Examining Impacts of Organizational Capabilities in Information Security: A Structural Equation Modeling Analysis

By Jacqueline Huynh Hall

B.S. in Electrical Engineering. December 1990, Old Dominion University

MBA in Information Systems. May 1998, Old Dominion University

M.S. in Systems Engineering, January 2009, The George Washington University

A Dissertation submitted to

The Faculty of
The School of Engineering and Applied Science
of The George Washington University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

May 15, 2011

Dissertation directed by

Thomas A. Mazzuchi

Professor of Operations Research and of Engineering Management

Shahram Sarkani

Professor of Engineering Management and Systems Engineering

The School of Engineering and Applied Science of The George Washington University certifies that Jacqueline Huynh Hall has passed the Final Examination for the degree of Doctor of Philosophy as of 18 March 2011. This is the final and approved form of the dissertation.

"Examining Impacts of Organizational Capabilities in Information Security: A Structural Equation Modeling Analysis"

Jacqueline Huynh Hall

Dissertation Research Committee:

Michael Stankosky, Professor of Engineering Management and Systems Engineering, Dissertation Research Committee Chair

Thomas A. Mazzuchi, Professor of Operations Research and of Engineering Management, Dissertation Co-Director

Shahram Sarkani, Professor of Engineering Management and Systems Engineering, Dissertation Co-Director

Thomas H. Holzer, Adjunct Professor of Engineering Management and Systems Engineering, Committee Member

Shahryar Sarkani, Adjunct Professor of Engineering Management and Systems Engineering, Committee Member

Copyright © 2011 by Jacqueline Hall

All rights reserved

Dedication

This work is dedicated to the most special people in my life, my husband John, our daughter Jessica, my parents John and Jeanne Huynh, and my brothers Lee Huynh and David Huynh, whose loving, caring, and sacrifices live on every page of this work.

Acknowledgments

First and foremost, I'd like to thank God for His countless blessings in every day of my life. Obvious among them are the ability to do what has been required of me throughout this challenging journey, and the involvement of many people through various means to help me fulfill this work. I am very grateful and humbled by this experience.

I wish to thank the members of my dissertation committee, Dr. Thomas Mazzuchi, Dr. Shahram Sarkani, and Dr. Thomas Holzer, for their insights and leadership shepherding me through the dissertation process. Many thanks also go to Dr. Michael Stankosky, the dissertation committee chair, and Dr. Shahryar Sarkani, for their scholarly support. I am also appreciative of the staff of the EMSE doctoral cohort program, especially Sara Noack, for their timely assistance and support whenever I needed.

I would like to express my sincere appreciation for Dr. Robert Norris, who graciously served as my external advisor. I feel extremely fortunate and humbled to have had the opportunity to meet him and receive his constant support, advice and insightful comments. This work owes a great deal of gratitude for his thorough review and ample feedback since the early versions. A simple thank you will never be enough to convey my gratefulness for his guidance, mentoring, encouragement, and kind support that vastly ensured my academic goals would be fulfilled.

I wish to thank my employer, the National Geospatial-Intelligence Agency (NGA), for providing the education assistance benefits. It is truly my privilege to work for one of the best organizations that takes an active role in fostering the professional development of its employees. I owe everlasting appreciation to Steve Stuban, my former supervisor, and

Rob Cowan for their continued efforts in inspiring me to make the decision to pursue the doctoral program. Their kind words of encouragement and support are also acknowledged. I wish to extend my gratitude to my senior managers, Barry Barlow, Mike Rodrigue, and Mike Carr, as well as Armando Costales, for their benevolent support in getting me much needed time to carry out this endeavor. I owe a special thank-you to my supervisor, Gary Feltz, for his flexibility and gracious support that enabled me to complete this work. Gary, along with Steve Stuban, also treated me with considerable respect and understanding, and made me feel like a worthy employee and colleague during this challenging time. I wish to thank my friends and colleagues at NGA, Tina Crawford, Jim Moran, Jayne Hope, Jeanne Stacey, Robert Bridges, Don McLean, and Tom Witherell, for their support, encouragement, and belief that I would complete this study. Special thanks also go to Dr. Ronzelle Green and everyone in the cohort for their encouragement and camaraderie support. Without the generous support of NGA and its people, this work would never have been possible.

I would like to extend my gratitude to the reviewers of my survey instrument, Dr. Terry Richardson, Lt Col Darren Hall, and Franklin Stone, and to the anonymous reviewers of my research article, for their praise and criticisms. Also special thanks go to the community of information security professionals for their participation in the research survey. The courteous support and astute comments of these people have made this research possible.

Finally, I am eternally grateful to my wonderful family for the love, support and sacrifices that continue to carry me through the most difficult challenges in my life.

In particular, I wish to express my heartfelt thank-you to my parents John and Jeannie Huynh, whose unconditional love, constant support, and selfless sacrifices have allowed me this privilege. My father's vision and tireless insistence on higher education of his children were the fuel that enabled my academic endeavors. My mother's love, patience, and strength continue to guide me through all my walks of life. I look up to her every day and pray that I will be a great mother to my daughter as she is to me. For this particular challenge, I am infinitely thankful to my parents for preparing more than 1600 mail survey packages, and for stocking my refrigerator with sufficient food and snacks on a weekly basis, so that I might have time and energy to concentrate on this work. Mom and Dad, thank you for your unending love and constant support that you continue to give me still today.

I am also appreciative of my brothers, Lee Huynh and David Huynh, and families, for their constant care and support. My brothers have always been there for me through many ups and downs in my life. I'm so grateful to have them to count on.

I wish to acknowledge my grandpa Tai Huynh and my brother Nghia Huynh, whose spirits and loving memories remain forever in my heart. The incessant feelings of their presence around me and their gentle guidance in my dreams have urged me on in this endeavor.

For this particular challenge of my life, I am eternally grateful to the two people, my husband John and our sweet daughter Jessica, who are always by my side and share my hopes and dreams for the future, although I was much less available as a wife and a mother than I should have been. John particularly found my personal goals important and this project worthwhile, and determined to see me through this challenge. His support,

patience, understanding, and willingness to go above and beyond the call of duty as husband and father, allowed my devotion to this work. He has not only taken care of this family on multiples fronts, but also helped my extended family when they needed, while putting up with my studies for the last several years. Without his sense of perspective that raised my spirit when I was most discouraged, I could not have gotten this far. John, thank you for always being there for our family, for facilitating the fulfillment of my scholarly dreams, and for encouraging me to be the best I can be. Significantly, it was my dearest Jessica and her endurance of our loss of precious time together that provided me the inspiration to complete this work faster than it could have been. Jessica, thank you for your warm hugs, beautiful cards and drawings, priceless "I Love You Mom" bookmarks, and remarkable report cards, which gave me the much needed and renewed strength to keep going when the project appeared to be impossible. Most importantly, thank you for being my daughter, and for being a wonderful and kind human being. I am extremely proud of you.

Abstract of Dissertation

Examining Impacts of Organizational Capabilities in Information Security: A Structural Equation Modeling Analysis

In today's modern business world, most organizations use information as a critical business asset to gain competitive advantage and create market value. Increasingly, an organization's ability to protect information assets plays a critical role in its ability to meet regulatory compliance requirements, increase customer trust, preserve brand strength or company reputation, maintain business resiliency, and thereby enhance organizational performance. As information technologies, global connectedness, and business requirements continue to evolve at a fast pace, organizations must recognize the importance of implementing an overall information security strategy to protect business information assets from increasingly sophisticated threats. Given the dynamic pace of business environments, the identification and understanding of the required capabilities to deliver an information security strategy becomes a key success factor. At the strategic level, organizations must be able to answer the question, "What are the minimum essential organizational capabilities required to support effective planning and execution of an overall information security strategy that best achieves organizational objectives and gains competitive advantage?"

This research identifies a set of essential organizational capabilities in the context of information security and examines the impacts of these organizational capabilities on information security strategy implementation success and organization performance. Organizational capabilities in this study include four factors: sense-making, decision making, asset availability, and operations management.

Based on existing literature in strategic management and information security, an original theoretical model was proposed and validated. A self-administered survey instrument was developed to collect empirical data from Certified Information Systems Security Professionals. Structural equation modeling techniques were used to test hypotheses and to fit the theoretical model.

Evidence from this research suggested that organizational capabilities encompassing sense-making, asset availability, and operations management are positively associated with successful implementation of information security strategy, which in turn positively affects organization performance. In addition, this research also demonstrated the indirect effects of the respective organizational capabilities on organization performance. However, significant effects of decision-making on information security strategy implementation success and organization performance respectively were not evidenced.

This research provides the first empirical research examining the impacts of organizational capabilities that can be used as the roadmap for further research explorations in information security from an organizational perspective. Additionally, this study contributes to the research community an original survey instrument that can be applied or built upon to collect data that furthers existing knowledge on the impacts of intangible assets in information security.

Research findings yield practical values for organizations in the private and public sectors by providing their decision and policy makers a better understanding of the viable predisposition of organizational capabilities in the context of information security, thus enabling firms to focus on acquiring the ones indispensable for improving organization

performance. This research also provides insights into the challenges information security professionals continue to face concerning organizational governance. Awareness of these shortcomings allows business leaders opportunities to make necessary changes in direction that enables information security professionals to succeed in their missions of protecting information and information assets.

Table of Contents

Dedication ..... **iv**

Acknowledgments ..... **v**

Abstract of Dissertation ..... **ix**

List of Figures ..... **xvi**

List of Tables ..... **xvii**

List of Acronyms/Symbols ..... **xix**

Glossary of Terms ..... **xx**

Chapter 1 – Introduction **1**

Statement of the Problem 2

Purpose of the Study 3

Limitations 5

Significance of the Study 6

Organization of the Document 7

Chapter 2 - Literature Review **9**

Information Security Strategy 9

Organization Performance 12

Organizational Capabilities 14

Sense-making 16

Decision-making 19

Asset Availability 22

Operations Management 24

Summary 26

Chapter 3 - Research Methodology 27

Identification of Research Questions 28

Hypothesis Formulation 28

Hypothesis 1 29

Hypothesis 2 29

Hypothesis 3 29

Hypothesis 4 30

Hypothesis 5 30

Hypothesis 6 30

Hypothesis 7 30

Hypothesis 8 31

Hypothesis 9 31

Theoretical Model Construction 31

Survey Instrument Development 37

Pretesting of the Survey 38

Design of Survey Instrument 42

Data Collection 51

Research Ethical Assurances 51

Research Participants 52

The Instrument Mailing Package 53
Survey Implementation Procedure 55
Data Analysis 56
Structural Equation Modeling (SEM) Approach 56
Basic Concepts of Structural Equation Modeling 57
Strengths of Structural Equation Modeling 59
Limitations of Structural Equation Modeling 60
SEM Analysis Procedures 62
Assessment of Confirmatory Measurement Model 63
Assessment of Confirmatory Structural Model 65
Summary 71

Chapter 4 - Results 72

Characteristics of The Sample 72
Data Screening 79
Confirmatory Measurement Model 81
Confirmatory Structural Equation Model 98
Analysis of Mediation Effects 107
Summary 110

Chapter 5 – Summary, Conclusions, and Recommendations 111

Summary of Hypothesis Tests 113

Conclusions 117

Implications 121

Recommendations for Future Research 123

References 125

APPENDIX A – SURVEY PRETEST FINDINGS 145

APPENDIX B – IRB EXEMPT APPROVAL 151

APPENDIX C – SURVEY COVER LETTER 153

APPENDIX D – SURVEY INSTRUMENT 155

APPENDIX E – PATH DIAGRAM NOTATIONS 160

APPENDIX F – ASSESSMENT OF NORMALITY 162

APPENDIX G – ADDITIONAL SEM ANALYSIS OUTPUTS 165

APPENDIX H – FEEDBACK FROM RESPONDENTS 171

List of Figures

Figure 1.1: General Mediation Model for the Hypothesized Relationships 4

Figure 3.1: Research Methodology Used in This Study.....27

Figure 3.2: Hypothesized Full Mediation Model.....33

Figure 3.3: Hypothesized Partial Mediation Model.....35

Figure 4.1: Confirmatory Measurement Model Six-Factor Solution.....95

Figure 4.2: Structural Equation Model of Six Latent Variables.....99

Figure 4.3: Results of Confirmatory Structural Equation Model.....103

Figure 4.4: Fitted Model Showing Standardized Direct and Indirect Effect Estimates 109

List of Tables

Table 3.1: Mapping of Variables and Variable Types 37

Table 3.2: Item Measures of Sense-making (SM) 43

Table 3.3: Item Measures of Decision-making (DM) 44

Table 3.4: Item Measures of Asset Availability (OA) 45

Table 3.5: Item Measures of Operations Management (OM) 46

Table 3.6: Item Measures of Information Security Strategy (IS) 47

Table 3.7: Item Measures of Organization Performance (OP) 48

Table 3.8: Alignment of Research Questions, Hypotheses, Survey Items, and Measurement Scales 49

Table 3.9: Acceptable Thresholds of Reliability, Validity and Model Fit Tests 70

Table 4.1: Responses by State 74

Table 4.2: Security Certification 75

Table 4.3: Level of Involvement in Information Security 75

Table 4.4: Years of Experience 76

Table 4.5: Job Function 76

Table 4.6: Organization Industry 77

Table 4.7: Organization Size 78

Table 4.8: Organization Revenues 78

Table 4.9: Varimax Rotated Factor Loading Matrix 83

Table 4.10: Results of the Principal Axis Factoring Extraction Method 85

Table 4.11: Reliability and Convergent Validity Analysis Results for SM.....87

Table 4.12: Reliability and Convergent Validity Analysis Results for DM 88

Table 4.13: Reliability and Convergent Validity Analysis Results for OA.....89

Table 4.14: Reliability and Convergent Validity Analysis Results for OM 90

Table 4.15: Reliability and Convergent Validity Analysis Results for IS 91

Table 4.16: Reliability and Convergent Validity Analysis Results for OP Construct.....92

Table 4.17: Results of Convergent and Discriminant Validity Analysis 93

Table 4.18: Measurement Model Fit Results.....94

Table 4.19: Structural Equation Model Fit Results.....101

Table 4.20: Regression Weights for Fitted Structural Equation Model.....105

Table 4.21: Standardized Effects of Organizational Capability Factors on Organization Performance.....108

Table A1: Pretest Findings, Observations, and Revision Decisions 146

Table E1: Summary of Path Diagram Notations.....161

Table F1: Univariate Skewness and Kurtosis Descriptive Statistics (N=428) 163

Table G1: Squared Multiple Correlations of the Fitted Model 166

Table G2: Covariances of the Fitted Model.....167

Table G3: Correlations of the Fitted Model.....168

Table G4: Variances of the Fitted Model.....169

List of Acronyms/Symbols

1.	AMOS	Analysis Of Moment Structures
2.	AVE	Average Variance Extracted
3.	CFA	Confirmatory Factor Analysis
4.	CFI	Comparative Fit Index
5.	CISSP	Certified Information System Security Professional
6.	IRB	Institutional Review Board
7.	$(ISC)^2$	International Information Systems Security Certification Consortium
8.	ML	Maximum Likelihood
9.	PAWS	Predictive Analytics Software
10.	RMSEA	Root Mean Square Errors Of Approximation
11.	SEM	Structural Equation Modeling
12.	SRMR	Standardized Root Mean Square Residual
13.	TLI	Tucker-Lewis Index
14.	χ^2	Model Chi-Square

Glossary of Terms

Asset availability: The ability to obtain and organize the competencies and processes needed to accomplish information security strategy goals and ensure employees have the necessary skills and resources to achieve it.

Competencies: Differentiated knowledge, skill, ability, distinctive organizational processes and other characteristics needed to perform a specific task.

Decision-making: The ability to make decisions with respect to courses of action and planning, to collaborate, empower, and communicate information security strategy, as well as to commit to information security initiatives in support of the missions and business functions of organizations.

Information Security Strategy: A plan of actions designed to minimize risks in information environments

Information Security Strategy Implementation: The degree to which information security programs protect and defend information and information systems against adversary threats on compromising the confidentiality, integrity, and availability, allow for better control of information assets, respond promptly to and recover quickly from information security attacks, while complying with legal, statutory, contractual, and internally developed requirements.

Operations Management: The ability to manage and deploy the combined competencies and resources across the organization in support of information security operations. This also involves the ability to measure and learn over time about risks and

the operational environment for continuous improvement to information security programs.

Organizational Capabilities: For the purpose of this study, organizational capabilities are defined as intangible assets consisting of competencies along with the dynamics of integrating and deploying those competencies with inimitable resources across organizational boundaries to operate the business.

Organization Performance: The degree to which organizations produce and accomplish business objectives and values for the various stakeholders. This includes preventing costly legal action related to the protection of information assets from government agencies, stockholders or others, improving customers service, preserving public's perception of brand strength or company reputation, and market valuation, while maintaining business resiliency in the face of an increasingly sophisticating risk environment.

Resources: Human, physical, financial, and technological resources used to accomplish the organizational goals.

Sense-making: The ability to develop high quality awareness and understanding of current and future threats and vulnerabilities, social, political and economical challenges, coupled with the organization's missions and constraints, and to lay out courses of actions for effective decision-making.

Chapter 1 – Introduction

Despite the increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations (Ernst & Young 2007; Ernst & Young 2008; Fratto 2009; TechAmerica 2009; PricewaterhouseCoopers 2008). Businesses have been urged to make information security a strategic issue for organizations to compete and survive in this era of the global economy and ever changing enterprise risk (Wood 1993; Ezingeard et al. 2005; Amaio 2009). Success in such demanding business environments depends in large part on implementing an effective information security strategy to protect information and information assets. Recent information security literature recommends organizations employ an overall information security strategy that integrates "people, processes, technology, and operations capabilities" to ensure effective defenses across the organization (Allen 2005; FFIEC 2006; NIST 2008). Additionally, the modern world of global connectedness and rapidly advancing information technologies has made technology-driven security solutions inadequate to meet information security challenges (Caralli 2004; Alberts et al. 2001; Alberts and Hayes 2003). In order to face the challenges and to take advantage of new opportunities brought forth by information technology advances, Caralli (2004) suggests organizations shift the focus from a technology-based information security strategy to an organizational-based approach that considers a core set of organizational capabilities. Therefore, the identification and understanding of organizational capabilities is essential

to logically recognize the relationship between information security strategy implementation success and organization performance.

Statement of the Problem

The overall objective of this research is to address two information security related issues. First, organizations need to have a clear understanding of the minimum essential capabilities required for effective information security strategy and build the ones indispensable for creating business value. In today's complex, competitive and dynamic marketplace, organizations may not be equally predisposed for effective implementation of their information security strategy. Thus, a key to information security strategy implementation success within organizations is the identification and assessment of preconditions necessary to deliver strategic goals. These preconditions refer to an organization's capabilities, the means by which information security strategy gets implemented.

Second, the organizational aspect of information security is still largely unexplored. Information security is an interdisciplinary field encompassing organizational, managerial, and technical aspects (Von Solms 2006; Werlinger et al. 2009). However, most prior research efforts on information security have been traditionally dedicated to the technical or managerial side (Chang & Ho 2006; Kankanhalli et al. 2003; Knapp et al. 2006). Among the limited number of studies concerning organizational capability, few have empirically analyzed organizational capability as a multidimensional construct (Kusunoki et al. 1998). In particular, there has been almost no evidence of information security research devoted to

empirical analysis of organizational capability as an aggregation of sense-making, decision-making, organizational assets, and operations management constructs. Of special importance, with the exception of research studies discussing these constructs as best practices in information security management literature, there is a lack of empirical research on these constructs as organizational capabilities impacting information security strategy effectiveness and organization performance.

Purpose of the Study

In efforts to contribute to the existing body of knowledge about the organizational aspect of information security, this study addresses the high level research question concerning impacts of organizational capabilities on information security strategy and organization performance. This is accomplished by proposing and validating a theoretical model that demonstrates the linkages between effective implementation of information security strategy and organization performance, with organizational capabilities as important factors influencing effective implementation of information security strategy and organization performance. In other words, this research suggests that information security strategy implementation success mediates the relations between organizational capabilities and organization performance. Figure 1.1 illustrates the general mediation model for addressing the research objectives. This general model suggests that the successful implementation of the information security strategy is

affected by organizational capabilities, and in turn influences the performance of an organization.

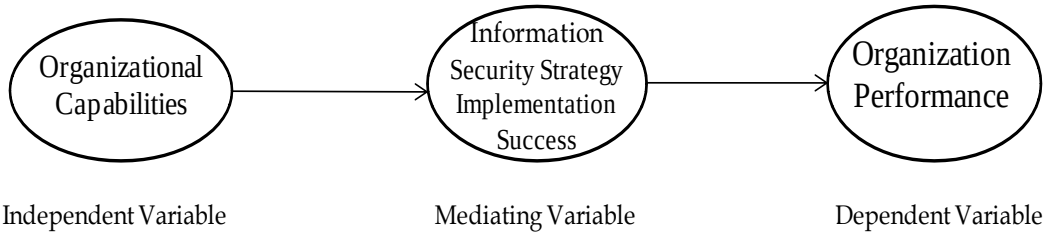


Figure 1.1. General Mediation Model for the Hypothesized Relationships

The following research questions were developed to guide this study.

Research Question 1: What is the relationship, if any, between information security strategy implementation success and organization performance?

Research Question 2: What are the relationships, if any, between organizational capabilities and information security strategy implementation effectiveness?

Research Question 3: To what extent do organizational capabilities influence organization performance?

The first two research questions sought to investigate the linkages between successful implementation of information security strategy and organization performance and organizational capabilities respectively. The third research question sought to explore and assess the level of impacts of organizational capabilities on organization performance.

Together, the perspectives of the prior work by Alberts and Hayes (2003) and Ulrich and Smallwood (2004) coupled with information security literature given by Allen (2005), Caralli (2004), FFIEC (2006), and NIST (2008) provide a useful theoretical foundation for defining the constructs to build the theoretical model. These include organizational capability constructs represented by sense-making, decision-making, asset availability, operations management, along with information security strategy implementation success and organizational performance constructs.

The approach to address the research questions is a quantitative methodology that involves fitting a hypothetical model to the observed data and testing the hypothesized relationships. The empirical data is collected from the certified information system security professionals using an original survey instrument of 50 items. The structural equation modeling (SEM) techniques are used to examine the relations among organizational capability, information security strategy implementation success and organization performance constructs. Structural equation modeling is a comprehensive statistical technique for testing hypothesis and fitting the structural model, and therefore appropriate for this study.

