>
<td>OPB5</td>
<td>My company’s Information Security Policy helps improve the company’s reputation.</td>
</tr>
<tr>
<td>30</td>
<td>OPB6</td>
<td>My company’s Information Security Policy leads to increased company’s revenue.</td>
</tr>
</tbody>
</table>