Limitations

Due to the general lack of available research in the underlying concept, an original survey was developed to collect empirical data. However, the survey instrument was perceived by respondents as designed with focus on medium-to-large firms in the private

sector. Future use of this instrument may benefit from higher response rates if the organization performance scale is revised to better apply to government/non-profit organizations. Further, there may be a potential source of bias resulting from the technical nature of the intended population. By polling primarily information security specialists, the results may have been partially influenced by their inherently technical perspective. In efforts to further the generalized knowledge of the impacts of organizational capabilities in information security, future research in which the respondent sample includes a reasonable mix of senior managers and information security professionals is recommended.

Significance of the Study

The study is beneficial not only to the business world, but also to the research community. In part, findings yield practical value for business leaders in understanding the viable predisposition of organizational capabilities in the context of information security, thus enabling firms to focus on acquiring the ones indispensable for improving organization performance.

Additionally, this work introduces the mix of organizational capability constructs that are essential to an organization's information security strategy and performance, while contributing to the literature for an empirical study on the effects of intangible assets in information security. This study is the first known empirical research examining the impacts of organizational capabilities that may have implications for further research opportunities and explorations in information security from an organizational perspective.

Additionally, this study contributes to the research community an original survey instrument that can be applied or built upon to collect data that furthers existing knowledge on the impacts of intangible assets in information security.

Organization of the Document

The current chapter provides an overall statement of the nature of the original research and the rationale for undertaking the study. The specific research questions along with an overview of the methodology that best addresses the research questions are described. The key terms that are relevant to the study are defined in this chapter. Limitations and significance of the study are also identified. The remainder of this document is organized as follows.

Chapter 2, Literature Review, presents a review of past research and studies in the fields of information security and strategic management. These interdisciplinary theoretical perspectives provide the conceptual foundation that is crucial for the identification of the constructs and the development of the theoretical model in this research. The content of the literature review also enables the generation of the questionnaire items for the original survey instrument.

Chapter 3, Research Methodology, presents the six methodological steps that are essential to the accomplishment of the identified research objectives. Topics such as the building of the theoretical model to test the hypothesized relationships, the development of an original survey instrument to collect empirical data, the data collection procedures to

implement the survey instrument at hand, and the data analysis methods based on SEM techniques are covered. Strengths and limitations of the SEM data analysis approach are also discussed.

Chapter 4, Results, reports the results of the quantitative analysis essential to validating the theoretical model and testing the hypotheses in this study. It comprises of two primary sections: the first section focuses on the characteristics of the research sample, and the second section discusses the results of the SEM analysis as it pertains to the research questions. Data screening procedures that must be considered prior to SEM analysis to identify and rectify potential problem, such as missing data and nonnormal distributions are described in this chapter.

Chapter 5, Summary, Conclusions, and Recommendations, provides a summary of main findings and a conclusion to sum up the purpose and findings reported in the study. Following these discussions, the implications of the current study and recommendations for further research opportunities are presented.

Chapter 2 - Literature Review

This chapter reviews each of the constructs critical to the development of the theoretical model for this research: information security strategy, organization performance, sense-making, decision-making, asset availability, and operations management. Generally speaking, there are few published studies with theoretical models illustrating key constructs hypothesized in this study. Primarily, prior works by Alberts and Hayes (2003) and Ulrich and Smallwood (2004) coupled with the information security literature of Allen (2005), Caralli (2004), FFIEC (2006), NIST (2007), and NIST (2008) and other researchers and practitioners provide a useful theoretical foundation for defining the constructs to build the theoretical model for this study.

Information Security Strategy

In the last decade, information and information security have moved beyond the boundaries of academia to play key roles to improve overall business objectives and create competitive advantage (Saugatuck Technology 2008; Schultz 2006; Tallon et al. 2000; Wood 1993). More and more businesses around the world now recognize information as a vital business asset, and their adequate protection is critical to the success of organizations in today's globally connected and complex business environment (Straub 1990; FFIEC 2006; McFadzean et al. 2007; Kaplan & Norton 2007). As such, information security is more challenging now than ever before to defend a business against increasingly

sophisticated information security threats (Anderson & Choobineh 2008; Park & Ruighaver 2008; Symantec 2009).

The challenges of a competitive marketplace with constantly changing busi ness requirements and the upward trend of cyber threats are requiring the need for a more strategic view of information security (Kankanhalli et al. 2003; Park & Ruighaver 2008; Straub 1990). Indeed, according to Allen (2005), "national and international regulations are calling for organizations to demonstrate due care with respect to security". This is crucial to providing an agile and trusted environment for organizations to compete and survive in the current marketplace. Organizations are urged to develop an information security strategy that incorporates and integrates a set of essential organizational capabilities that enable them to triumph over shortcomings due to dynamic changes in technology and globalization, and to rapidly anticipate and respond to a wide array of emerging and complex challenges (NIST 2008; Park & Ruighaver 2008; Kankanhalli et al. 2003). NIST (2008) stated that, "to mitigate risk from the global supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide, defense-in-breadth approach." Lack of a proactive information security strategy to make information available, accessible, assured, and appropriately protected can disrupt operations and pose serious risks to the organization's performance and competitiveness as well as to those of customers (Fratto 2009; Wood 1993; FFIEC 2006; Allen 2005).

An information security strategy is a plan of action designed to minimize the risk in information environments, and focus on return on investment and value from information security program, while complying with legal, contractual, and organizational requirements (Nyanchama 2005; FFIEC 2006; Amaio 2009). According to FFIEC (2006), an information security strategy should incorporate four key concepts. First, appropriate prevention, detection, and response mechanisms should be included to ensure a comprehensive and robust security framework. Second, access restriction measures such as security domains, least permissions, and least privileges should be established to prevent unauthorized access and limit potential harmful actions. Third, multiple-layered security controls between threats and organizational assets should be implemented to increase the probability of detecting attacks. Finally, policies and procedures should be integrated as part of the organization's governance structure and technology design that guide users of their security responsibilities and ensure information security compliance. FFIEC concluded that information security policies, standards, and procedures provide the means by which information security objectives can be measured. Additionally, McFadzean et al. (2007) suggested that to ensure the effectiveness of the strategy, information security must add value to the organization's aims and objectives, as well as its business processes, business operations, employees and customers. ISACA (2009) opined further that an effectively managed information security strategy can be instrumental in helping an enterprise meet its business goals.

Organization Performance

Richard et al. (2009) suggested that competitiveness has made organizational performance crucial to the continued existence and success of organizations in the modern business landscape. Consequently, the concept of organizational performance is one of the most important subjects for researchers as evidenced in the management literature, whereby organization performance is included as a dependent, independent, or control variable in numerous published articles (March and Sutton 1997 as cited in Richard et al. 2009; Richard et al. 2009). Richard et al. also argued that despite much that has been published, there is little consensus on the definition of organizational performance as evidenced in a study by Kirby (2005). However, the authors referred to organization performance as outcomes of a firm in three specific areas: (1) financial performance (profits, return on assets, return on investment, etc.); (2) product market performance (sales, market share, etc.); and (3) shareholder return (total shareholder return, economic, value added, etc.). They elucidated that the measurements of these outcomes allow firms and managers to evaluate specific actions necessary to improve the ability of an organization to deliver goods and services and to survive, compete, and gain competitive advantage.

Wood (1991) posited that an organization can benefit from its ability to protect information and the environment in which it exists through implementing an effective information security strategy. The author opined further that by understanding the tangible benefits of meeting information security objectives, management may be motivated to

invest more resources to ensure successful implementation of their information security strategy. Wood cited four potential benefits resulting from the effective implementation of information security that include improved image of the organization as a conscientious corporate citizen, enhanced customer confidence, new products and services, and new security features for existing products and services.

In a study where data were collected through interviews of company executives, Ezingeard et al. (2005) developed a four-layer model categorizing benefits of information assurance: (1) *Operational benefits*: those benefits with immediate positive impacts on the organization's ability to deliver goods and services more efficiently or effectively, (2) *Tactical benefits*: those benefits with medium-term positive impacts on the organization's relationships with its trading partners, (3) *Strategic benefits*: long-term benefits in nature and connected with competitive advantage, and (4) *Organizational benefits*: those benefits sought by the owners or key stakeholders of the organization.

A number of information security publications in recent years also indicated that information security provides benefits to business. Among them are created are through minimizing risks to operations and business, maintaining compliance with the law, preserving brand strength and company reputation, increasing customer trust, sustaining business resiliency, realizing higher performance gains and financial savings, and thereby achieving organizational objectives and improving business performance (Caralli 2004; van Opstal & Council on Competitiveness 2007; Nyanchama 2005; NIST 2007; Kim 2004).

In a study on information security objectives and practices, Ma (2004) reviewed the information systems management literature concerning the goal setting and strategic alignment, wherein a positive relationship between business strategy and performance was evidenced. As part of this review, positive relations among information system strategy, information system effectiveness, and business performance were also affirmed.

Organizational Capabilities

Success in meeting the challenges posed by the modern world necessitates business focus on the preconditions that are critical to the effective implementation of an information security strategy to protect and defend information assets against adversarial threats on compromising confidentiality, integrity, and availability. In general, these preconditions are designated as capabilities, within the classical strategic management and organizational theory literature (Gold et al. 2001; Kelly & Amburgey 1991; Wernerfelt 1984; Teece et al. 1997; Prahalad & Hamel 1990; Barney 1991; Barney & Zajac 1994). The concept of organizational capabilities has been the focus of research in the field of strategic management and organizational theory, even though it has various definitions (Ansoff 1965; Porter 1985; Ulrich & Lake 1991; Grant 1991; Stalk et al. 1992; Kusunoki 1998; Rangone 1999; Eisenhardt & Martin 2000; Ulrich & Smallwood 2004; Smallwood and Panowyk 2005; Wethyavivorn et al. 2009). Regardless of the various classifications, most research shares the same viewpoint that organizational capabilities have the potential

to become a source of sustainable competitive advantage, and that they are difficult to imitate and substitute (Barney 1991; Collis 1994; Teece et al. 1997; Kusunoki et al. 1998).

Over the years, numerous studies in strategic management have indicated that strategy is critical for achieving business objectives and competitive advantage (Porter 1985; Prahalad & Hamel 1990; Cockburn et al. 2000; Eisenhardt & Martin 2000; Slater & Olson 2001). However, as Smallwood and Panowyk (2005) suggested, it is capabilities that give stakeholders confidence that an organization can develop and execute its strategy. The resource-based view of strategy also reaffirms the strategic importance of organizational capabilities in enabling firms to plan, formulate, and implement their strategies (Barney and Zajac 1994). Indeed, according to Ulrich and Smallwood (2004), organizational capabilities are what people respect most and expect from successful companies, not their organizational structure or their specific approaches to management. Additionally, research indicated that organizational capabilities cannot be built independent of leadership (Ulrich & Smallwood 2004; King 1999). Besides leadership, Ulrich and Smallwood also suggested some other capabilities organizations must possess to be able to carry out their missions and objectives: talent, speed, shared mind-set and coherent identity, accountability, collaboration, innovation and efficiency. Smallwood and Panowyk (2005) concluded that a business gains advantage only when it possesses appropriate organizational capabilities that "drive every aspect of performance, including customer satisfaction, competitive positioning, and bottom-line results".

In the rapidly changing technology and highly connected environments, Alberts and Hayes (2003) proposed a framework that considered a set of essential capabilities for identifying "the shortcomings of existing force structure, concepts of operations, personnel, education, training, material, and systems" required for successful information warfare operations. This framework consists of the ability to make sense of the situation, to work in a coalition environment, to possess appropriate means, and to orchestrate the means to respond in a timely manner. Although the focus of Albert and Hayes's framework is on military and government, it can also apply to other organizations as they will likely encounter similar shortcomings facing challenges of the modern world.

Overall, there are few published studies with theoretical models that illustrate the organization capability concepts in terms of sense-making, decision-making, asset availability, and operations management in literature. Each of these variables has a literature base, although some of which may be limited than others. Nonetheless, the contents of the literature review provide a useful theoretical perspective for the research,.

Sense-making

In general, sense-making tasks often involve searching for documents that are relevant for a purpose and then extracting and reformulating information so that it can be used (Alberts et al. 2006). Moreover, Alberts & Hayes (2003) indicated that sense-making involves not only sharing information and recognizing trends, but also generating options, predicting adversary actions and reactions, and understanding the effect of choices of actions.

Sense-making is sometimes confused with situational awareness. Although the phenomena may be related, they have different meanings. Modern researchers seem to differentiate these aspects in the manner as follows. Klein et al. (2006) indicated that "sensemaking is a motivated, continuous effort to understand connections (which can be among people, places, and events) in order to anticipate their trajectories and act effectively". In contrast, Endsley (1995) pointed out that situational awareness is about the state of knowledge "that's achieved – either knowledge of current data elements, or inferences drawn from these data, or predictions that can be made using these inferences". In a broad sense, situational awareness means using observations to understand what is likely to happen in order to devise appropriate actions (Perla et al. 2000; Endsley 2004; Weick et al. 2005)

In protecting information and defending information assets, practitioner literature suggests that preparation is vital to successful information security practices (ODNI 2008). This includes the ability to anticipate change, a process that embodies recognizing and understanding early indicators, as well as developing and providing effective warnings of potential and ongoing information security attacks to decision-makers. Operations throughout organizations need to know when the information security threats changes to adapt and respond rapidly and appropriately. This process is generally best understood as situational awareness.

With the growing use of information technology that accounts for the increased status of information security, situational awareness in information security has become

widely recognized among researchers and practitioners as playing a crucial role in the successful information security program (Thomson & von Solms 1998; Straub & Welke 1998; Siponen 2001; NIST 2003). Information security awareness is defined in the research literature as a state wherein users in an organization are made aware of and committed to security objectives (Rezgui and Marks 2008; Siponen 2000), and in the practitioner literature as activities that seek to focus the attention of an individual or organization to information security concerns and act effectively in a given situation (ODNI 2008; NIST 2003; NIST 2010). The key objective of information security awareness is to heighten the significance of information security and the possible negative effects of security problems that enable appropriate actions to prevent and correct security breaches (Hansche 2001; Kruger & Kearney 2006; Chen et al. 2008a). This is normally accomplished by using means such as education and training to provide users adequate knowledge of their information security responsibilities, organizational policies, and how to properly use and protect the organization's information assets (NIST 2003; ISO 2005).

Although the literature suggested that situational awareness fundamentally plays a critical role in sense-making, it simply represents one of the dimension delineating sense-making as suggested by Alberts & Hayes (2003). This is not surprising since sense-making is the ability to make sense of a situation, a process that is undertaken to develop situational awareness and understanding of situations that requires attention, in which knowledge enables courses of actions to facilitate decision making (Perla 2000; Leedom 2001; Alberts et al.2001; Alberts 2002). Thus, Alberts & Hayes (2003) concluded, awareness,

knowledge and understanding are the dimensions of sense-making, whereas decisions are the products of sense-making.

Decision-making

As implied in the preceding section, decision-making is related to the concept of sense-making, thus demonstrating some levels of dependency on awareness, knowledge, and understanding. In an age of uncertainty and change, successful sense-making distinguishes the most effective leaders through their ability to quickly extract and analyze all relevant information and to constantly readjust and align organizational goals and objectives as they take in new information (MIT). Alberts et al. (2001) argued that although decisions obviously can be made independently of any awareness, knowledge and understanding, such decisions would essentially be random rather than decisive, and would, therefore, likely prove decision-making ineffective. In the realm of information warfare, Alberts alone, and with others, defined effective decision-making as the capability to form focused and timely decisions that proactively and accurately respond to emerging opportunities and threats with the available means and capabilities (Alberts 2002; Alberts & Hayes 2003; Alberts et al. 2001).

In business and politics, the central tenet of decision-making is generally associated with leadership, a position that is somewhat different from a management position (Kotter 1990; McCrimmon 2008). As McCrimmon (2008) pointed out, when executives make decisions, they are acting as managers, therefore, the segregation between leadership and management should be rejected.

Similarly, Anderson and Choobineh (2008) argued that the security decision-making process should be made not only at the tactical and operational levels, but also at the strategic level. At the tactical and operational levels of an organization, decision making focuses on the optimization of security resources through the implementation of information security governance that integrated plans, personnel, procedures, guidelines and technology to minimize security risks and resulting losses. At the strategic level, "information, executive sponsorship, and management leadership" coupled with "choices between alternative solutions" are essential to the successful implementation of information security best practices (e.g. plans, personnel, procedures, guidelines). The authors suggested that effective and timely decision-making are based on data and information concerning assets and processes to be protected, impacts and likelihood of breaches, and costs and effectiveness of best practices. Hence, Anderson and Choobineh concluded, "management must be able to evaluate the current state of detection and prevention capabilities for purposes of compliance and fulfillment of security plans, and to discover gaps between current capabilities and future period needs".

Wood (1993) suggested that information security is not just a technical issue, but a business issue that "should be of great concern to top management". More than ten years later, FFIEC (2006) echoed Wood by stating that "information security is a significant business risk that demands engagement of the Boards of Directors and senior business management." Indeed, significant leadership focus on support and commitment was placed on individuals who participate in the decision making process at the oversight and

management level, as well as at the executive and board levels (Allen 2005; ISACA 2005; Knapp et al. 2006; McFadzean et al. 2007; NIST 2007; GAO 2006). Top management support has been identified as highly critical to the success of an information security program. Publications stated that without senior management's full support of the information security program and commitment of appropriate resources to achieve information security objectives, the employee's sense of obligation or responsibility to the program may be discouraged, which in turn may be detrimental to the success of the information security program (Knapp et al. 2006; GAO 2006; ISACA 2005; Knapp et al. 2005; NIST 2007). According to Allen (2005), the ability of an organization to achieve and sustain information security starts with executives' sponsorship and commitment brought about by governance actions. Executives can demonstrate an active commitment through activities such as visible participation and action, ongoing communication and clear intention to support information security initiatives and to mitigate security risks, serving as role models in placing high priority on information security, and promoting workforce collaboration to protect business assets (NIST 2007; ISACA 2005).

McFadzean et al. (2007) suggested a number of reasons that call for greater board commitment and involvement in information security planning and control. In part, the highly regulated and interconnected business world has made the tasks of achieving compliance with information security laws and regulations paramount than ever before. Thus, institutional investors increasingly search for organizations that demonstrate good corporate governance and risk management policy as positive indications of a shareholder-

value focus. Further, a good level of alignment between an organization's information resources and its business strategy can be a significant source of competitive advantage. Finally, successful implementation of information standards and policies require active board engagement and commitment.

Asset Availability

A review of the literature indicated that definitions of "assets" vary from one organization or individual to another. In the broadest sense, assets include a broad range of tangible or intangible resources representing ownership of value. Tangible assets include physical items such as buildings and equipment, whereas intangible assets include non-physical resources such as information and data. In a review of recent business articles, Hughes et al. (2006) pointed out that most U.S. companies identified organizational assets, predominantly the intangible assets such as innovation, brands, research and development capabilities, human capital, and supply chain efficiencies, as key factors of long-term strategies crucial for achieving organizational goals. Similarly, Adams (2006) referred to intangible assets of a corporation as the intellectual capital, including a broad range of people, and knowledge and relationship assets, which is the key to the organization's growth, innovation, and competitive advantage. In the realm of information security, Ashboul (2010) classified information and information systems as tangible and intangible assets. The NIST SP-800 series described an asset, or organizational asset, as "a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems" (Kissel 2006). Furthermore, McCumber

(2005) defined an asset as "anyone or anything that requires protection such as people, which are a key asset, facilities, equipment, inventory, and certainly information and data". ISO (2005) suggested that an organization may have many types of assets encompassing information, software assets, physical assets, services, people and their qualifications, skills, and experience, and intangibles such as reputation and image of the organization. Notwithstanding various meanings of assets, the information security literature proliferated in recent years indicates a consensus among researchers and practitioners, in which information and information resources are the organization's most valuable assets, and therefore, must be protected and safeguarded from threats (Straub 1990; ISO 2005; FFIEC 2006; McFadzean et al. 2007; Kaplan & Norton 2007; Ashboul 2010).

As previously discussed, the pace, scale, and complexity of change are unprecedented in the dynamic global environment. In this modern world, geographic borders and jurisdictional boundaries are vague, local happenings cause global impacts and vice versa, risks are not easily detected, identified or tracked, and threats are sophisticated and agile. Therefore, information security is more critical and more challenging than ever before to protect information and information assets in this highly interconnected world. Despite technical advances that provide existing tools to protect information assets, technology alone is not sufficient as information security threats and vulnerabilities have also increased (Alberts 2002; Deloitte 2008; ISACA 2009). Caralli (2004) pointed out that security in the information age is a business problem, and thus can no longer be managed effectively from the technical sidelines or as a stand-alone

discipline. Caralli elucidated further that organizations must integrate, synchronize, deploy, and direct many of its existing core competencies to work together to provide effective solutions. According to NIST (2007), in addition to management commitment, inadequate resources often challenge the successful implementation of information security strategy. Wethyavivorn et al. (2009) pointed out that the lack of capabilities to obtain and deploy various resources and competencies poses a critical problem for organizations to effectively compete in the future market to achieve organizational goals.

Availability along with confidentiality and integrity are important elements of the information security concept. If confidentiality refers to the protection of information from unauthorized access and integrity represents the accuracy and robustness of data, then availability is the timeliness factor (McCumber 2005). In this era of interconnectedness, advanced technology, and rapidly changing threats, Alberts & Hayes (2003) suggested that the ability to act jointly and quickly often distinguish winners from all others. The authors elucidated that the underlying capability is essential in ensuring a response at the appropriate time, which is a timeliness factor.

Operations Management

In this modern business world of global economy, extremely dynamic interconnectedness and ever-changing enterprise risk, a static security program will become ineffective over time (Reymann 2007). Hence, the implementation of information security strategy cannot be viewed as a rigid execution of plans. Caralli (2004) asserted that an organization's ability to act appropriately and, more importantly,

sustain success, starts with the transition "toward a security management process that is strategic, systematic, and repeatable—in other words, efficient at using security resources and effective at meeting security goals on a consistent basis". Similarly, Rayman (2007) suggested that firms implement continuous risk assessment, monitoring, alerting, compliance, and training best practices throughout the organization to ensure effective resource allocations, thus enabling organizations to focus on revenue generating activities. Conversely, those that have not done so continue to struggle with reactive security measures, over-allocated resources for troubleshooting activities, and enforcing compliance.

An important part of any organization's approach to implementing security are the policies, procedures, standards and guidelines that are established roles and responsibilities for users of the organization's information and information assets. Collectively, these documents provide the guidance needed to determine how security will be implemented in the organization (Conklin et al. 2004). Like other managed activities, successful implementation requires aligning the information security strategy with business strategy, implementing performance metrics to measure real success, scheduling periodic revision of plans, and incentivizing for achieving security goals (Corby 2002; Anderson and Choobineh 2008).

Summary

This chapter presented a review of literature in the fields of information security and strategic management. These interdisciplinary theoretical perspectives provided the conceptual foundation necessary for identifying the hypothesized constructs. These include information security strategy, organization performance, along with organizational capabilities represented by sense-making, decision-making, asset availability, and operations management. Additionally, knowledge was also gained from the content of the literature review, enabling the researcher to develop the hypothetical research model and the survey instrument.

The next chapter describes in detail the research methodology for conducting this research. The building of the theoretical model used to test the hypothesized relationships and the development of an original survey instrument to collect empirical data for validating the research hypotheses are discussed. The basic concepts of the structural equation modeling techniques applied in this research to validate the consistency between the proposed research model and the empirical data are also provided.

Chapter 3 - Research Methodology

In an effort to contribute to the generalized knowledge in information security, the overarching purpose of this research is to examine the issues of information security from the perspective of organizational capabilities. This perspective suggests that there is a cause and effect relationship between successful implementation of information security strategy and organization performance, with an organization's information security capabilities as important factors affecting this relation.

This chapter describes the methodology used to assess the identified research objectives. This research methodology consists of six steps as illustrated in Figure 2.1 below. The sections that follow describe these steps in detail.

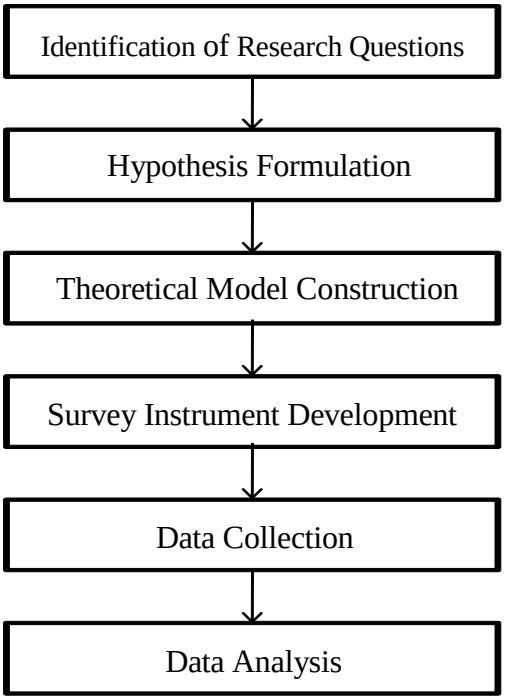


Figure 2.1. Research Methodology Used in This Study

Identification of Research Questions

The basic tenet of any scientific endeavors is the identification of specific research questions to provide a conceptual basis and focus for the theory to be studied (Salkind 2009; Ohab 2010). In this study, a thorough review of existing literature presented in the previous chapter garnered the researcher insights necessary to formulate the questions that reflected the overall research purpose. The research questions (RQ) for this study are identified below.

RQ1. What is the relationship, if any, between information security strategy implementation success and organization performance?

RQ2. What are the relationships, if any, between organizational capabilities and information security strategy implementation success?

RQ3. To what extent do organizational capabilities actually influence organization performance?

Hypothesis Formulation

Once the questions that served as the guiding light for the research were firmly established, the next logical step was to devise a set of hypotheses to address the research questions. In this study, a set of hypotheses was developed based on the content of literature reviewed. These hypotheses transformed the research questions into declarative statements that were deemed more suitable to testing using the data analysis method

discussed herein. The following hypotheses were developed to address the research questions.

Hypothesis 1

$H1_0$: Successful implementation of an overall information security strategy is positively associated with organization performance.

$H1_A$: Successful implementation of an overall information security strategy is not positively associated with organization performance.

Hypothesis 2

$H2_0$: Sense-making is positively associated with information security strategy implementation success.

$H2_A$: Sense-making is not positively associated with information security strategy implementation success.

Hypothesis 3

$H3_0$: Decision-making is positively associated with information security strategy implementation success.

$H3_A$: Decision-making is not positively associated with information security strategy implementation success.

Hypothesis 4

$H4_0$: Asset availability is positively associated with information security strategy implementation success.

$H4_A$: Asset availability is not positively associated with information security strategy implementation success.

Hypothesis 5

$H5_0$: Operations management is positively associated with information security strategy implementation success.

$H5_A$: Operations management is positively associated with information security strategy implementation success.

Hypothesis 6

$H6_0$: Sense-making and organization performance is fully mediated by information security strategy implementation success.

$H6_A$: Sense-making and organization performance is not mediated by information security strategy implementation success.

Hypothesis 7

$H7_0$: Decision-making and organization performance is fully mediated by information security strategy implementation success.

$H7_A$: Decision-making and organization performance is not mediated by information security strategy implementation success.

Hypothesis 8

$H8_0$: Asset availability and organization performance is fully mediated by information security strategy implementation success.

$H8_A$: Asset availability and organization performance is not mediated by information security strategy implementation success.

Hypothesis 9

$H9_0$: Operations management and organization performance is fully mediated by information security strategy implementation success.

$H9_A$: Operations management and organization performance is not mediated by information security strategy implementation success.

Theoretical Model Construction

After the research questions and corresponding hypotheses were successfully finalized, the researcher proceeded to construct a model to depict the hypothesized relations among variables. Indeed, the data analysis procedure employed in this study, namely structural equation modeling, necessitates the specification of a priori model before any analysis could take place (Kline 2005).

A model is a statistical statement or a predicted pattern of relations between two or more variables (Hoyle 1995; Reinard 2006). Therefore, the theoretical model enables a researcher to methodologically estimate the hypothesized impacts among elements of the model (Hoyle 1995; Maruyama 1995; Reinard 2006). To better demonstrate the

hypothesized effects, a path diagram is often used to visually illustrate the theoretical model. Within a model, each variable can be defined either as independent variable (exogenous) or dependent variable (endogenous). The designation of a construct variable as independent or dependent is therefore determined by whether or not an arrow is drawn from one variable to another variable (Schumacker & Lomax 2004). Independent variables are variables that have no arrowheads pointing toward them and are not influenced by other variables (Schumacker & Lomax 2004; Maruyama 1995). In contrast, dependent variables are influenced by other variables in the models and have arrowheads pointing toward them (Schumacker & Lomax 2004; Maruyama 1995).

Following an extensive review of relevant theory and literature, a hypothetical model was constructed to demonstrate the hypothesized relations among organizational capabilities, effective implementation of information security strategy, and organization performance. Figure 3.2 presents the path diagram illustrating this theoretical model, wherein six constructs are hypothesized, Sense-Making, Decision-Making, Asset Availability, Operations Management, along with Information Security Strategy Implementation Success and Organization Performance.

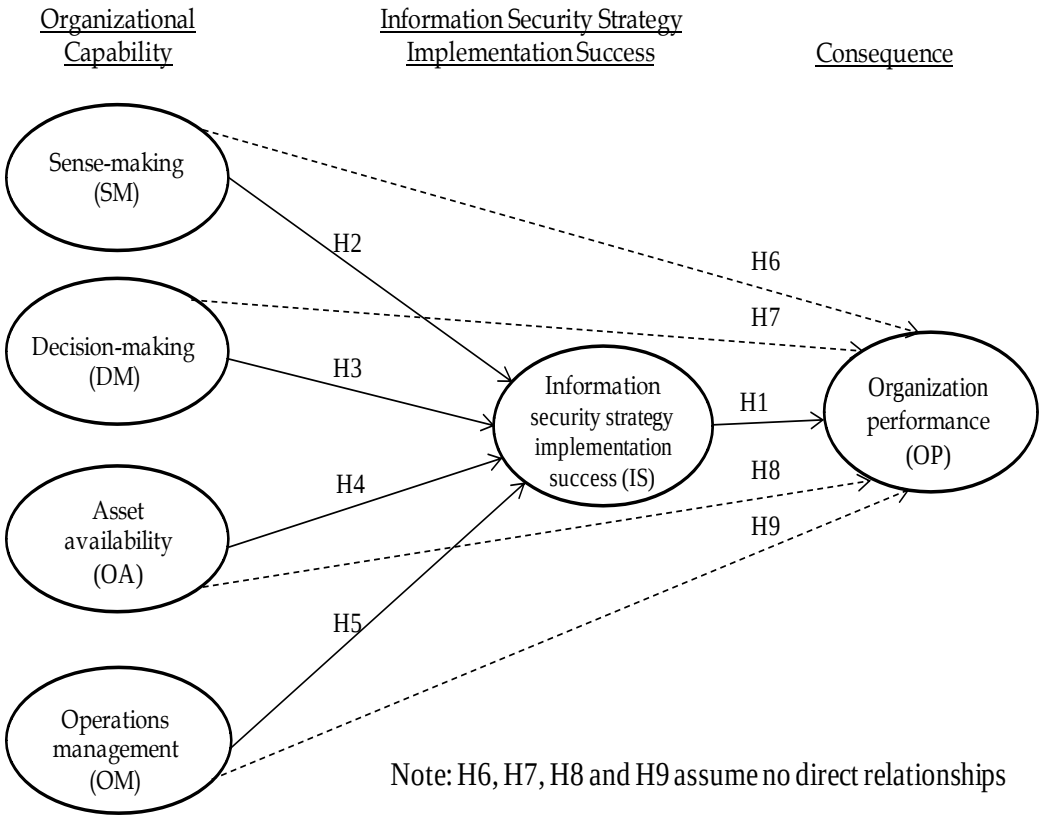


Figure 3.2. Hypothesized Full Mediation Model

In this model, Sense-making, Decision-making, Asset Availability, and Operations Management are independent variables, while Organization Performance is a dependent variable. Note that Information Security Strategy Implementation Success is a dependent variable with reference to the independent variables, and at the same time an independent variable with reference to the dependent variable Organization Performance. The dual role of the Information Security Strategy Implementation Success variable demonstrates the

characteristics of a mediation effect, explaining how and why a relation comes about between an independent variable and a dependent variable or a consequence variable (Baron & Kenny 1986). A mediating effect is created when there is a third variable that intervenes between an independent and dependent variables (Hair et al. 2006). This third variable is referred to as the mediating variable or intervening variable. In the underlying model, the successful implementation of information security strategy is expected to be a mediating variable or mediator that mediates the relationships between organization capabilities and organization performance.

A model with a hypothesized mediating effect can produce direct and indirect effects. A direct effect is defined as the causal influence of one variable on another (Baron & Kenny 1986; Maruyama 1995; Hoyle 1995). Direct effect is graphically represented by a straight one-headed arrow, pointing from cause to effect. An indirect effect is a sequence of two or more direct effects that embody the influence of one variable on another through the presence of one or more mediating variables (Baron & Kenny 1986; Maruyama 1995; Hoyle 1995).

It is possible that successful implementation of information security strategy completely mediates the relations between organizational capabilities and organization performance. However, it is also conceivable that organizational capabilities have effects on an organization's performance through other pathways and not entirely on the effective implementation of information security strategy. Subsequently, a model that represents this competing hypothesis was constructed as shown in Figure 3.3.

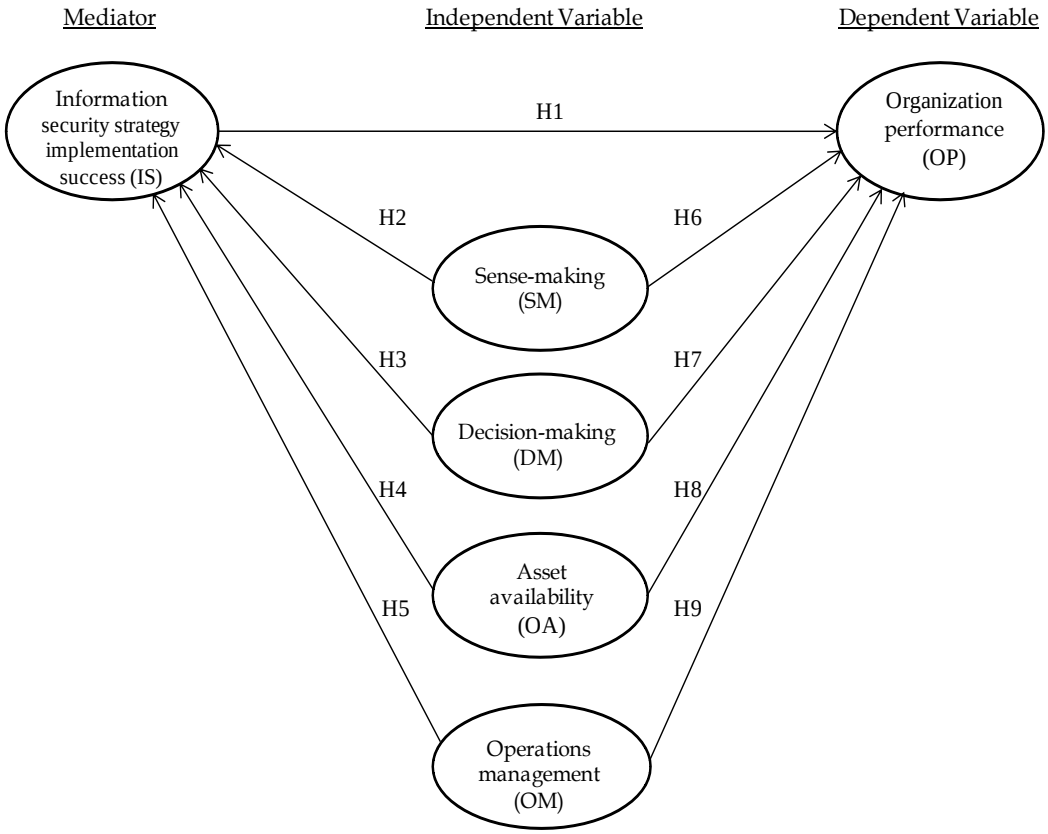


Figure 3.3. Hypothesized Partial Mediation Model

The representation in Figure 3.3 illustrates a hypothesized model with partially mediated relationships. This model suggests that independent variables Sense-making, Decision-making, Asset Availability, and Operations Management also have effects on the dependent variable Organization Performance that are not explained by Information Security Strategy Implementation Success, which represents a mediating variable.

It is necessary to note that each line with a one-headed straight arrow in Figures 3.2 and 3.3 represents a hypothesized direct effect, also termed *path*, of an independent variable on dependent variable. These hypothesized direct effects are represented by paths H1 to H9 and are statistically estimated by path coefficients, also termed regression coefficients. The coefficient represents the amount of change in the dependent variable for a one unit change in the independent variable.

A summary of the hypothesized variables and corresponding variable types (independent, dependent, mediating) is presented in Table 3.1. Other terms, such as exogenous, endogenous and intervening, that are used interchangeably with each of the variable types in this study are also provided in this table. Differences between exogenous and endogenous variables are further explained later in this chapter.

Table 3.1

Mapping of Variables and Variable Types

Variable Type	Other Terms Used	Variable
Independent	Exogenous	Sense-making
		Decision-making
		Asset Availability
		Operations Management
Dependent	Endogenous	Organization Performance
Mediator	Intervening	Information Security Strategy Implementation Success

Survey Instrument Development

Once the path diagram depicting the theoretical model and hypothesized relationships was specified, the next task was to obtain empirical data necessary to validate the theoretical model and estimate the strength of the proposed relationships. In light of a broad review of relevant theoretical literature and existing research in strategic management and information security that revealed the lack of history of previous research related to the present study, the development of an original survey instrument was required. The goal of this survey was to identify the impacts of organizational capabilities in terms of sense-making, decision-making, asset availability, and operations management on

information security strategy and organization performance. Consequently, the content of literature review enabled the researcher to generate questionnaire items for the survey instrument and to develop construct scales. Additional knowledge was garnered by evaluating global and national information security surveys that were publicly available and accessible from various secondary sources.

Pretesting of the Survey

Hair et al. (2006) suggested that pretesting should be performed whether measures are developed for a study or taken from various sources. Subsequently, the researcher submitted the originally developed questionnaire to two survey methodologists for peer and technical reviews to ensure the quality of the questionnaire. As results of feedback and consideration of comments in the reviews, the questionnaire was revised and subsequently pre-tested to ensure quality and effectiveness of the instrument prior to implementing the actual survey procedure. The survey pretest was conducted with a small group of information technology professionals. The pretest was necessary to serve three functions in this study. First, it was to ensure the questionnaire and instructions could be well understood and the response categories were comprehensive (Bourque & Fielder 2003). Second, it was to assess whether any items or item wording may unnecessarily increase the respondent's burden in completing the survey (Bourque & Fielder 2003). Third, the pretest was to study the respondent's cognitive processes including comprehension, recall, decisions and judgment, along with response processes that respondents used to answer survey questions (Willis 2005).

Pretest Participant. Participants of the pretest were selected to include both sets of people who do, as well as those who do not, exhibit the key characteristic of interest that paralleled those of the intended population, i.e., information security professionals. Specifically, of the ten pretest participants, six were information security professionals with various certification backgrounds and job duties. The remaining four participants indicated that although they did not earn any security certification, and their job duties indirectly involved information security, they had a good understanding of information security. Based on self-reporting, each of the six information security professionals indicated possessing at least one security certification and more than 8 years of experience in information technology or information security. In addition, among the participants, four were from government/non-profit organizations, four from information and communication technology (ICT) organizations, one from an education/training institute, and one from a financial/banking service firm. It was also noted that six participants were from organizations with more than 10,000 employees and annual revenues/budgets of more than $100 million. Reports of gender, race and ethnicity were not necessary as such information were not requested on the survey.

Pretest Procedures. The researcher conducted one-on-one pretests with participants using the paper questionnaire during a seven-day campaign. All pretests took place in the participants' offices located in Northern Virginia. Each pretest session comprised of two procedures and took approximately one hour to complete. The first

procedure was a 20-minute session involved an introduction and a self-administered survey. The second procedure consisted of a 40-minute cognitive interview.

To better replicate the actual cognitive conditions of a self-administered mail survey, each pretest participant was provided a sealed envelope including a cover letter and a pretest paper questionnaire. Each participant was orally given a brief overview of the pretest activities. Participants were informed that the pretest was intended to identify any overt and covert problems with the survey as well as assessing the respondent's burden in answering the questions. Additionally, participants were asked to mark the confusing words, items, or questions that were not understandable for later follow-up by placing an "X" in the margin next to the underlying issue.

The researcher then instructed participants to open the envelope and to complete the survey as if they had just received it in the mail. All participants took time to read the cover letter accompanying the questionnaire as expected. Participants were timed as they filled out the survey. Total response times for completing the survey ranged from to 12 minutes 15 seconds to 16 minutes 39 seconds, with an average administration time of 14 minutes 36 seconds. The results demonstrated that the estimated time of 15-20 minutes necessary for the respondent to complete the survey was reasonable.

Upon receiving the respondent's completed survey, the researcher carried out the cognitive interviews using verbal probing, paraphrasing, and think-aloud techniques suggested by Willis (2005). Each participant was invited to report any general thoughts and impressions regarding the survey, before each question was specifically probed. The

researcher used a scripted set of probing questions to focus the respondent on particular aspects of the question-response task. The respondents were asked how they chose among response choices and how they interpreted reference periods. The researcher also used a modified version of the think-aloud technique following completion of the survey. The respondents were instructed to verbalize their thoughts and to highlight any difficulties they had with understanding questions, recalling relevant information, or responding within the intended response categories. In addition, the researcher used the paraphrasing technique to ask the respondents to repeat the question in their own words and what a particular term meant. The respondent's feedback was intended to enable the researcher to learn whether the respondent understood the question and interpreted it in the manner intended, and whether better wordings for questions could be used. Findings, observations and decisions of the pretest interviews are provided in Appendix A. Only relevant issues were reported in this table.

In summary, the cognitive interviews provided the researcher an important means of finding out potential problems concerning the respondent's processing of the survey prior to actual data collection. It allowed the researcher the opportunity to uncover respondents' confusion with the overall meaning of the question or misinterpretation of individual terms or concepts. Additionally, the researcher was able to identify how the respondents processed their thoughts as they answered the questions. Altogether, the pretest findings were useful for making decisions about necessary revisions as well as understanding what the questions were actually measuring for analysis purposes. Results of

the pretest were evaluated and used in refining the questionnaire and the study design. However, none of the pretest survey results was applied in the final study results, analysis, and findings.

Design of Survey Instrument

The final questionnaire, with a total of 50 items, was divided into two sections consisting of information security questions and demographic questions. The first section involved 43 items in three parts -- *Organizational Capabilities, Information Security Strategy,* and *Organization Performance*. This section aimed at identifying the relationships between variables by asking respondents to rate the declarative statements using a five-point Likert-like measurement scale. Each of these statements represented an indicator or independent variable designed to measure the corresponding conceptual constructs. The second section encompassed 7 questions intended to obtain general demographic information of the survey samples. Following this last section was a qualitative box that allowed optional feedback from survey participants. Respondents could use the provided space to share additional thoughts that might not necessarily relate directly to the research inquiry. `

Part A, *Organization Capabilities*, used 5-point Likert-like scales (*No Extent, Little Extent, Some Extent, Moderate Extent, Great Extent*) to solicit information about the extent to which the respondent's organization implemented organizational capabilities in terms of sense-making, decision-making, asset availability, and operations management. Higher scores indicated greater levels of implementation of organizational capabilities. The

questions in this part were further separated into 4 sub-scales representing four organizational capability constructs. The first sub-scale, *Sense-making*, consisting of 6 items (1 through 6), used to measure the organization's capability to develop high quality situational awareness and understanding of the internal and external environments. The second sub-scale, *Decision-making*, consisted of 7 items (7 through 13) aimed at evaluating the organization's capability to collaborate, make, and communicate decisions concerning information security. The third sub-scale, *Competencies*, involved 9 items (14 through 22) designed to assess the organization's capability to possess appropriate means and resources to respond to information security threats. Finally, the fourth sub-scale, *Operations Management*, used 6 items (23 through 28) to determine the extent to which the respondents' organization coordinated and deployed information security assets. Tables 3.2 to 3.5 present the items measures for the organization capability scales.

Table 3.2.

Item Measures of Sense-making (SM)

Item	Description
SM1	Assesses the environmental impacts (i.e., social, political and economical) on information security.
SM2	Uses a systematic process to identify potential adversary actions or reactions.
SM3	Analyzes available information to determine risks to the enterprise.
SM4	Keeps current on the evolving capabilities of attackers and potential attackers.
SM5	Keeps decision makers informed of vital information security developments.
SM6	Provides appropriate security education and awareness on information assets protection.

Table 3.3.

Item Measures of Decision-making (DM)

Item	Description
DM1	Aligns information security objectives with the overall business goals.
DM2	Illustrates clear intention to support information security initiatives.
DM3	Links organizational governance structure to information security governance to provide consistency in planning, implementing, and delivering security in the organization.
DM4	Commits appropriate resources to achieve information security objectives.
DM5	Promotes workforce collaboration to protect business assets from information security attacks.
DM6	Takes measures to build a more competent enterprise that can defend business against increasingly sophisticated information security threats.
DM7	Communicates clear vision to mitigate information security risks.

Table 3.4.

Item Measures of Asset Availability (OA)

Item	Description
OA1	Deploys an integrated combination of competencies and resources to protect information assets. (Competencies refer to knowledge, skill, and ability needed to perform a specific task.)
OA2	Recruits people with appropriate information security competencies.
OA3	Retains a cadre of trained information security professionals.
OA4	Uses formal mechanisms such as training, policies, procedures, processes and technologies to ensure a secure, reliable, responsive, and trusted information technology environment.
OA5	Uses formal mechanisms such as policies, procedures, processes and technologies to enforce information security compliance.
OA6	Implements necessary procedures to ensure effective configuration management of all changes to information related systems.
OA7	Ensures continuity of mission-critical operations through contingency planning.
OA8	Reviews information security policy regularly to ensure its adequacy.
OA9	Provides a balance between security controls and access to information.

Table 3.5.

Item Measures of Operations Management (OM)

Item	Description
OM1	Assigns all security controls needed to protect the mission/business processes to responsible parties with accountability for development, implementation, and assessment.
OM2	Uses project management best practices to manage information security programs.
OM3	Uses metrics to identify the achieved security performance in its operational environment.
OM4	Uses metrics to increase accountability through the collection, analysis, and reporting of relevant performance-related data.
OM5	Uses metrics to facilitate decision making.
OM6	Documents incidents to provide lessons learned that help modify information security strategy.

Part B, *Information Security Strategy*, consisting of 9 items (29 through 37), was used to measure the degree to which an organization's information security programs protected and defended information and information systems against adversary threats. Each item was rated on a 5-point Likert-like scale *(Very Ineffective, Somewhat Ineffective, Neutral, Somewhat Effective, and Very Effective),* in which higher scores indicated greater effective implementation of information security strategy. The item measures for information security strategy are provided in Table 3.6.

Table 3.6.

Item Measures of Information Security Strategy (IS)

Item	Description
IS1	Maintains appropriate protection of information assets.
IS2	Achieves information security compliance with legislation, regulatory or industry requirements.
IS3	Upholds information security policies and standards.
IS4	Responds promptly to information security attacks.
IS5	Recovers quickly following system failure or interruption.
IS6	Keeps information security risks to a minimum.
IS7	Sustains continuity of mission-critical operations.
IS8	Prevents damages to information assets.
IS9	Allows for better control of information assets.

Part C, *Organization Performance*, comprised of 6 items (38 through 43) to solicit information regarding the degree to which the respondent's organization produced and accomplished business objectives and values for the various stakeholders. A 5-point Likert-like scale *(Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree)* was used to rate the participant's responses to the items. Higher scores on this scale reflected greater organization effectiveness. The item measures for organization performance are provided in Table 3.7.

Table 3.7.

Item Measures of Organization Performance (OP)

Item	Description
OP1	Increases customer trust.
OP2	Prevents costly legal action from government agencies, stockholders, or others.
OP3	Preserves public's perception of brand strength or company reputation.
OP4	Improves customer service.
OP5	Preserves market valuation.
OP6	Maintains business resiliency in the face of a constantly changing risk environment

Lastly, the *Demographic Questions* section consisted of 7 questions, 44 through 50, devised to compare the demographic distributions among information security professionals. These questions encompassed respondent's security certifications (question 44), level of involvement in information security (question 45), job function (question 46), and years of experience (question 47), along with organization's industry (question 48), annual revenues (question 49), and number of employees (question 50). Questions 44, 45, 47, and 48 were measured using the nominal scales to describe variables that were categorical or continuous in nature (Salkind, 2009). On the other hand, the interval measurement scales were applied to questions 46, 49 and 50 to describe variables having equal units of measurement between each variable (Salkind, 2009). Table 3.8 provides an

alignment of survey items, measurement scales, and corresponding research questions and hypotheses.

Table 3.8.

Alignment of Research Questions, Hypotheses, Survey Items, and Measurement Scales

Research Question	Hypothesis	Survey Item	Measurement Scale
RQ1. What is the relationship, if any, between information security strategy implementation success and organization performance?	H1: Successful implementation of an overall information security strategy is positively associated with organization performance.	29-43	Ordinal
RQ2. What are the relationships, if any, between organization capabilities and information security strategy implementation success?	H2: Sense-making is positively associated with information security strategy implementation success.	1-6, 29-37	Ordinal
	H3: Decision-making is positively associated with information security strategy implementation success.	7-13, 29-37	Ordinal
	H4: Asset availability is positively associated with information security strategy implementation success.	14-22, 29-37	Ordinal

Research Question	Hypothesis	Survey Item	Measurement Scale
	H5: Operations management is positively associated with information security strategy implementation success.	23-37	Ordinal
RQ3. To what extent do organizational capabilities influence organization performance?	H6: Sense-making and organization performance is partially mediated by information security strategy implementation success.	1-6, 29-44	Ordinal
	H7: Decision-making and organization performance is partially mediated by information security strategy implementation success.	7-13, 29-44	Ordinal
	H8: Asset availability and organization performance is partially mediated by information security strategy implementation success.	14-22, 29-44	Ordinal
	H9: Operations management and organization performance is partially mediated by information security strategy implementation success.	23-44	Ordinal

Data Collection

Research Ethical Assurances

The researcher completed the Human Subject Protections Training (Cititraining) as required prior to performing the proposed study. Additionally, the researcher was motivated to submit the survey instrument, the cover letter, along with an "Exempt From IRB Review Request" to the George Washington University (GWU) Institutional Review Board (IRB). The IRB Review Exemption Form includes the required information describing the proposed research such as research purpose, study population and sample size, subject recruitment methods, research methodology, research risks and benefits, and confidentiality and privacy assurance. Subsequently, the IRB waiver request was approved (see Appendix B).

The researcher conducted the study strictly in accordance with the established ethical standards. Prospective participants were informed of their un-coerced, voluntary consent to participation. Despite a possible risk, though a minor one, caused by loss of time that the respondent used to fill out the questionnaire, there were no anticipated physical risks or psychological issues associated with participating in this study.

Furthermore, the respondent's anonymity and confidentiality were positively assured. In addition to the promise of confidentiality, the researcher also affirmed that no identifiable information such as the respondent's name, address, associated organization, etc… was recorded on the survey form regardless of a tracking number assigned to each questionnaire. These tracking identifiers, which were designed to keep participants'

responses anonymous, were handled solely and responsively by the researcher, along with other data respondents may have provided. Appropriate security measures were taken to prevent data loss, unauthorized access, or divulgence of private information. The results of all returned surveys was reported in an aggregated form without identifying the respondent or associated organization should the study be published as a doctoral dissertation or in academic journals or trade publications.

Research Participants

The intended survey population consisted of Certified Information System Security Professionals (CISSPs) who may have a strong background and years of experience in information technology and information security. A collection of sampling units selected for this study was identified primarily from the International Information Systems Security Certification Consortium (ISC)². The (ISC)² is a non-profit global organization headquarters in the United States with various offices in London, Hong Kong and Tokyo. It is recognized as a leading institute in educating and certifying information security professionals in more than 135 countries ((ISC)^2 2010). Those successfully completing the competency requirements earn the CISSP designation, or other security credentials such as Certified Secure Software Life Cycle Professional (CSSLP), Certification and Accreditation Professional (CAP), and Systems Security Certified Practitioner (SSCP) ((ISC)^2 2010). The name and contact information of targeted samples were selected at random and compiled from the (ISC)² member directory that was publicly available on the (ISC)² Website. Only (ISC) ² respondents who resided within the United States and the

District of Columbia were included in the sample compilation. Upon completing the research, this data set would be purged from all of the researcher's related databases. To ensure the adequacy of statistical test results, researchers suggested that a sample size of 200 or greater is reasonable when using the Structural Equation Modeling (SEM) analysis to analyze models (Kline 2005; Hoe 2008), such as those in this study. Rules of thumb found in literature are that the sample size can be as few as 5 subjects per variable or as high as 20 times the number of variables in the model (Bentler and Chou 1987; Mitchell 1993; Schumacker & Lomax 2004). For this study of 43 proposed variables, a sample size of 215 or greater is adequate for the intended data analysis procedure.

The Instrument Mailing Package

A survey instrument package was prepared for mailing to each of the targeted respondents. Each package consists of a cover letter, postage-paid return envelope, a questionnaire, along with incentive tokens. Dillman et al. (2009) asserted that if an incentive is used to encourage participation, it is important to emphasize that it is offered as "a small token of appreciation" to establish trust and respect for respondents.

The main section of the 1-page cover letter (see Appendix C) encompassed two objectives. First, the letter served as an invitation soliciting information security professionals to participate in the underlying survey. Second, it functioned as an instructional guide that communicated in an effective manner certain critical information concerning the research to potential respondents. The combined invitational-instructional cover letter conveyed to possible respondents the purpose of the survey, how the

respondent was selected and why the respondent was important to the study, what the respondent was being asked to do and the estimated completion time, plus the researcher's statement of confidentiality assurance, phone numbers and contacts to call with questions. The second item was a pre-addressed stamped return envelope. Each of these envelopes was affixed with a label consisting of the researcher's name and address along with a unique tracking identifier linked to a specific participant for tracking purposes. Despite this tracking number, the respondent's contact information and any corresponding responses and comments would be treated with utmost confidentiality. The last physical item included in the package was the final survey instrument of 50 self-administered questionnaire items (see Appendix D). Taken together, these materials were placed in a large envelope to be mailed to the intended subject. The participant's name and address, coupled with a tracking number identical to that on the return envelope, were generated on a mailing label and affixed to this large envelope.

In appreciation of participants' time and effort responding to the survey, two incentives were offered. In part, the note section of the cover letter indicated that one dollar ($1) would be donated to the American Red Cross for each completed survey, and respondents would be entered into a drawing for a $50 VISA Gift Card. Additionally, a statement was incorporated in the questionnaire immediately following the demographic section signifying that the published survey results would be made available to respondents upon request.

Survey Implementation Procedure

The primary data collection method in this study was the self-administered mail survey developed and tested by the researcher. A paper questionnaire package was mailed to each targeted respondent to collect data required for the validation and testing of the conceptual model and the research hypotheses. When the required sample size was not achieved after 3 months and 1000 paper surveys distributed, the researcher attempted an alternative data collection method using emailed surveys. If successful, the email survey method would reduce the researcher's survey costs significantly. An electronic survey package, consisting of a cover letter and a questionnaire in electronic format that are equivalent to those in the paper form, was sent as an email attachment to additional targeted respondents randomly selected from the (ISC) ² sample frame. Participants had the options of completing the questionnaire and returning the responses electronically, or printing out the questionnaire, completing it on paper, then mailing or faxing the responses to the researcher. Of the 315 CISSP recipients of the electronic questionnaires, 11 returned completed responses in email attachments. The resulting response rate was less than 4%. As a consequence of the low response rate, the electronic survey procedure was aborted and all email responses were discarded. The data collection campaign using the postal-mail survey method resumed for 2 more months and paper surveys were further distributed to 619 additional CISSP respondents. Follow-up reminders were also sent to ensure higher response rates. At the end of the 5th month, the number of responses received by the researcher exceeded the required minimum sample size, enabling the conclusion of the data

collection campaign. In all, the mail survey administration resulted in a distribution of 1619 paper questionnaire packages, of which 433 sample responses were received.

Data Analysis

Data collected using the mail surveys was entered into the Predictive Analytics Software (PASW) Statistics 18 Graduate Pack. This application enabled the researcher to obtain descriptive information for the samples and to perform reliability coefficient analysis for all variables. The Analysis of Moment Structures (AMOS) 18, a PASW extension, was also used to conduct the structural equation modeling analysis of the surveyed data in this study.

Structural Equation Modeling (SEM) Approach

Structural equation modeling is not a single statistical technique. Rather SEM refers to a comprehensive data-analytic tool that combines elements of the first generation multivariate techniques such as multiple regression analysis, factor analysis, and path analysis (Kline 2005; Hershberger et al. 2003). It is thus considered the second generation of the multivariate analysis (Fornell, 1987). Other terms used interchangeably are covariance structure analysis, covariance structure modeling, or analysis of covariance structures as SEM uses a variance-covariance matrix among observed variables to estimate latent variables (Kline 2005; Valluzzi et al. 2003; Schumacker & Lomax 2004). SEM has evolved over the years into a methodological framework that allows researchers across disciplines to address a set of interconnected research questions in a single,

methodical, and comprehensive analysis by quantitatively testing the hypothesized relationships among latent and observed variables (Hancock & Miller 2006; Schumacker & Lomax 2004; Gefen et al. 2000). SEM is considered a confirmatory analysis, meaning it is useful for testing and potentially confirming theory (Hair et al. 2006). As such, SEM necessitates the development of a theoretical model that specifies not only the number of constructs involved, but also the expected relationships among those constructs prior to analysis.

Basic Concepts of Structural Equation Modeling

Latent Versus Observed Variables. Researchers are often interested in studying theoretical phenomena that are not measured directly. In SEM, these theoretical concepts are termed constructs, unobserved variables, latent variables, or factors. Latent variables are hypothetical variables that are not directly measured or observable, but are inferred from a set of observed variables. For example, the ability to develop high quality situational awareness or sense-making is a latent variable that represents an organizational capability construct. The successful implementation of information security strategy is another latent variable, representing the information security strategy construct. Unlike latent variables, observed variables are variables that can be measured by using means such as tests in an experiment or items in a survey instrument. Observed variables are often referred to as indicators, manifest or measured variables. For example, questionnaire items 1-6 in this research survey are indicators used to define the construct of sense-making.

Exogenous Versus Endogenous Latent Variables. In working with SEM models, it is helpful to distinguish between latent variables that are exogenous and those that are endogenous variables. Exogenous variables are synonymous with independent variables whereas endogenous variables are dependent variables. Exogenous latent variables are those that predict other latent variables. In contrast, endogenous variables are dependent variables that are predicted by other latent variables in the model. The causes of exogenous latent variables are unknown and thus not illustrated in the models, while endogenous latent variables have expected causes that are explicitly represented in the models. Moreover, a predicted variable is endogenous even if it sequentially predicts another variable. For example, this study hypothesizes that sense-making, decision-making, asset availability, and operations management (exogenous latent variables) influence information security strategy implementation successful (endogenous latent variable), which in turn leads to higher organization performance (endogenous latent variable).

Measurement Errors. In addition to the direct effects between latent variables, the direct effects of the factors on the observed variables are also represented in the model. Furthermore, each observed variable also has another direct effect caused by all other unique sources represented by the measurement error term. These unique sources of variance represent random error or unreliability and all sources of systematic variance not due to factors (Kline 2005). The observed variable measurement error is defined as the portion of the observed variable score that is measuring something other than what the latent is hypothesized to measure (Schumacker & Lomax 2004).

Residual Errors. Unlike measurement error terms that represent errors associated with unobserved variables, residual terms represent errors in the prediction of endogenous latent variables from exogenous latent variables (Byrne 2001). In other word, the residuals indicate the differences between the observed and predicted values of the dependent variable.

The Path Diagram. A path diagram is often used to visually portray the hypothetical model. By convention, latent variables are depicted as ellipses or circles, and observed variables are represented by rectangles. The impact of one variable on another is illustrated by one-headed straight arrows, pointing from the cause to the subsequent effect. The covariances or correlations between pairs of variables are depicted by curved doubled-headed arrows. Measurement and residual error terms are in essence unobserved variables, and thus represented by small circles or ellipses. A summary of the general path notation is provided in Appendix E.

Strengths of Structural Equation Modeling

There are a number of prominent strengths that play fundamental roles in the increasing popularity of SEM among researchers and scientists as commonly discussed in the literature (Tomarken & Waller 2005; Kline 2005; Schumacker & Lomax 2004; Hershberger et al. 2003; Gefen et al. 2000; Maruyama 1998). In part, an important feature is the ability to incorporate and integrate factor analysis of latent variables and structure analysis of paths connecting the latent variables. Factor analysis is designed to link observed measures to a smaller number of underlying conceptual constructs (Maruyama

1998). It allows the use of multiple measured variables to better understand a wide range of theoretical constructs or areas of scientific inquiry represented by latent variables. Structural analysis maps paths between latent variables and analyzes all the paths simultaneously in one operation. The combined analysis enables not only the measurement errors of the observed variables to be represented and analyzed as an integral part of the structural model, but also factor analysis to be performed concurrently with the hypothesis testing rather than one at a time. Another commonly acknowledged strength is the accessibility of the model fit measures that permits rigorous analysis of complex hypothetical interactions that may involve a large number of equations, and provides statistics evaluation at both the individual path and construct level and the overall model level. Additionally, Tomarken & Waller (2005) emphasized that SEM allows researchers to test the hypothetical model in question directly. This is done by aligning the investigator's proposed concept with the null hypothesis rather than the alternative hypothesis as traditionally used in the non-SEM statistical applications. For this reason, researchers are generally interested in not rejecting the null hypothesis when using SEM techniques to conduct statistical analyses of their studies (Hersherberger et al. 2003).

Limitations of Structural Equation Modeling

Although the technique of SEM is a broad and flexible analytical tool, it is not without limitations as in any other statistical methods. Potential issues that are deemed most relevant to this study relate to sample sizes, model specification, and model fit indices.

Most importantly, sample size has always been a major concern in the application of SEM. It is generally understood among statisticians that SEM requires large sample sizes to maintain the power of statistical tests and to obtain reliable covariance and correlation estimates (Kline 2005; Schumacker & Lomax 2004). However, there is little consensus on how large the sample needs to be. With this reality in mind, a critical sample size in the 200 range was offered as a benchmark (Tomarken & Waller 2005; Kline 2005; Garver & Mentzer 1999; Chou & Bentler 1995; Hoelter 1983). Subsequently, Hoe (2008) concluded that, as a rule of thumb, a sample size of at least 200 provides sufficient statistical power to estimate parameters and to determine satisfactory model fit. Another rule of thumb that takes into account the relations between sample size and path model complexity is to have the sample size of at least 10 times the number of parameters to be estimated in the model (Kline 2005). Additionally, Bentler and Chou (1987) suggested a ratio of 5 to 10 cases per latent variable would be sufficient. Conversely, Kline (2005) warned that the statistical accuracy may be questionable if the cases/parameters ratio is less than 5:1.

Further, the techniques of SEM is a confirmatory approach, thus it requires the specification of the research model prior to analysis, which consumes the most time and effort of the researcher (Kline 2005; Schumacker & Lomax 2004). The researcher must therefore ensure the theoretical model has the basis that reflects established theory, previous research results, or even an educated guess based on the researcher's insights and experience about the hypothesized relationships prior to data collection (Kline 2005).

Finally, another issue that continues to challenge SEM users is the conflicting guidance on what fit indices to report and what acceptable cut-off values to use (Hu & Bentler 1999). Traditionally, the Chi-Square goodness-of-fit test is the fundamental measure used to evaluate the ability of a model to reproduce the observed data. The difference between sample correlations and implied population correlations by the model is used to calculate a Chi-Square value. A small difference will result in a non-significant Chi-Square value, indicating a fit between the theoretical model and the sample data. On the other hand, if the model is not supported by the empirical data, the difference between the correlations will be large, reflecting a significant Chi-Square value. In general, researchers are interested in obtaining a non-significant Chi-Square at a 0.05 threshold relative to the degrees of freedom (Schumacker & Lomax 2004; Hooper et al. 2008). However, there are significant concerns about using the Chi-Square test because its probability is sensitive to sample size. That is, the model will almost always be rejected when the sample size is large enough (more than 200), while it is difficult to reject the model with small samples (Marsh et al. 1988; Maruyama 1998; Schumacker & Lomax 2004; Kline 2005; Reinard 2006). Moreover, Chi-Square is also affected by the size of correlations: the higher the correlations, the higher the Chi-square. Thus, the model tends to be rejected if the correlations in the model are large (Kline 2005).

SEM Analysis Procedures

The hypotheses proposed in this study were tested against empirical data using a two-step SEM process suggested by Anderson & Gerbing (1988). This process

encompasses an assessment of the confirmatory measurement models and an assessment of the confirmatory structural model.

Assessment of Confirmatory Measurement Model

The first step involves using confirmatory factor analysis (CFA) to validate the hypothesized measurement models that embody the relations of observed variables to the underlying constructs or latent variables in a theoretical model. CFA is theory driven, meaning the researcher must specify *a priori* the factors that exist among a set of measured items and the relations between the factors and corresponding indicators, which together represent the researcher's measurement theory (Hair et al. 2006). The CFA technique is then used to provide a confirmatory test of how well observed variables represent a smaller number of constructs, and how well measured variables represent constructs that are not measured directly. Multiple criteria including unidimensionality, internal reliability, convergent and discriminant validity are used to assess the strengths of measurement between the item indicators and associated constructs. A model that does not pass these criteria may need to be modified or the theory base will need to be reassessed.

Unidimensionality. The ability of a set of measured variables to measure one and only one construct is referred to as unidimensionality (Anderson & Gerbing 1988). A factor loading matrix is computed and assessed whether each measured item loads with a high coefficient on one and only one hypothesized factor as intended (Gefen 2003). In general, a loading coefficient above 0.60 is considered high, and below 0.40 is low (Gefen and Straub 2005). Further, when sample sizes of 200 or greater are used, factor

loadings of 0.40 or above are required for significance at the 0.05 level (Hair et al. 2006). Eigenvalues exceeding 1.0 are used to determine the factor solutions (Gefen and Straub 2005). Furthermore, the presence of cross-loadings indicates a unidimensionality issue. Thus, items with low or cross loadings are candidates for deletion (Hair et al. 2006).

Reliability. In general terms, reliability is an assessment of the degree of internal consistency between multiple measurements of a variable (Hair et al., 2006). A reliability coefficient called the Cronbach's alpha (α) is the most widely used statistical tool to identify the extent to which a construct is reliable. The general rule of thumb is that a Cronbach's alpha between 0.7 and 0.8 suggests fair reliability (Hair et al., 2006). High values of coefficient alpha, e.g. 0.8 or higher, indicate internal reliability reflecting that all questionnaire items of the same construct consistently measure the same concept or area of interest (Cronbach 1951; Reinard 2006). Additionally, the scale reliability can also be ensured by examining the means, variances and correlations of items that make up the scale. Good items require (a) large variances, (b) expected values near the middle, (c) all item correlations should be positive and have the same magnitude, and (d) all items should correlate with the sum of the rest (Blunch 2008).

Convergent Validity. The degree to which indicators of a specific construct converge or share a high proportion of variance in common in comparison to items measuring other constructs (Urbach & Ahlemann 2010). In SEM, item loading estimates that are significant at $p < 0.05$ with t-tests > 1.96 provide a useful start in assessing relations between the items and their corresponding constructs (Anderson & Gerbing 1988).

Another approach involves the examination of the average variance extracted (AVE) for each construct proposed by Fornell and Larcker (1981). In general, an AVE value of at least 0.50 indicates the ability of a latent variable to explain more than half of the variance of its indicators.

Discriminant Validity. While convergent validity evaluates the relations of the questionnaire items to the underlying constructs, discriminate validity assesses the extent to which a construct is truly distinct from other constructs (Warner 2008). A common approach to appraising discriminant validity is using the criterion proposed by Fornell & Larcker (1981). The Fornell & Larcker criterion requires that a latent construct explains its indicators more than it explains other constructs. This is accomplished by ensuring the AVE of each construct is greater than the construct's highest squared correlation with any other construct (Urbach & Ahlemann 2010). Passing this test provides evidence of discriminant validity.

Assessment of Confirmatory Structural Model

Once the measurement models in the first step are successfully validated, the second step can begin that consists of the structural model specification and analysis. Structural model specification is accomplished by assigning relationships from one latent variable to another based on the research hypotheses. A path diagram is used to depict the structural model by extending the proposed structural paths among the latent variables of the measurement models. The structural model structure analysis focuses on estimating the hypothesized relationships between latent variables and to fit the structural model. The

hypothesized relationships are statistically estimated by the magnitude of path coefficients specifying the strength of the relationships between latent variables. Research suggests that path coefficients should exceed 0.10 at the significance level of 0.05 to account for a certain impact within the model (Urbach & Ahlemann 2010). Finally, hypothesis testing may be completed by conducting statistical tests of the fit between the theoretical structural model and the collected data using various model fit statistics described below. Using SEM techniques, researchers are not interested in statistically significant differences. Rejecting the theoretical model would mean rejection of the hypothesis.

Model fit provides a global examination of the degree to which the theoretical model fits the observed data. Researchers have sought alternative model fit indices to avoid the problems linked to the conventional Chi-Square test. However, given the abundance of fit statistics available in SEM, researchers can become overwhelmed and may have difficulty choosing among them (Tanaka 1993; Hooper et al. 2008).

Consequently, it has been suggested that researchers choose fit statistics based on their personal preferences (Schreiber 2008). Based on prior research guidelines and the state of practice, it is sensible to report the Chi-Square statistic along with its associated degree of freedom (*df*) and p value, the χ^2/df ratio, the root mean square errors of approximation (RMSEA) and associated confidence interval, the standardized root mean square residual (SRMR), the comparative fit index (CFI), and the Tucker-Lewis index (TLI).

Model Chi-Square (χ^2): The Chi-Square goodness-of-fit test is also known as the likelihood ratio chi-square or generalized likelihood ratio. It is the most common fit index for evaluating the degree of discrepancy between the variance-covariance matrix implied by the hypothetical model and that from the observed data (Hu & Bentler 1999; Maruyama 1998; Hoyle 1995). Goodness-of-fit tests provide the researcher the basis to determine whether the hypothetical model being tested should be rejected or accepted. A model would be accepted if it yields a non-significant Chi-Square at the 0.05 threshold level (Schumacker & Lomax 2004; Hooper et al. 2008). As previously discussed, concerns about the validity of the Chi- Square as an index of fit have generated considerable debate among SEM scholars (Hoyle 1995). Consequently, Schreiber (2008) suggested researchers report the Chi-Square value along with the associated degrees of freedom and p-level; however, these statistics should not be used to justify the fit between the theoretical model and the data due to the limitations noted above.

Relative Chi-Square (χ^2/df): The ratio of Chi-Square and degrees of freedom was recommended to supplement the Chi-Square statistic (Marsh et al. 1988; Maruyama 1998; Kline 2005). The χ^2/df ratio, also couched normal or normed Chi-Square, is an attempt to adjust the impact of sample size on the Chi-Square statistic (Schumacker & Lomax 2004; Kline 2005). A value of less than 5 is indicative of a tenable model fit (Wheaton et al. 1977; Bollen 1989; Schumacker & Lomax 2004; Kline 2005).

RMSEA: The Root Mean Square Errors of Approximation (RMSEA) was originally introduced by Steiger and Lind (1980, cited in Steiger 1998) and advanced by

Brown and Cudeck (1993). The RMSEA is a parsimony-adjusted index in which its formula accounts for the model complexity (Kline 2005). This statistic measures the error of approximation, which concerns the ability of the hypothetical model to produce the population covariance matrix (Brown & Cudeck 1993). The RMSEA is one of the most commonly used fit statistics (McDonald & Ho 2002). One of the key features of the RMSEA is that it allows for the determination of the confidence intervals to augment the point estimates (MacCallum et al. 1996). Confidence intervals provide more information regarding model fit as opposed to using simply the population parameter estimated by the RMSEA (Chen et al. 2008b). Of late, the general consensus among authorities is that an RMSEA value between 0.06 and 0.08 and a confidence interval range from 0.00 and 0.08 indicate a good fitting model (Kline 2005; Schreiber, J.B. et al. 2006; Schreiber 2008).

SRMR: The Standardized Root Mean Square Residual (SRMR) is a measure of the mean absolute covariance residuals, reflecting the average standardized differences between the observed and predicted covariances (Kline 2005). Ideally, the residuals should be about zero if there is a perfect model fit. Thus, the smaller the SMRR, the better the model fit. A value of the SMRR less than 0.05 indicates a well-fitting model (Byrne 2001), less than 0.08 is widely considered a good fit (Hu & Bentler 1999.

CFI: The Comparative Fit Index (CFI), also known as the Bentler (1990) Comparative Fit Index, is one of the most widely used fit indexes due in part to its insensitivity to model complexity (Fan et al. 1999; Hair et al. 2006). The CFI assesses the improvement in fit of the researcher's model compared to an independence or null model

which assumes all observed and hence latent variables in the model are unrelated (Kline 2005). Generally, CFI varies from 0 to 1. However, values of the CFI greater than or equal to 0.95 have been recommended as indicative of good fit (Hu & Bentler 1999).

TLI: The Tucker-Lewis Index (TLI), also known as non-normed fit index, was first developed for factor analysis but was extended to SEM (Schumacker & Lomax 2004). Similar to CFI, TLI is used to compare a specified model against a null model. The TLI is not normed, thus its values can fall below 0 or above 1. Typically, values of TLI close to 1 indicate good fit. Hu & Bentler (1999) have suggested values of TLI greater than or equal to 0.95 as the threshold.

A summary of the acceptable cutoff values of the unidimensionality, reliability and validity measures, along with the acceptable thresholds of the fit indexes applied in this study are presented in Table 3.9.

Table 3.9.

Acceptable Thresholds of Reliability, Validity and Model Fit Tests

Test	Acceptable Cutoff Value
Unidimensionality	
Item Loading	> 0.4
Eigenvalue	≥ 1
Reliability	
Cronbach's Alpha	≥ 0.7
Convergent Validity	
Standardized Estimate	Significant at $p < 0.05$ with t-tests > 1.96
AVE	≥ 0.5
Discriminant Validity	
AVE	≥ highest squared correlation with other constructs
Model Fit	
Relative Chi-Square	≤ 5
RMSEA	Between 0.06 and 0.08
SMRR	≤ 0.08
CFI	≥ 0.95
TLI	≥ 0.95

Summary

This chapter described the research methodology that was applied to address the research questions.

In part, this chapter illustrated the building of the theoretical model used to test the hypothesized relationships among organizational capabilities, information security strategy implementation success and organization performance. The model was influenced by existing theories and the researcher's creativity and insight in strategic management and information security.

The literature review necessitated the development of an original survey instrument to collect empirical data for validating the research hypothesis. Consequently, this chapter explained the design and construction of the survey instrument in detail. Pretesting of the survey instrument was conducted that allowed the researcher to receive empirical feedback from a small controlled sample. The pretest results were incorporated to refine the final questionnaire.

Next, the data collection procedures using the survey instrument at hand were presented. A survey instrument package that consists of a cover letter, a four-page questionnaire and a pre-addressed stamped envelope was prepared and mailed to each of the targeted respondents. The researcher's ethical assurance was also described.

Finally, this chapter discussed the data analysis methods based on SEM techniques, in which a two-step SEM process suggested by Anderson & Gerbing (1988) was used to test the hypothesized structural model against the empirical data.

Chapter 4 - Results

This chapter documents the quantitative results of the survey data collected for this study. It consists of two principal sections. The first section focuses on the characteristics of the responses to the Survey of Organizational Capabilities Affecting Information Security Effectiveness. The dissertation research survey was administered in early summer 2010 to the randomly selected sample units consisting of those attaining the Certified Information System Security Professionals (CISSPs) certification. The second section discusses the results of the SEM analysis of the collected data as it pertains to the research questions. This section consists of statistical evaluations of the confirmatory measurement models and structural model. Following are the sections that present the findings resulting from the analysis of empirical data.

Characteristics of The Sample

Of the 1,619 paper surveys, the researcher received 433 responses from interested participants, of which 5 were dropped due to incomplete data. The paper survey method resulted in 428 usable responses, demonstrating a reasonable sample size required for the data analysis method employed in this study. The sample responses were received from participants residing in 48 States and the District of Columbia, with at least one survey received from each responding state, resulting in a response rate of 26.75%. In terms of information security qualifications, 99.1% of the usable samples were from respondents possessing one or more security certifications, of which 96.7% specified the CISSP. Regarding job duties, 85.5% of respondents were directly involved in information security, 13.3% were indirectly involved, and 1.2% were not involved at all. Furthermore, 84.8% of

respondents identified themselves as having more than 8 years of experience in information technology/information security. With respect to the organization's size, 54.7% of respondents were from companies with 5,000 or more employees. Additionally, the revenues profile of the usable responses also biased toward larger organizations with 56.3% having annual revenues of over $100 million. Moreover, the survey participants were well representative of firms across different industry types/sectors. These include government/non-profit (116), information communications and technology (ICT) (94), insurance, financial, banking (76), healthcare, medical, pharmaceuticals (28), education/ training (20), retail/wholesale (18), manufacturing/industrial (15), engineering (14), utilities (12), and other (35). Tables 4.1 to 4.8 present the demographic data of the responses in this study relating to geographic location, information security qualification, levels of involvement in information security, job function, and years of experience, along with organization's industry, revenues, and number of employees.

Table 4.1.

Responses by State

States	Counts	Percent	States	Counts	Percent
Alaska	3	0.70%	Montana	2	0.47%
Arizona	28	6.54%	Nebraska	2	0.47%
Arkansas	6	1.40%	Nevada	7	1.64%
California	19	4.44%	New Hampshire	4	0.93%
Colorado	18	4.21%	New Jersey	12	2.80%
Connecticut	2	0.47%	New Mexico	2	0.47%
Delaware	3	0.70%	New York	15	3.50%
District of Columbia	4	0.93%	North Carolina	4	0.93%
Florida	16	3.74%	Ohio	14	3.27%
Georgia	22	5.14%	Oklahoma	2	0.47%
Hawaii	6	1.40%	Oregon	4	0.93%
Idaho	4	0.93%	Pennsylvania	3	0.70%
Illinois	15	3.50%	Rhode Island	2	0.47%
Indiana	6	1.40%	South Carolina	11	2.57%
Iowa	4	0.93%	South Dakota	4	0.93%
Kentucky	8	1.87%	Texas	12	2.80%
Louisiana	2	0.47%	Utah	1	0.23%
Maine	2	0.47%	Virginia	37	8.64%
Maryland	28	6.54%	Washington	5	1.17%
Massachusetts	8	1.87%	West Virginia	4	0.93%
Michigan	18	4.21%	Wisconsin	7	1.64%
Minnesota	12	2.80%	Wyoming	1	0.23%
Mississippi	1	0.23%			
Sub-Total	254	59.35%	Sub-Total	174	40.65%
			Total	428	100.00%

Table 4.2.

Security Certification

Certification	Count	Percent
CISSP	414	96.73%
CAP	1	0.23%
CISA	3	0.70%
SSCP	2	0.47%
Other*	4	0.93%
None	4	0.93%
Total	428	100.00%

Note: *CISSP - Certified Information Systems Security Professional, CAP - Certification and Accreditation Professional, CISA – Certified Information Systems Auditor, SSCP - Systems Security Certified Practitioner.*

* These individuals may have one or more security certifications other than listed in this table. Examples include: Certified Ethical Hacker (CEH), Certified Information Privacy Professional (CIPP), Certified Information Security Manager (CISM), Information Systems *Security* Engineering Professional (ISSEP), etc.

Table 4.3.

Level of Involvement in Information Security

Involvement	Count	Percent
Directly involve	366	85.50%
Indirectly involve	57	13.30%
Do not involve at all	5	1.20%
Total	428	100.00%

Table 4.4.

Years of Experience

Number of Years	Count	Percent
Less 5-8 years	7	1.60%
Between 5-8 years	58	13.60%
Between 8-15 years	159	37.10%
More than 15 years	204	47.70%
Total	428	100.00%

Table 4.5.

Job Function

Job Function	Count	Percent
Architecture and Engineering	34	7.94%
Budget, Finance or Accounting	1	0.23%
Information Technology/Information Security	317	74.07%
Management /Strategic Planning	27	6.31%
Operations or Production	7	1.64%
Sales and Marketing	14	3.27%
Other	28	6.54%
Total	428	100.00%

Table 4.6.

Organization Industry

Industry	Count	Percent
Aerospace/ Engineering	14	3.27%
Agriculture/Chemicals	2	0.47%
Consumer Products/Retail/Wholesale/Distributor	18	4.21%
Education/Training	20	4.67%
Energy/Utilities	12	2.80%
Government/Non-profit	116	27.10%
Healthcare/Medical/Pharmaceuticals	28	6.54%
Information, Communications and Technology	94	21.96%
Insurance/Financial/Banking Services	76	17.76%
Manufacturing/Industrial	15	3.50%
Oil/Gas/Consumable Fuels	2	0.47%
Other	31	7.24%
Total	428	100.00%

Table 4.7.

Organization Size

Number of Employees	Count	Percent
15,000 or more	169	39.49%
10,000 - 14,999	32	7.48%
5,000 - 9,999	33	7.71%
1,000 - 4,999	87	20.33%
500 - 999	26	6.07%
100 - 499	46	10.75%
Less than 100	35	8.18%
Total	428	100.00%

Table 4.8.

Organization Revenues

Annual Revenues	Count	Percent
$1 billion or more	170	39.72%
$500 million - $999.99 million	35	8.18%
$100 million - $499.99 million	36	8.41%
$50 million - $99.99 million	27	6.31%
$10 million - $49.99 million	26	6.07%
$5 million - $9.99 million	14	3.27%
$1 million - $4.99 million	18	4.21%
Less than $1 million	10	2.34%
Don't know	92	21.50%
Total	428	100.00%

Data Screening

As with other statistical techniques, data should be carefully examined to ensure necessary distributional assumptions are reasonable and remedies for potential problems are identified prior to SEM analysis. Analyses based on datasets that seriously violate assumptions or contain errors, inconsistencies in responses or measurements can yield misleading results (Warner 2008). Consequently, the data file was proofread and compared with the data sources to ensure errors and inconsistencies in responses are identified and corrected as appropriate. Next, several data screening measures suggested by Kline (2005) were assessed that include sample size, measurement scale, missing values, and multivariate normality.

In SEM applications, large sample sizes are required to maintain the power of statistical tests and to obtain reliable covariance and correlation estimates (Kline 2005; Schumacker & Lomax 2004). However, there is little consensus on how large the sample needs to be. As a result, a critical sample size in the 200 range was offered as a benchmark (Tomarken & Waller 2005; Kline 2005; Garver & Mentzer 1999; Chou & Bentler 1995; Hoelter 1983). Another rule of thumb suggested that a ratio of 5 to 10 cases per latent variable would be sufficient (Bentler and Chou 1987). Hence, this dataset of 428 observations is more than sufficient in comparison to these benchmarks.

The classic levels of measurement or measurement scales for variables defined by Stevens (1946) include nominal, ordinal, interval and ratio. It has been indicated that all four types of variables can be used in SEM (Schumacker & Lomax 2004). Thus, the

present dataset consisting of ordinal variables based on 5-point Likert scales is appropriate for SEM analysis in this study.

There were 5 responses with extensive missing values. Consequently, the respective responses were dropped as previously indicated. Since the dataset sample is relatively large, the dropped data represent an insignificant percentage of the total sample and thus, should be of little concern (Kline 2005).

The most common estimation method for SEMs is maximum likelihood (ML) estimation. A key assumption for this method is multivariate normality for the exogenous variables. Even though it is not sufficient to conclude multivariate normality, it has been suggested that evidence of univariate distributions that have skew and kurtosis within reasonable ranges are sufficient to satisfy the multivariate normality assumption (Hair et al. 2006; Kline 2005). Different rules of thumb have been given based on various computer simulation studies for SEM models. However, Kline states that variables with absolute values of standardized skew index greater than 3.0 indicate extreme skewness and values of standardized kurtosis index greater than 10 indicate extreme kurtosis. Although the dataset demonstrated acceptable univariate kurtosis values, some variables in the dataset indicated extreme univariate skewness as shown in Appendix F.

Hence, multivariate nonnormality was determined based on the established thresholds. The course of action was to use the bootstrap method, a solution recommended by Schumaker & Lomax (2004), which is available in SEM to remedy the

multivariate nonnormality problem. Bootstrapping is a statistical resampling procedure that takes a random sample of the dataset as a substitute for the population and resamples from it a specified number of times to generate sample bootstrap estimates and associated standard errors. It was identified as a useful technique in determining robustness under assumptions of multivariate normality.

Confirmatory Measurement Model

This study examined the relations between six hypothesized constructs defined as Sense-making (SM), Decision-making (DM), Asset Availability (OA), Operations Management (OM), Information Security Strategy Implementation Success (IS), and Organization Performance (OP). Before the constructs were subject to confirmatory factor analysis, a factor loading matrix was estimated to define the factor structure. Factor loadings for each observed variable were examined to identify the correlation of that variable to the underlying construct (Hair et al. 2006). In confirmatory factor analysis, the constructs, known as latent variables or factors, are unobserved variables and are inferred by the respective questionnaire items, also termed observed variables. Principle axis factoring with varimax rotation method was conducted using PAWS Statistics 18 to compute the factor loading matrix. Factor rotation assists in the interpretation of the factors by transforming a set of observed variables into fewer uncorrelated latent variables where each represents a dimension in the data (Blunch 2008). This is accomplished through maximizing the significant loadings of variables on a single factor (Hair et al. 2006). Given the sample size of 428 in this study, items with significant cross

loadings or loadings below the general cut-off value of 0.40 were removed. The varimax-rotated factor matrix is shown in Table 4.9. As seen in this table, all items demonstrated higher loadings with their corresponding factors, with the exception of items SM1, OA6, OA7, OA8, OA9 and OM1 where loadings fell below the cutoff criterion. Thus the course of action was to remove these variables from subsequent analyses, leaving 37 variables in the analysis.

The Eigenvalues were also examined to ensure whether each of the factors account for the variance of at least one variable (Hair et al. 2006). Table 4.10 contains the information regarding the six proposed factors and their relative explanatory power as expressed by corresponding eigenvalues. The first unrotated factor accounted for more than 68% which is a large share of the total variance in the data. Additionally, after the rotation, each of the factors had an eigenvalue above 1.0, and the six factor structure represented 63.29 % of the total variance explained. These values were above the cutoff values, e.g., 1.0 for eigenvalue and 60% or higher for the total variance, recommended by Hair et al. (2006).

Combining all of the above criteria together supports the conclusion of unidimensionality. Hence the six factor solution is appropriate for further analysis in this study. Consequently, a distinct measurement model was defined for each of the six latent variables that include: 5-item sense-making, 7-item decision-making, 5-item asset availability, 5-item operations management, 9-item information security strategy implementation success, and 6-item organization performance.

Table 4.9.

Varimax Rotated Factor Loading Matrix

	SM	DM	OA	OM	IS	OP
SM1	**.388**	.296	.038	.159	.144	.178
SM2	**.529**	.368	.142	.195	.291	.097
SM3	**.583**	.263	.195	.187	.347	.206
SM4	**.629**	.240	.242	.162	.235	.161
SM5	**.560**	.278	.190	.180	.249	.179
SM6	**.471**	.370	.177	.196	.295	.152
DM1	.275	**.648**	.115	.212	.230	.230
DM2	.267	**.702**	.177	.164	.213	.185
DM3	.239	**.662**	.170	.321	.250	.117
DM4	.179	**.585**	.273	.164	.330	.189
DM5	.275	**.615**	.221	.204	.265	.242
DM6	.318	**.571**	.260	.207	.318	.184
DM7	.281	**.640**	.220	.264	.296	.174
OA1	.283	.407	**.498**	.138	.390	.190
OA2	.239	.346	**.571**	.183	.159	.237
OA3	.297	.281	**.633**	.190	.252	.224
OA4	.237	.326	**.522**	.251	.455	.156
OA5	.189	.303	**.456**	.249	.310	.177
OA6	.091	.292	**.313**	.278	.475	.159
OA7	.147	.244	**.197**	.302	.517	.248
OA8	.219	.354	**.299**	.279	.472	.217
OA9	.124	.357	**.246**	.168	.497	.288

	SM	DM	OA	OM	IS	OP
OM1	.144	.401	.258	**.251**	.447	.258
OM2	.090	.343	.266	**.417**	.306	.234
OM3	.205	.262	.194	**.747**	.290	.164
OM4	.242	.281	.156	**.731**	.290	.191
OM5	.235	.287	.110	**.730**	.260	.221
OM6	.327	.249	.172	**.435**	.383	.177
IS1	.176	.358	.134	.138	**.652**	.249
IS2	.187	.191	.231	.133	**.599**	.216
IS3	.234	.310	.199	.129	**.613**	.261
IS4	.214	.169	.168	.209	**.593**	.231
IS5	.161	.081	.123	.173	**.589**	.257
IS6	.237	.343	.131	.139	**.628**	.253
IS7	.235	.143	.034	.203	**.607**	.297
IS8	.239	.170	.040	.185	**.700**	.298
IS9	.222	.316	.151	.213	**.599**	.271
OP1	.193	.229	.149	.163	.336	**.616**
OP2	.124	.136	.197	.114	.353	**.599**
OP3	.113	.133	.127	.103	.222	**.757**
OP4	.146	.149	.051	.135	.263	**.728**
OP5	.080	.126	.093	.107	.167	**.817**
OP6	.170	.222	.133	.161	.293	**.652**

Note: Intended factor loadings were outlined and items with loadings below 0.40 on their respective factor were shaded.

Table 4.10.

Results of the Principal Axis Factoring Extraction Method

Total Variance Explained						
Factor	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
IS	21.848	50.810	50.810	7.245	16.849	16.849
DM	2.409	5.602	56.412	5.642	13.121	29.971
OP	1.570	3.651	60.063	4.649	10.812	40.783
OM	1.290	3.000	63.063	3.465	8.057	48.840
SM	1.173	2.729	65.792	3.426	7.968	56.808
OA	1.001	2.327	68.119	2.786	6.479	63.288

The measurement models were next estimated using confirmatory factor analysis to evaluate the construct internal reliability and validity prior to simultaneously estimating measurement and structural models.

Internal reliability was assessed by computing a Cronbach's alpha reliability coefficient for each of the six constructs. Research literature suggested a reliability coefficient threshold of 0.70 indicating acceptable internal consistency (Hair et al. 2006). It is found that all constructs' Cronbach α ranged from 0.869 to 0.934, demonstrating a high degree of internal reliability consistency. Additionally, all values of item means and standard deviations were reasonable and within the expected ranges. Also notice that all

item-to-total correlations were positively greater than 0.40 with no excessive values. Item-to-total correlation is the simple correlation between the item and the sum of the rest with a minimum value of 0.40 as the norm (Blunch 2008).

In SEM, convergent validity is tested by assuring t-value of 1.96 at the 0.05 level for all item loadings (Anderson & Gerbing 1988; Schumacker & Lomax 2004). All items yielded standardized loadings statistically significant at $p < 0.05$ with t-tests > 1.96, indicating strong relations between the items and their corresponding constructs. Additionally, all values of the average variance extracted (AVE) for each construct were greater than the norm 0.05. Thus, the convergent validity was confirmed.

Discriminant validity was confirmed by examining the pairwise factor variances, where the AVE for each construct was greater than the squares of the correlations between the construct and all other constructs (Fornell and Larcker 1981). It is obvious that all values along the diagonal were greater than those in corresponding rows and columns, thus aiding in the determination for construct distinctiveness.

Tables 4.11 to 4.17 present the results of the reliability, convergent and discriminant validity analyses for each of the six constructs.

Table 4.11.

Reliability and Convergent Validity Analysis Results for SM

a. Scale Reliability and Item Statistics

Cronbach's α	Observed Variable	Mean	Standard Deviation	Standardized Estimate	t-test
0.869	SM2	3.40	1.210	0.706	--
	SM3	3.99	1.012	0.844	15.771
	SM4	3.98	1.017	0.798	14.731
	SM5	3.81	1.064	0.759	14.073
	SM6	3.67	1.142	0.715	13.598

b. Inter-Item and Item-to-Total Correlation Matrix

	SM2	SM3	SM4	SM5	SM6
SM2	1.000				
SM3	.617	1.000			.
SM4	.531	.667	1.000		
SM5	.494	.606	.626	1.000	
SM6	.546	.539	.544	.604	1.000
Item-to-Total	0.654	0.742	0.716	0.703	0.672

Table 4.12.

Reliability and Convergent Validity Analysis Results for DM

a. Scale Reliability and Item Statistics

Cronbach's α	Observed Variable	Mean	Standard Deviation	Standardized Estimate	t-test
0.934	DM1	3.50	1.100	0.806	--
	DM2	3.68	1.169	0.828	20.122
	DM3	3.33	1.216	0.818	19.566
	DM4	3.28	1.116	0.773	17.753
	DM5	3.30	1.176	0.819	19.165
	DM6	3.50	1.134	0.823	19.118
	DM7	3.25	1.165	0.859	20.496

b. Inter-Item and Item-to-Total Correlation Matrix

	DM1	DM2	DM3	DM4	DM5	DM6	DM7
DM1	1.000						
DM2	.774	1.000					
DM3	.706	.705	1.000				
DM4	.577	.631	.638	1.000			
DM5	.630	.642	.653	.662	1.000		
DM6	.603	.629	.624	.659	.739	1.000	
DM7	.667	.690	.697	.659	.698	.766	1.000
Item-to-Total	.775	.798	.788	.745	.788	.788	.823

Table 4.13.

Reliability and Convergent Validity Analysis Results for OA

a. Scale Reliability and Item Statistics

Cronbach's α	Observed Variable	Mean	Std. Dev	Standardized Estimate	t-test
0.908	OA1	3.68	1.100	0.839	--
	OA2	3.57	1.154	0.784	18.781
	OA3	3.55	1.216	0.854	21.279
	OA4	3.66	1.085	0.832	20.471
	OA5	3.80	1.062	0.773	18.391

b. Inter-Item and Item-to-Total Correlation Matrix

	OA1	OA2	OA3	OA4	OA 5
OA 1	1.000				
OA 2	.665	1.000			
OA 3	.708	.782	1.000		
OA 4	.696	.571	.682	1.000	.
OA 5	.655	.524	.592	.777	1.000
Item-to-Total	.791	.733	.808	.788	.725

Table 4.14.

Reliability and Convergent Validity Analysis Results for OM

a. Scale Reliability and Item Statistics

Cronbach's α	Observed Variable	Mean	Std. Dev	Standardized Estimate	t-test
0.909	OM2	3.31	1.094	0.655	--
	OM3	3.13	1.156	0.910	16.058
	OM4	3.06	1.175	0.919	16.001
	OM5	3.10	1.178	0.886	15.678
	OM6	3.61	1.126	0.693	12.929

b. Inter-Item and Item-to-Total Correlation Matrix

	OM2	OM3	OM4	OM5	OM6
OM2	1.000				
OM3	.613	1.000			
OM4	.569	.844	1.000		
OM5	.578	.795	.820	1.000	
OM6	.545	.616	.617	.635	1.000
Item-to-Total	.647	.847	.841	.832	.684

Table 4.15.

Reliability and Convergent Validity Analysis Results for IS

a. Scale Reliability and Item Statistics

Cronbach's α	Observed Variable	Mean	Std. Dev	Standardized Estimate	t-test
0.932	IS1	3.91	0.985	0.823	--
	IS2	4.11	0.942	0.727	17.114
	IS3	3.89	0.990	0.797	19.447
	IS4	4.21	0.939	0.736	17.207
	IS5	4.03	0.912	0.672	15.152
	IS6	3.74	1.040	0.844	21.110
	IS7	4.09	0.958	0.729	16.840
	IS8	3.99	0.950	0.839	20.639
	IS9	3.70	0.953	0.823	19.972

b. Inter-Item and Item-to-Total Correlation Matrix

	IS1	IS2	IS3	IS4	IS5	IS6	IS7	IS8	IS9
IS1	1.000								
IS2	.677	1.000							
IS3	.694	.694	1.000						
IS4	.592	.546	.611	1.000					
IS5	.501	.440	.463	.634	1.000				
IS6	.715	.589	.681	.590	.554	1.000			
IS7	.549	.480	.553	.563	.570	.589	1.000		
IS8	.670	.546	.610	.593	.608	.705	.706	1.000	
IS9	.658	.562	.640	.570	.523	.725	.570	.738	1.000
Item-to-Total	.788	.698	.768	.724	.655	.803	.704	.808	.776

Table 4.16.

Reliability and Convergent Validity Analysis Results for OP

a. Scale Reliability and Item Statistics

Cronbach's α	Observed Variable	Mean	Std. Dev	Standardized Estimate	t-test
0.912	OP1	3.82	0.964	0.779	--
	OP2	3.92	0.923	0.741	16.176
	OP3	4.06	0.907	0.824	18.302
	OP4	3.85	0.952	0.807	17.746
	OP5	3.79	0.911	0.839	18.374
	OP6	3.92	0.938	0.788	17.280

b. Inter-Item and Item-to-Total Correlation Matrix

	OP1	OP2	OP3	OP4	OP5	OP6
OP1	1.000					
OP2	.621	1.000				
OP3	.652	.649	1.000			
OP4	.634	.548	.650	1.000		
OP5	.611	.573	.703	.719	1.000	
OP6	.617	.617	.611	.629	.680	1.000
Item-to-Total	.744	.708	.780	.756	.786	.749

Table 4.17.

Results of Convergent and Discriminant Validity Analysis

	SM	DM	OA	OM	IS	OP
SM	**0.779**					
DM	0.631	**0.735**				
OA	0.680	0.705	**0.879**			
OM	0.477	0.499	0.530	**0.578**		
IS	0.559	0.554	0.642	0.450	**0.655**	
OP	0.389	0.386	0.447	0.313	0.456	**0.585**

Note: Average variance extracted was bolded and shown along the diagonal

Finally, the six measurement models were evaluated on multiple model fit criteria used in SEM to determine the fit between the hypothesized model and the observed data (McDonald and Ho 2002). Although all model fit statistics approached these levels, an examination of modification indices indicated that a better fit would be achieved if the error terms between the observed variables of the same constructs were free to correlate. After the correlated error terms were implemented, the modified measurement models were statistically superior compared to the original ones. Table 4.18 presents the final model fit statistics for the measurement models, assuming no relations among the latent constructs. Overall, the confirmatory factor analysis demonstrated good test results with acceptable internal reliability, convergent and discriminant validity. Further, the SRMR, CFI, TLI, and RMSEA values exceeded the guidelines, indicating good-fitting

measurement models. A visual diagram depicting the final six-factor confirmatory measurement model as a result of the CFA is shown in Figure 4.1.

Table 4.18.

Measurement Model Fit Results

Model	χ^2	*df*	*p*	χ^2/df	SRMR	CFI	TLI	RMSEA
Acceptable fit thresholds				< 5	≤ 0.05	≥ 95	≥ 95	< 0.08
SM	9.941	3	0.019	3.314	0.0167	0.993	0.977	0.074
DM	27.622	11	0.004	2.511	0.0192	0.993	0.986	0.059
OA	1.756	2	0.416	0.878	0.0056	1.000	1.001	0.000
OM	7.046	3	0.070	2.349	0.0101	0.997	0.991	0.056
IS	59.238	21	0.000	2.821	0.0244	0.986	0.975	0.065
OP	19.412	7	0.007	2.773	0.0176	0.992	0.992	0.064

Note: χ^2 = Chi-square; *df* = degrees of freedom; p = probability value; SRMR = standardized root mean square residual; CFI = comparative fit index; TLI = Tucker Lewis index; RMSEA = root mean square errors of approximation

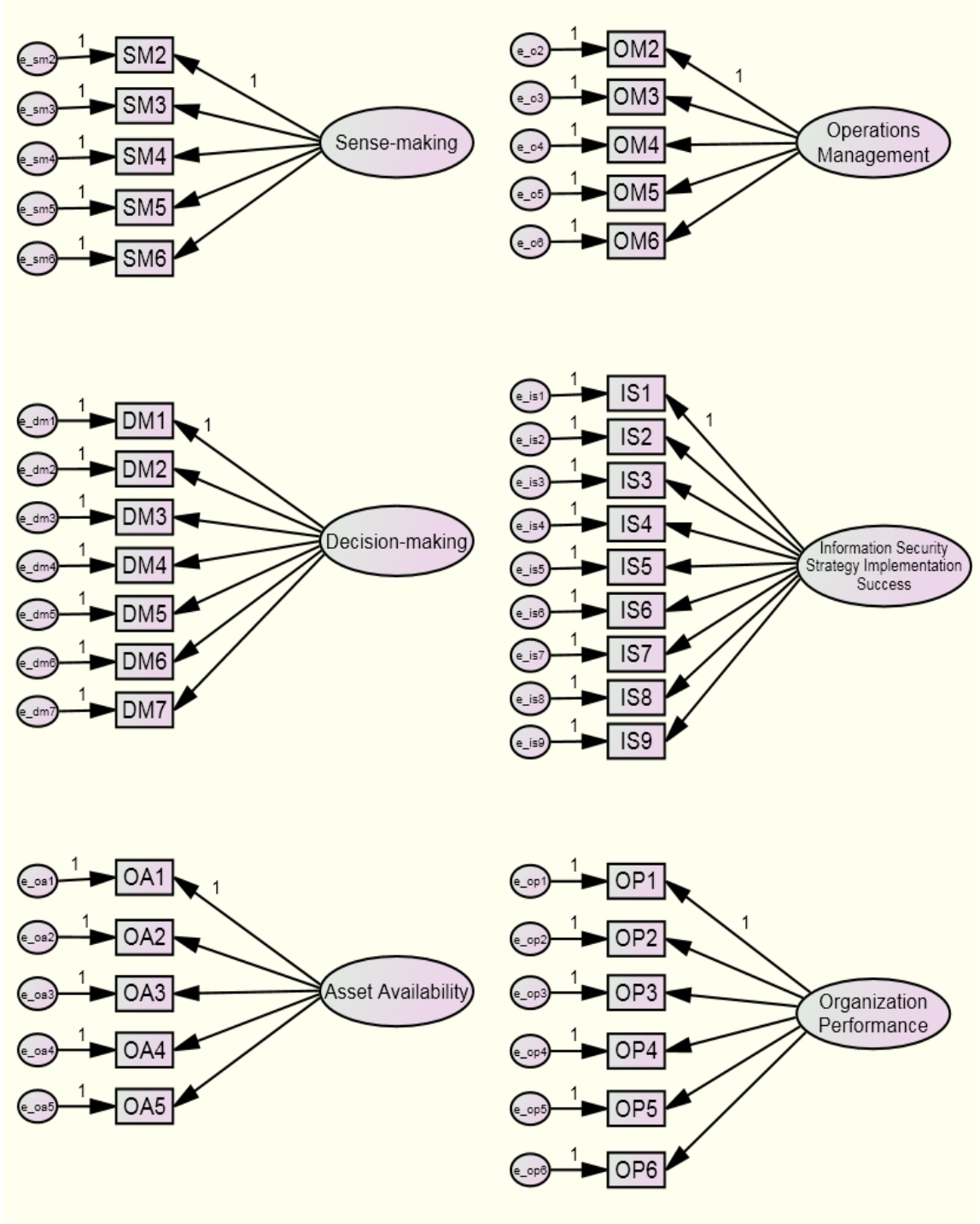


Figure 4.1. Confirmatory Measurement Model Six-Factor Solution

Examining Figure 4.1, there are five latent dependent variables (constructs or factors) depicted graphically by ovals, and 37 observed variables represented by rectangles. The latent variable Sense-making is measured by observed variables SM2, SM3, SM4, SM5, and SM6. The latent variable Decision-making is measured by observed variables DM1, DM2, DM3, DM4, DM5, DM6, and DM7. The latent variable Asset Availability is measured by the observed variables OA1, OA2, OA3, OA4, and OA5. The latent variable Operations Management is measured by the observed variables OM2, OM3, OM4, OM5, and OM6. The latent variable Information Security Strategy Implementation Success is measured by the observed variables IS1, IS2, IS3, IS4, IS5, IS6, IS7, IS8, and IS9. Finally, the latent variable Organization Performance is measured by the observed variables OP1, OP2, OP3, OP4, OP5, and OP6. The paths in the figure that point from one variable to another represent the direct effects that are statistically estimated by path coefficients or factor loadings, which are generally interpreted as regression weights in unstandardized or standardized form. In general, all latent variables must be assigned a scale. This is accomplished by constraining the regression weights of one indicator to 1 in each set of indicators designed to measure the same latent variables. This fixed parameter is referred to as a reference variable and, thus, not estimated.

The CFA model in Figure 4.1 also encompassed 37 measurement error variances denoted by small sized circles. The observed variable measurement error is defined as the portion of the observed variable score that is measuring something other than what

the latent is hypothesized to measure (Schumacker & Lomax 2004). Since the error term is not measurable, each measurement error term must also have its scale determined. However, the coefficient and the variance of an error term cannot be simultaneously estimated (Blunch 2008). In general, the variance is estimated and, thus, the coefficient is fixed at 1.0. This effectively sets the error term's measurement units to the same as the observed variable's units. Although not shown in the model, there are measurement error variances, depicted by curved, doubled headed arrows, indicating that they have shared variance or are correlated.

In the proposed model, all of the measures are reflective, meaning that the direction of causality is from the latent construct to the measured items. Each construct has a series of indicators that share a similar concept. Empirically, these indicators would tend to move together: when one changes, systematic change will occur in the other (Hair et al. 2006). Hence the confirmatory measurement model was hypothesized as reflective.

Confirmatory Structural Equation Model

Upon the successful specification of the measurement model, the next step was to develop a SEM model. Subsequently, a structural equation model was constructed in AMOS as shown in Figure 4.2. This model embodies the measurement models and structural model whereby the hypothesized relationships were extended among the latent variables of the CFA measurement model based on the dictated theory. The structural component of this model represents the hypothesis that organization performance derives from the successful implementation of information security strategy, which in turns, is influenced by the organization's capabilities in the context of information security.

The interpretation of the measurement model portion of the SEM model was previously discussed in detail in the section of CFA, thus elaboration is not necessary here. Examining the structural part of the SEM model, there are four exogenous latent variables in terms of Sense-making (SM), Decision-making (DM), Asset Availability (OA), and Operations Management (OM) that are postulated as being correlated with each other, as indicated by the curved two-headed arrows joining them. These exogenous latent variables are linked to the endogenous latent variable represented by Information Security Strategy Implementation Success (IS), which in turn is linked to another endogenous latent variable represented by Organization Performance (OP). These direct effects are depicted graphically by unidirectional arrows, pointing from the cause variable to the effect variable.

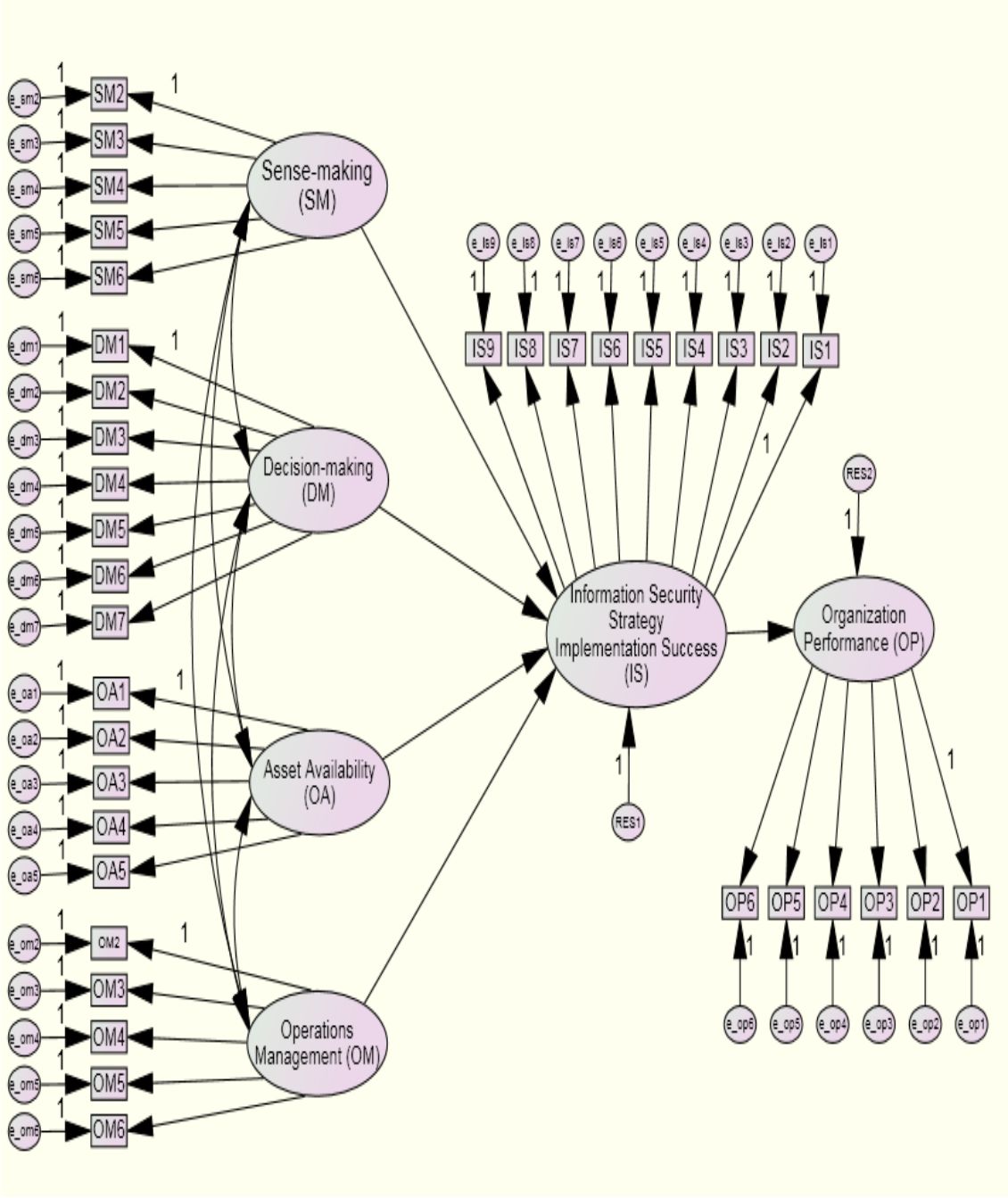


Figure 4.2. Structural Equation Model of Six Latent Variables

Finally, residual errors associated with the regression of Information Security Strategy Implementation Success (IS) on the exogenous latent variables, and the regression of Organization Performance (OP) on Information Security Strategy Implementation Success (IS), are captured by the disturbance terms RES1 and RES2 respectively. Hair et al. (2005) advised that absolute values of standardized residuals greater than 4.0 suggest a potential unacceptable level of error. Whereas absolute values of standardized residuals between 2.5 and 4.0 deserve some attention, however, changes to the model may not be necessary if there are no other problems associated with the associated variables.

The core parameters of interest in SEM that focus on the analysis of covariance structures are the regression coefficients, the variances and covariances of the independent variables. One important caveat in working with structural equations models, as Byrne (2001) pointed out, is to count the number of parameters in the model to be estimated prior to performing the analyses. This is necessary to ensure the model is statistically identified. With p observed variables, there are $p(p+1)/2$ data points to estimate the model parameters. Given 37 observed variables in the model, there were $37(37+1)/2 = 703$ pieces of information from which to derive the parameters of the model. The resultant number of distinct parameters embodies 31 measurement regression coefficients, 5 structural regression coefficients, 37 measurement error variances, 2 residual error variances, 4 independent variable variances, and 24 covariances. The 1's assigned to regression path parameters represent a fixed value of 1.00 and, thus, these parameters are not estimated. In total, there were 103 parameters that must be estimated in SEM analysis. The SEM model

yielded 600 degrees of freedom (703-103), resulting in an overidentified model that enabled the estimation of the fit values. An overidentified model is one in which the number of parameters to be estimated is less than the number of data points such as the unique variance and covariances of observed variables (Byrne 2001). It has positive degrees of freedom that allow for fitting of the SEM model.

The full SEM model depicted in Figure 4.2 was then evaluated using AMOS with the maximum likelihood method to assess the fit of the hypothetical model to the observed data. The confirmatory structural model results presented in Table 4.19 suggest that the hypothetical model provides a reasonably good fit.

Table 4.19.

Structural Equation Model Fit Results

χ^2	*df*	*p*	χ^2/df	SRMR	CFI	TLI	RMSEA
1069.1	600	0.000	1.782	0.0466	0.963	0.959	0.043

The overall model χ^2 value is 1069.1 with 600 degrees of freedom, which is rather large and significant at p = 0.000. However, all alternative fit statistics (χ^2/df = 1.782, SRMR = 0.0466, CFI = 0.963, TLI = 0.959, RMSEA = 0.043) exceeded acceptable fit threshold levels, suggesting a good fit between the hypothesized model and the collected data.

The SEM path diagram with the resultant standardized measurement and structural parameter estimates, along with the error terms of the observed variables is presented in Figure 4.3. The model data confirms significant and positive associations between Information Security Strategy Implementation Success (IS) and Organization Performance (OP), Asset Availability (OA), Sense-making (SM), Operations Management (OM). The relationships between IS and OP, OA are significant at $p < 0.001$ respectively, and the relationships between IS and SM, OM are significant at $p < 0.01$ respectively (H1, H2, H4, and H5 are supported). Of these hypothesized relationships, the path coefficient between Information Security Strategy Implementation Success and Organization Performance is the greatest (0.74), followed by Asset Availability and Information Security Strategy Implementation Success (0.50), Sense-making and Information Security Strategy Implementation Success (0.19), and then Operations Management and Information Security Strategy Implementation Success (0.17). However, there is no significant correlation between Decision-making and Information Security Strategy Implementation Success at the level of $p < 0.05$ (H3 is not supported). The error variances of the observed variables are small in magnitude, and in comparison with each other, one is no excessively larger than another, indicating a reasonable specification of the confirmatory structural equation model (Schumacker & Lomax 2004).

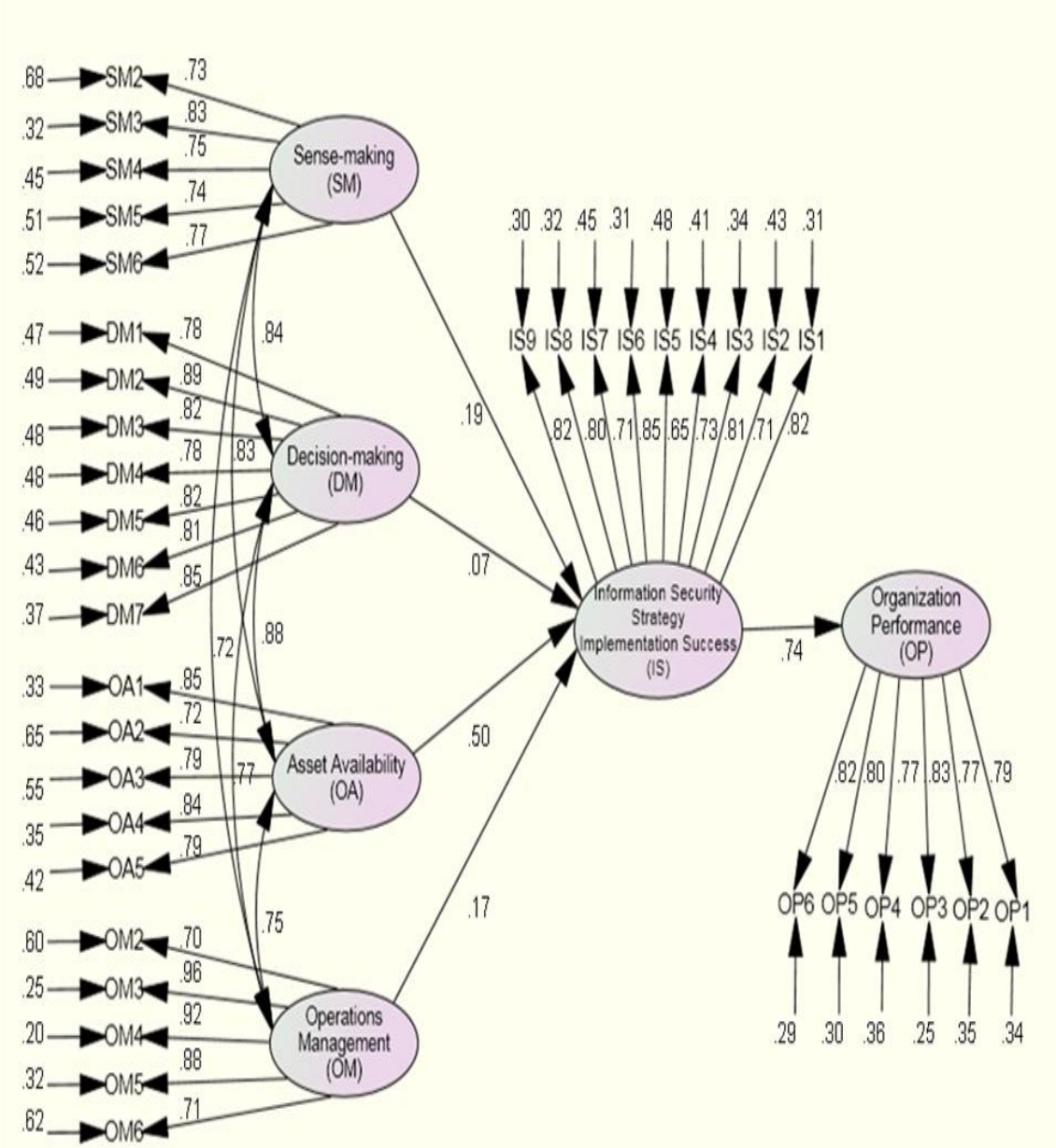


Figure 4.3. Results of Confirmatory Structural Equation Model

The results of the hypothesized structural regression coefficients along with the measurement regression weights in unstandardized and standardized forms are presented in Table 4.20. As shown in this table, with the exception of the path DM →IS, all other paths have regression weights that are significantly different from zero at the level of $p < 0.05$. Fitted regression weights and standardized regression weights reflect the change in the dependent variable for each unit change in the dependent variable. For example, when the IS factor increased by one standard deviation, the OP factor increased by 0.74 standard deviation. Additional outputs of AMOS analysis including standardized direct, indirect and total effects, along with correlations, variances, and covariances are provided in Appendix G.

Table 4.20.

Regression Weights for Fitted Structural Equation Model

Variable		Variable	Estimate	Stand. Error	Critical Ratio	*P*	Standardized Estimate
IS	<---	DM	0.063	0.09	0.70	0.485	0.066
IS	<---	OA	0.435	0.09	5.10	***	0.504
IS	<---	SM	0.176	0.07	2.62	0.009	0.192
IS	<---	OM	0.181	0.06	3.15	0.002	0.170
OP	<---	IS	0.696	0.05	13.64	***	0.737
DM1	<---	DM	1.000				0.731
DM2	<---	DM	1.090	0.05	23.34	***	0.830
DM3	<---	DM	1.163	0.06	18.83	***	0.751
DM4	<---	DM	1.019	0.06	17.46	***	0.738
DM5	<---	DM	1.117	0.06	18.39	***	0.774
DM6	<---	DM	1.076	0.06	18.12	***	0.780
DM7	<---	DM	1.159	0.06	19.54	***	0.800
OA1	<---	OA	1.000				0.821
OA2	<---	OA	0.882	0.05	17.14	***	0.784
OA3	<---	OA	1.008	0.05	19.28	***	0.816
OA4	<---	OA	0.955	0.05	20.55	***	0.826
OA5	<---	OA	0.895	0.05	19.06	***	0.791
OM2	<---	OM	1.000				0.697
OM3	<---	OM	1.368	0.08	16.91	***	0.901
OM4	<---	OM	1.424	0.09	16.15	***	0.922
OM5	<---	OM	1.360	0.08	16.48	***	0.878
OM6	<---	OM	1.045	0.07	14.27	***	0.707

Variable		Variable	Estimate	Stand. Error	Critical Ratio	*P*	Standardized Estimate
IS1	<---	IS	1.000				0.822
IS2	<---	IS	0.827	0.05	18.36	***	0.713
IS5	<---	IS	0.986	0.05	14.41	***	0.807
IS6	<---	IS	0.845	0.05	21.16	***	0.729
IS7	<---	IS	0.725	0.05	16.25	***	0.645
IS8	<---	IS	1.087	0.05	19.32	***	0.846
IS9	<---	IS	0.833	0.05	19.97	***	0.708
OP1	<---	OP	0.937				0.799
OP2	<---	OP	0.963	0.05	17.24	***	0.819
OP3	<---	OP	1.000	0.05	18.36	***	0.794
OP4	<---	OP	0.923	0.06	17.36	***	0.765
OP5	<---	OP	0.983	0.05	17.77	***	0.829
OP6	<---	OP	0.960	0.06	17.98	***	0.772

Note: *** p < .001 (two-tailed)

Analysis of Mediation Effects

In the SEM model presented in Figure 4.2, Information Security Strategy Implementation Success is hypothesized as mediating the relationship between organization capability factors, represented by Sense-making, Decision-making, Asset Availability, and Operations Management, and Organization Performance. Since the fit test demonstrated a good-fitting model, it supports the mediating role of the Information Security Strategy Implementation Success. However, to address the research question concerning the extent of the relations between organization capabilities (independent variables) and organization's performance (dependent variable), additional tests were necessary. A series of steps recommended by Hair et al. (2005) were applied to evaluate mediation effects. If there are indications of any direct relations between independent variables and dependent variable, then the full mediation is not supported. Then, if there are indirect paths between independent variables and dependent variable and their estimates are significant, thus partial mediation is supported.

The SEM techniques were used to analyze the effects between the hypothesized variables. Table 4.21 reports the decomposition of effects of independent variables (Sense-making, Decision-making, Asset Availability, and Operations Management) on the dependent variable (Organization Performance), whereby the total effect of one factor on another is the sum of the direct and the indirect relationships between the factors. The results in this table indicate no direct relations between independent variables and dependent variable, thus the partial mediation is not supported. However, the results

illustrate the indirect effects between the underlying variables. Although the size of each indirect effect is small, it is proportional to the magnitude of the standardized direct effects that were evaluated in a previous section. Asset Availability has the greatest standardized indirect effect on Organization Performance is (0.372, p<.001), followed by Sense-making (0.141, p<.01), then Operations Management (0.125, p<.01). The results therefore support the full mediation model with Information Security Strategy Implementation Success as the mediator variable. In other words, the relationships between organizational capability factors, in terms of Asset Availability, Sense-making, and Operations Management, and Organization Performance are completely mediated by Information Security Strategy Implementation Success. Hence, hypotheses H6, H8, and H9 are supported. Conversely, the strength of the indirect effect of Decision-making on Organization Performance, which is 0.049, is trivial relative to others. Small indirect effects that are less than 0.08 are seldom of interest and rarely add to the substantive conclusions (Hair et al. 2006). Thus H7 is not supported. Figure 4.3 presents the path diagram illustrating the results of the full mediation model. The dotted paths depict the indirect effects between variables.

Table 4.21.
Standardized Effects of Organizational Capability Factors on Organization Performance

Variable	Direct Effects	Indirect Effects	Total Effects
Sense-making	0.000	0.141	0.141
Decision-making	0.000	0.049	0.049
Asset Availability	0.000	0.372	0.372
Operations management	0.000	0.125	0.125

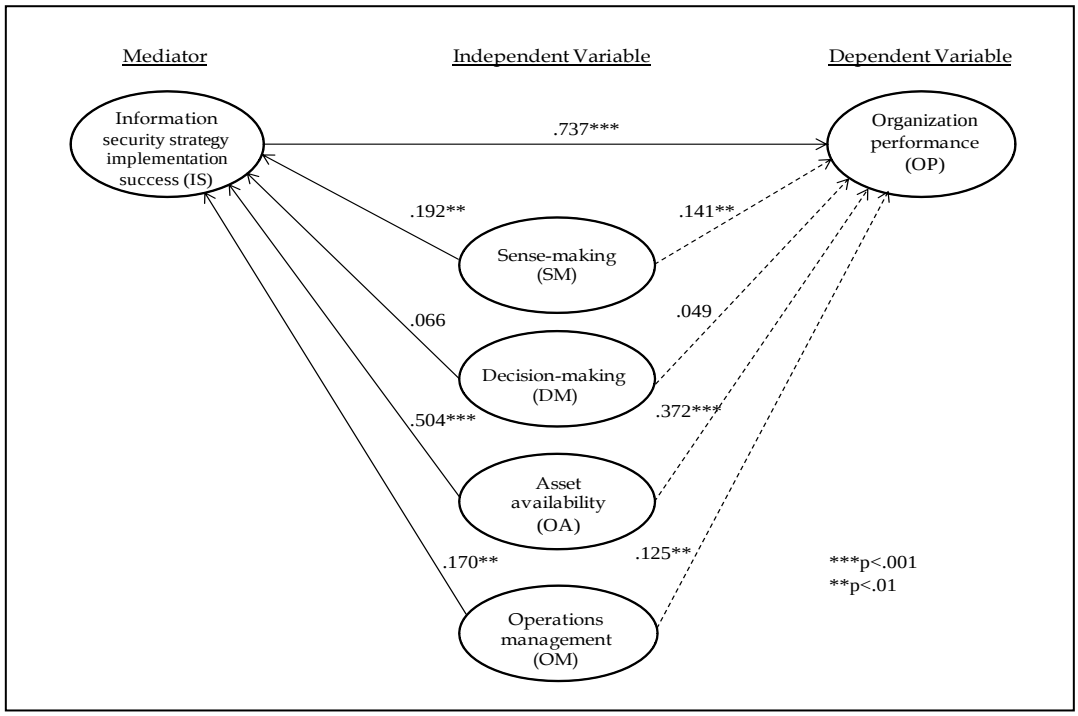


Figure 4.4. Fitted Model Showing Standardized Direct and Indirect Effect Estimates

Summary

This chapter presented the results of the empirical data analysis including descriptive analysis of sample characteristics using PAWS software and SEM analysis of the theoretical model using AMOS. The data screening procedures enabled the validation of assumptions required for SEM prior to running the analysis. Most of the required assumptions were satisfied with the exception of multivariate normality. The bootstrapping technique available in SEM was used as a remedy to correct the normality problem.

A theoretical model was fitted to demonstrate the hypothesized relationships among proposed constructs that consist of Sense-making, Decision-making, Asset Availability, Operations Management, Information Security Strategy Implementation Success, and Organization Performance. The reliability and validity of the theoretical model were evaluated through confirmatory measurement model and confirmatory structural model assessments. Consequently, the six-factor model was determined appropriate for SEM analysis. All fit statistics indicated a reasonable fit between the hypothetical model and the empirical data, and seven of the nine null hypotheses were supported. The summary of findings, along with conclusions and recommendations for future research are discussed in the next chapter.

Chapter 5 – Summary, Conclusions, and Recommendations

This research was designed to address the research questions concerning the impacts of organizational capabilities in information security. Three questions developed for investigation were:

Research Question 1: What is the relationship, if any, between information security strategy implementation success and organization performance?

Research Question 2: What are the relationships, if any, between organizational capabilities and information security strategy implementation effectiveness?

Research Question 3: To what extent do organizational capabilities influence organization performance?

The approach to address the research questions was a quantitative methodology that involves fitting a hypothetical model to the observed data and to test the hypothesized relationships. This was achieved by proposing and validating a theoretical model that demonstrates the linkage between information security strategy implementation success and organization performance, with organizational capabilities as key factors influencing the successful implementation of information security strategy. The research propositions asserted that essential organization capabilities must include developing high quality awareness and understandings of internal and external situations, making decisions with respect to planning and courses of action, obtaining and retaining appropriate skills and resources, as well as managing and measuring the information security program. These organization capabilities were represented in the model by the

sense-making, decision-making, asset availability, and operations management variables. The model also consists of two additional variables, information security strategy implementation success and organization performance, thus encompassing six hypothesized constructs.

Based on existing literature in information security and strategic management, an original survey instrument was developed to collect empirical data. Using confirmatory factor analysis, the theoretical constructs were evaluated and evidence of acceptable internal reliability, convergent validity, and discriminant validity was assured. A structural equation modeling approach was utilized to quantitatively analyze data and to test the validity of the research hypothesis. Structural equation modeling is a comprehensive statistical technique for hypothesis testing and fitting the structural equation model, taking into account observed and latent variables as well as measurement error terms (Schumacker & Lomax 2004). Although Chi-Square is the traditional measure used in assessing overall model fit, it tends to be unreliable when sample sizes larger than 200 are used (Reinard 2006). Researchers suggested that alternative fit indexes be used as there is no agreement on the best single approach for evaluating model fit. Amid the large sample size used in this study (428), alternative fit tests including χ^2/df, SRMR, CFI, TLI, RMSEA were reported. In the hypothesized model, all fit statistics exceed the thresholds for acceptable fit, indicating a good fit between sample data and the theoretical patterns in the data.

Summary of Hypothesis Tests

Based on the quantitative analysis using SEM techniques, a reasonable fit between the hypothetical model and the empirical data was demonstrated, and seven of nine null hypotheses were supported. Each of the research questions was addressed from the results of the hypothesis tests. To answer Research Question 1, Hypothesis H1 was examined. Hypotheses H2, H3, H4, and H5 were evaluated to address Research Question 2. Finally, Hypotheses H6, H7, H8, and H9 were assessed to answer Research Question 3. As aforementioned, in SEM, theoretical hypothesis is often aligned with the null hypothesis, which specifies that a model does not contradict the empirical data (Tomarken & Waller 2005). Statistically speaking, researchers are most interested in having the null hypothesis supported when using the SEM approach (Hershberger 2003). The results of the hypothesis tests in this research are based on the empirical analysis with SEM techniques that address the research questions concerning the relations among organizational capabilities, information security strategy, and organization performance, and are summarized below.

Research Question 1: What is the relationship, if any, between information security strategy implementation success and organization performance?

Null Hypothesis 1: Successful implementation of an overall information security strategy is positively associated with organization performance.

The SEM analysis demonstrated a direct relationship between the Information Security Strategy Implementation Success and Organization Performance latent variables

represented by a significant standardized regression weight. Based on this finding, the null hypothesis 1 is supported.

Research Question 2: What are the relationships, if any, between organizational capabilities and information security strategy implementation effectiveness?

Null Hypothesis 2: Sense-making is positively associated with information security strategy implementation success.

The Sense-making latent variable was found to have a positive effect on the Information Security Strategy Implementation Success latent variable, represented by a statistically significant standardized regression weight. Thus, the null hypothesis 2 is supported.

Null Hypothesis 3: Decision-making is positively associated with information security strategy implementation success.

The SEM analysis indicated no statistically significant relations between the Decision-making latent variable and the Information Security Strategy Implementation Success latent variable. Thus, the null hypothesis 3 is rejected.

Null Hypothesis 4: Asset availability is positively associated with information security strategy implementation success.

The quantitative analysis indicated a strong relation between the Asset Availability and Information Security Strategy Implementation Success latent variables, represented by a statistically significant standardized regression weight. Therefore, the null hypothesis 4 is supported.

Null Hypothesis 5: Operations management is positively associated with information security strategy implementation success.

The SEM analysis demonstrated a positive relation between the Operations Management latent variable and the Information Security Strategy Implementation Success latent variable, which was represented by a statistically significant standardized regression weight. Thus, the null hypothesis 5 is supported.

Research Question 3: To what extent do organizational capabilities influence organization performance?

Null Hypothesis 6: Sense-making and organization performance is fully mediated by information security strategy implementation success.

The SEM analysis of the confirmatory structural model demonstrated the mediating role of the Information Security Strategy Implementation Success latent variable. Additionally, there was no indication of direct effect between the Sense-making and Organization Performance latent variables, and the indirect effect between these variables was statistically significant. Hence, the null hypothesis 6 is supported.

Null Hypothesis 7: Decision-making and organization performance is fully mediated by information security strategy implementation success.

The quantitative analysis of empirical data did not indicate any significant relation between the Decision-making and Organization Performance latent variables. Hence, the null hypothesis 7 is not supported.

Null Hypothesis 8: Asset availability and organization performance is fully mediated by information security strategy implementation success.

The SEM analysis demonstrated the mediating role of the Information Security Strategy Implementation Success. There was no indication of any direct effect between the Asset Availability and Organization Performance latent variables. However, the indirect effect between these variables was found statistically significant. Thus, the null hypothesis 8 is supported.

Null Hypothesis 9: Operations management and organization performance is fully mediated by information security strategy implementation success.

The mediating role of the Information Security Strategy Implementation Success was previously demonstrated. There was no direct effect between the Operations Management and Organization Performance latent variables. However, the indirect effect between these variables was found statistically significant. Hence, the null hypothesis 9 is supported.

Conclusions

The purpose of this research was to address the three research questions that evaluate the relationship between information security strategy implementation success and organization performance, as well as identify and examine the impacts of organization capabilities in information security, thereby contributing to the body of knowledge in an emerging field. Data was collected using an original self-administered mail survey of Certified Information Systems Security Professionals. The resultant 428 usable responses were analyzed with the SEM techniques to validate the theoretical model and test the hypotheses, thus, addressing the research questions.

With respect to the first research questions that sought to investigate the linkage between successful implementation of information security strategy and organization performance, the results have shown that information security strategy implementation success has a positive and direct effect on organization performance. Evidence shows that the effective implementation of information security strategy provides the conditions under which an improvement in organization performance is likely to occur. This may be accomplished through a combination of activities such as maintaining appropriate protection of information assets, achieving information security compliance with legislation, regulatory and industry requirements, upholding information security policies and standards, responding promptly to information security attacks, recovering quickly from systems failure or interruption, keeping information security risks to a minimum, sustaining continuity of mission-critical operations, preventing damages to and allowing

for better control of information assets. The result is consistent with the theory suggesting that effective information security strategy can be instrumental in helping an enterprise meet its business goals (ISACA 2009).

With respect to the second research question that sought to investigate the linkage between organizational capabilities and successful implementation of information security strategy, the study indicated that organizational capabilities consisting of sense-making, asset availability, and operations management have direct effects on successful implementation of information security strategy. Of the organizational capabilities surveyed, the asset availability factor, reflecting the extent to which an organization is able to obtain and organize the competencies, resources and processes needed to accomplish information security strategy goals is the most critical organizational capability in the model. Next to asset availability, sense-making is the second most essential capability that reflects the ability to extract meaningful information and to make appropriate decisions. Finally, evidence also shows a significant relationship between operations management and successful implementation of information security, demonstrating that the capability to orchestrate available means and capabilities is related to effective information security strategy.

The results showed strong correlations between decision-making and other organizational capabilities, namely sense-making, asset availability, and operations management. This finding is consistent with the general consensus that leadership plays a

key role in developing and deploying organization capabilities crucial for competitive advantage (Ulrich & Lake 1991; King 1999; Ulrich & Smallwood 2004).

Conversely, the research did not find a significant correlation between decision-making and successful implementation of information security strategy, and the indirect effect of decision-making on organization performance is minimal. Given the research sample of mostly information security professionals, these findings reflect, for the most part, the perspective of technical respondents, which indicate a possible conflict between technical members and senior managers. Some participants, presumably technical, expressed their frustrations towards top management as reflected in their optional feedback. A representative comment is provided below.

> *"One can have an effective information assurance program, validated by independent parties, without direct management support… Given the right mix of individuals possessing the applicable enthusiasm and talents, excellent information security program can and do flourish… If managers simply do not impede the process, the right people can maintain an effective program… Money does not guarantee an effective information assurance program; rather it is the individuals who devise, manage and implement it. Therefore, recruitment of those individuals is of paramount importance."*

On the other hand, a non-technical participant expressed a different perspective in that information security is not critical to an organization:

"A business must pay its bills, which comes from selling its goods or services at a profit. Without profit, the business must close its doors. Security for most companies is a necessary cost of doing business, but not the objective."

Additional feedback from respondents most relevant to the area of investigation is provided in Appendix H. Taken together, the present study gives the impression of a cultural issue that may be the consequences of some level of distrust, dissatisfaction, lack of confidence, or combinations of any two or more of these behaviors, on the part of technical members towards the leadership's commitment and decision-making ability. Nonetheless, this finding is not surprising. In a study examining the relationship between trust, culture and risk communication among information technology technical members and managers, Koskosas & Paul (2004) noted that "not all IT employees participate in decision-making with regard to security issues, and that, in effect, a few distrusted the motives, attitudes and beliefs of top management". Furthermore, in a study that surveyed a broad cross-section of federal agency Chief Information Security Officers (CISOs), $(ISC)^2$ (2009) cited governance issues as one of the greatest concerns of CISOs. Among the areas of concerns were the need for more senior management buy-in, the persistence of organizational stovepipes, and the leadership and bureaucratic obstacles to success. $(ISC)^2$ also quoted one CISO's statement "We're fighting ourselves" as an evidence of persistent uncertainty at the governance level. And yet, more than a year later, information security

professionals continue to face organizational challenges related to governance as reflected in the findings of this current survey.

With respect to the third research question that sought to explore and assess the extent to which organizational capabilities effect organization performance, the mediating role of information security strategy implementation success that accounts for the indirect effects on organization performance from organizational capabilities was evidenced. Thus, it is concluded that the effects of organizational capabilities (e.g. sense-making, decision-making, asset availability) on organization performance are mediated by effective information security strategy implementation. In other words, the capabilities of an organization in the information security context, represented by the ability to make sense of a situation, the ability to obtain and deploy available means and capabilities, and the ability to manage those means, effect the successful implementation of information security strategy, which in turn explains the improvement in the performance of the organization.

Implications

The results of this research are expected to provide several implications. In part, the research offers valid implications for organizations seeking to positively substantiate the resources devoted to information security. By analyzing an organization's information security capabilities as an aggregation of sense-making, decision-making, asset availability, and operations management constructs, this study provides business an understanding of, and insight into, the viable predisposition of organizational capabilities in the context of

information security. Evidence of organizational capabilities' positive effects on information security strategy and organization performance highlights the importance and consequences of an organization's intangible assets as it competes in today's challenging marketplace. Business leaders should focus on acquiring organizational capabilities that provide high valued contributions to the accomplishment of information security strategy goals and organizational objectives, thus, in turns, enabling their businesses to achieve market-leading performance and competitive advantage.

In part, this research also provides insights into the challenges information security professionals continue to face concerning organizational governance. Awareness of these shortcomings allows business leaders opportunities to make necessary changes in direction that enables information security professionals to succeed. Executives can bring about changes in governance through activities such as visible participation and action, ongoing communication and clear intention to support information security initiatives and to mitigate security risks, and serving as role models in placing a high priority on information security (NIST 2007; ISACA 2005). The risks are high for taking no action, as information security professionals are at the forefront of the ongoing battle to protect information and information assets needed to achieve business goals and objectives. A motivated security professional workforce is crucial to the survival of an organization in the complex and rapidly changing networked environments.

Lastly, this work provides the first empirical research examining the impacts of organizational capabilities that can be used as the roadmap for further research

explorations in information security from an organizational perspective. Additionally, this study contributes to the research community an original survey instrument that can be applied or built upon to collect data that furthers existing knowledge on the impacts of intangible assets in information security.

Recommendations for Future Research

Several recommendations are suggested for future research. First, as previously indicated, a possible limitation of this study concerns the survey instrument as it was perceived to be designed with a focus on medium-to-large firms in the private sector. Future use of this instrument may benefit from higher response rates if the organization performance scale is revised to better apply to government/non-profit organizations. For example, a research participant stated that "There is no business value for a government agency. There are compliance requirements, but no real penalties for non-compliance." Follow-on studies are recommended to examine the moderating effects of the size and type of organizations on the association between organizational capabilities and information security strategy implementation.

Second, there may be a potential source of bias resulting from the technical nature of the intended population. By polling primarily information security specialists, the results may have been partially influenced by their inherently technical perspective. For greater generalizability of the results, the targeted sample should include a reasonable mix of information security professionals and individuals in managerial and strategic planning

positions. In today's environment, information security is increasingly seen as a business driver, which reflects the need for involvement and support at the board and executive levels and throughout the organization. Thus, to further the generalized knowledge of the impacts of organizational capabilities in information security, the recommendation to incorporate a higher percentage of senior managers and executives in the respondent sample is worth investigating.

Third, the inconclusive result concerning the effects of decision-making on information security strategy implementation success and organization performance provides opportunities for further studies. Three recommendations for advancing general knowledge in this area are formulated. First is the proposal to build upon this study that integrates technical and managerial insights in order to gain more benefits from different perspectives. Countering this recommendation is an interest in understanding the managerial perspectives as compared to the technical ones. A survey of executives and managers, using the same instrument, to gather their views and compare them to the findings in this study would be intriguing. This is necessary to examine the concept of diverse views between information security professionals and senior managers. Finally, empirical research that explores the issues of governance, the factors that influence the decision-making capability and how it relates to effective implementation of information security strategy and organization performance should also be considered in order to achieve a definitive conclusion on the role of decision-making and governance in information security.

References

Adams, M. (2006), "Intangible Assets, Tangible Risks", *Risk Factor*, 2(4), pp.1-3, available at: http://www.complianceresearchgroup.com/Documents/RiskFactor-ServiceIndustryRisks.pdf, (accessed 28 October 2010).

Alberts, D.S. (2002), *Information Age Transformation: Getting to a 21st Century Military*, Washington D.C.: CCRP Publication Series.

Alberts, D., Garstka, J.J., Hayes, R.E. & Signori, D.T. (2001), *Understanding Information Age Warfare*, Washington D.C: CCRP Publication Series.

Alberts, D. & Hayes, R.E. (2003), *Power to the Edge: Command, Control in the Information Age*. Washington D.C.: CCRP Publication Series.

Allen, J. (2005), *Governing for Enterprise Security*, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, available at: http://www.sei.cmu.edu/reports/05tn023.pdf (accessed 11 February 2010).

Amaio, T.E. (2009), *Exploring and Examining the Business Value of Information Security: Corporate Executives' Perceptions*, Ph.D Diss., Northcentral University.

Anderson, E. & Choobineh, J. (2008), "Enterprise Information Security Strategies", *Computers & Security*, 27 (1-2), pp. 22-29.

Anderson, J.C. & Gerbing, D.W. (1988), "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach", *Psychological Bulletin*, 103(3), pp. 411-423.

Ansoff, I. (1965), *Corporate Strategy*, Penguin Books, New York.

Alshboul, A. (2010), Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. *Communications of the IBIMA*, 50(79), pp. 1–9.

Barney, J. (1991), "Firm Resources and Sustained Competitive Advantage", *Journal of Management*, 17(1), 99-120.

Barney, J.B. & Zajac, E.J. (1994), "Competitive Organizational Behavior: Of Competitive Advantage", *Strategic Management Journal*, 15(S1), pp. 5-9.

Bennett, J.A. (2000), "Focus on Research Methods Mediator and Moderator Variables in Nursing Research: Conceptual and Statistical Differences", *Research in Nursing & Health*, (23), pp. 415-420.

Bentler, P.M. (1990), "Comparative Fit Indexes in Structural Models", *Psychological Bulletin*, 107(2), pp. 238-246.

Bentler, P.M. & Chou, C.P. (1987), "Practical Issues in Structural Modeling", *Sociological Methods and Research*, 16(1), pp. 78-117.

Bersherger, S.L., Marcoulides, G.A. & Parramore, M.M. (2003), "Structural Equation Modeling: An Introduction", in Bruce Pugesek et al. (Eds.), *Structural Equation Modeling: Applications in Ecological and Evolutionary Biology*. New York: Cambridge University Press, pp. 3-41.

Blunch, N. (2008), *Introduction to Structural Equation Modelling Using SPSS and Amos*, London: SAGE.

Bollen, K.A. (1989), *Structural Equations With Latent Variables*, New York: Wiley.

Bollen, K.A. (1996), *Testing Structural Equation,* 4th ed., Newbury Park, California [etc.]: Sage Publications.

Bourque, L.B. & Fielder, E.P. (2003), *How to Conduct Self-Administered and Mail Survey*, 2nd ed., Thousand Oaks California: Sage Publications.

Brown, M.W. & Cudeck, R. (1996), "Alternative Ways of Assessing Model Fit", in Bollen & Long (Eds.), *Testing Structural Equation,* Newbury Park, California [etc.]: Sage Publications, pp. 146-162.

Byrne, B. (2001), *Structural Equation Modeling with Amos: Basic Concepts, Applications, and Programming*, Mahwah N.J.: Lawrence Erlbaum Associates.

Caralli, R.A. (2004), *Managing for Enterprise Security*, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, available at: http://www.sei.cmu.edu/reports/04tn046.pdf (accessed 11 February 2010).

Chang, S.E. & Ho, C.B. (2006), "Organizational Factors to the Effectiveness of Implementing Information Security Management", *Industrial Management & Data Systems*, 106 (3), pp. 345-361.

Chen, C.C., Medlin, B.D. & Shaw, R. (2008a), "A Cross-Cultural Investigation of Situational Information Security Awareness Programs", *Information Management & Computer Security*, 16(4), pp. 360–376.

Chen, F., Curran, B., Bollen, K., Kirby, J., & Paxton, P. (2008b), "An Empirical Evaluation of the Use of Fixed Cutoff Points in RMSEA Test Statistic in Structural Equation Models", *Sociological Methods & Research*, 36(4), pp. 462-494.

Chou, C. & Bentler, P.M. (1995), "Estimates and Tests in Structural Equation Modeling", in Hoyle, R (Ed.), *Structural Equation Modeling: Concepts, Issues, and Applications*. Thousand Oaks, California: SAGE Publications, pp. 37-55.

Cockburn, I.M., Henderson, R.M. & Stern, S. (2000), "Untangling the Origins of Competitive Advantage", *Strategic Management Journal*, 21(10/11), 1123-1145.

Collis, D.J. (1994), "How Valuable Are Organizational Capabilities?", *Strategic Management Journal*, 15, 143-152.

Creswell, J. (2009), *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* 3rd ed., Thousand Oaks: Sage Publications.

Cronbach, L.J. (1951), "Coefficient Alpha and the Internal Structure of Tests", *Psychometrika*, 16(3), pp. 297–334.

Deloitte (2008), "Gaining Momentum: The 2008 Energy & Resources Global Security Survey", available at: http://www.deloitte.com/assets/Dcom-Turkey/Local Assets/Documents/Turkey-En_ers_ER-SecuritySurvey_220808.pdf (accessed 28 October 2010).

Dillman, D., Smyth, J.D. & Christian, L.M. (2009), *Internet, Mail, and Mixed-Mode Surveys: The Tailored Design Method.* 3rd ed., Hoboken N.J.: Wiley & Sons.

Eisenhardt, K.M. & Martin, J.A. (2000), "Dynamic Capabilities: What Are They?", *Strategic Management Journal*, 21 (10-11), pp. 1105-1121.

Endsley, M.R. (1995), "Situational Awareness and the Cognitive Management of Complex Systems", *Human Factors*, 37(1), pp. 85-104.

Ernst & Young (2007), “Ernst & Young 2007’s Global Information Security Survey”, available at: http://www2.eycom.ch/publications/items/2007_giss/2007_ey_giss.pdf (accessed 28 October 2010).

Ernst & Young (2008), “Ernst & Young 2008’s Global Information Security Survey”, available at: http://www.ey.com/Publication/vwLUAssets/GISS_2008/$FILE/GISS2008.pdf (accessed 28 October 2010).

Ezingeard, J., McFadzean, E. & Birchall, D. (2005), “A Model of Information Assurance Benefits”, *Information Systems Management*, 22(2), pp. 20-29.

Fan, X., Thompson, B. & Wang, L. (1999), “Effects of Sample Size, Estimation Methods, and Model Specification on Structural Equation Modeling Fit Indexes”, *Structural Equation Modeling*, 6(1), pp. 56-84.

FFIEC (2006) “Information Security Booklet”, available at: http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf (accessed 28 October 2010).

Fornell, C. (1987), "A second generation of multivariate analysis: Classification of methods and implications for marketing research," In *Review of Marketing*, Houston, M.J. (ed.), American Marketing Association, Chicago, pp. I407–1450.

Fornell, C. & Larcker, D.F. (1981),“Evaluating Structural Equation Models with Unobservable Variables and Measurement Error”, *Journal of Marketing Research*, 18(1), pp. 39-50.

Fraenkel, J. & Wallen, N. (2009), *How to Design and Evaluate Research in Education* 7th ed., New York NY: McGraw-Hill.

Fratto, M. (2009), "2009 Strategic Security Survey", available at: http://i.cmpnet.com/custom/strategicsecurity/assets/InformationWeek_Analytics_2009_Strategic_Security_Survey.pdf (accessed 28 October 2010).

GAO (2006), "*Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs*", GAO Report 06-897T.

Garver, M. S. and Mentzer, J.T. (1999), "Logistics Research Methods: Employing Structural Equation Modeling To Test For Construct Validity", *Journal of Business Logistics*, 20(1), pp. 33-57.

Gefen, D. (2003), "Assessing Unidimensionality Through Lisrel: An Explanation and Example", *Communications of the Association for Information Systems*, 12, pp. 23-47.

Gefen, D. & Straub, D., (2005), "A Practical Guide to Factorial Validity Using Pls-Graph: Tutorial and Annotated Example", *Communications of the Association for Information Systems*, 16, pp. 91-109.

Gefen, D., Straub, D.W. & Boudreau, M.C. (2000), "Structural Equation Modeling And Regression: Guidelines for Research Practice", *Communications of the Association for Information Systems*, 4(7), pp.1-76.

Gold, A.H., Malhotra, A. & Segars, A.H. (2001), "Knowledge Management: An Organizational Capabilities Perspective", *Journal of Management Information Systems*, 18 (1), pp.185-212.

Grant, R.M. (1991), "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation", *California Management Review*, 33(3), 114-135.

Hair, J. et al. (2006), *Multivariate Data Analysis*, 6th ed., Upper Saddle River N.J.: Pearson Prentice Hall.

Hall, J., Sarkani, S. & Mazzuchi, T.A. (2010), "Moderating Roles of Organizational Capabilities in Information Security", paper presented at the 5th International Conference on i-Warfare & Security (ICIW 2010), 8-9 Apr 2010, Dayton, Ohio.

Hancock, G. & Mueller, R.O., Eds (2006), *Structural Equation Modeling: A Second Course*, Greenwich Conn.: IAP.

Hansche, S. (2001), "Designing a Security Awareness Program: Part 1", *Information Systems Security*, 9(6), pp. 14-23.

Hershberger, S.L., Marcoulides, G.A. & Parramore, M.M. (2003), Structural Equation Modeling: An Introduction, in Pugesek, B. et al. (Eds.), *Structural Equation Modeling: Applications in Ecological and Evolutionary Biology*. New York: Cambridge University Press, pp. 3-41.

Hoe, S. (2008), "Issues and Procedures in Adopting Structural Equation Modeling Technique", *Journal of Applied Quantitative Methods*, 3(1), pp. 76-83.

Hooper, D., Coughlan, J. & Mullen, M.R. (2008), "Structural Equation Modelling: Guidelines for Determining Model Fit", *The Electronic Journal of Business Research Methods*, 6(1), pp.53–60.

Hoyle, R.H. (1995), *Structural Equation Modeling: Concepts, Issues, and Applications*, Thousand Oaks: Sage Publications.

Hoelter, J.W. (1983), "The Analysis of Covariance Structures: Goodness-of-fit Indices", Sociological *Methods and Research*, 11, 325-344.

Hu, L. & Bentler, P.M. (1999), "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis' Conventional Criteria Versus New Alternatives", *Structural Equation Modeling*, 6(1), pp. 1-55.

Huang, C.D. & Hu, Q. (2007), "Achieving IT-Business Strategic Alignment via Enterprise-Wide Implementation of Balanced Scorecards", *Information Systems Management*, 24(2), 173-184.

Hughes, S.B., Caldwell, C.B. & Gjerde, K.A.P. (2006), "Promoting Investments in Intangible Organizational Assets through Aligned Incentive Compensation Plans", *Management Accounting Quarterly*, 7(4), pp. 1-8.

ISACA (2009), "An Introduction to the Business Model for Information Security", available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/An-Introduction-to-the-Business-Model-for-Information-Security.aspx (accessed 28 October 2010).

(ISC)^2, (2009), *The 2009 State of Cybersecurity from the Federal CISO' Perspective - An (ISC)2 Report*, available at: http://media.haymarketmedia.com/Documents/7/FederalCISOSurveyReport_1638.pdf (accessed 28 October 2010).

(ISC)^2 (2010), International Information Systems Security Certification Consortium (ISC)^2 Certification and Education, available at: https://www.isc2.org/credentials/default.aspx [Accessed December 14, 2010].

ISO (2005), "Information Technology - Security Techniques - Code of Practice for Information Security Management", ISO/IEC 27002.

Kankanhalli, A., Teo, H., Tan, B.C.Y. & Wei, K. (2003), "An Integrative Study Of Information Systems Security Effectiveness", *International Journal of Information Management*, 23 (2), pp.139-154.

Kaplan, R.S. & Norton, D.P. (2007), "Using the Balanced Scorecard as a Strategic Management System", *Harvard Business Review*, 85 (7/8), pp.150-161.

Kelly, D. & Amburgey, T. L. (1991), "Organizational Inertia and Momentum", *The Academy of Management Journal*, 34 (3), pp. 591-612.

Kim, G., (2004), "Does Security Set the Right Goals?", *Security Management*, 48(6), 182.

King, S. (1999), *Organizational Capabilities and Competitive Advantage: Senior Managers' Perceptions of Past Use, Past Payoff, and Future Use*, PhD Dissertation, Connecticut, USA: The University of Connecticut, available at:

http://proquest.umi.com.proxygw.wrlc.org/pqdweb?index=19&did=733962681&SrchMode=1&sid=1&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1296491103&clientId=31812 (accessed 31January 2011).

Kirby, J. (2005), "Toward a Theory of High Performance", *Harvard Business Review*, 83(7/8), pp. 30-39.

Kissel, R., Ed. (2010), "Draft Glossary of Key Information Security Terms", National Institute of Standards and Technology, NIST IR 7298 (Draft), available at: http://csrc.nist.gov/publications/drafts/nistir-7298/draft-nistir-7298-rev1_glossary-key-security-terms.pdf (accessed 2 February 2010).

Klein, A. (2007), "Building an Identity Management Infrastructure for Today...and Tomorrow", *Information Systems Security*, 16, 74-79.

Klein, G., Moon, B. & Hoffman, R.R. (2006), "Making Sense of Sensemaking 1: Alternative Perspectives", *IEEE Intelligent Systems*, 21(4), pp. 70-73.

Kline, R. (2005), *Principles and Practice of Structural Equation Modeling* 2nd ed., New York: Guilford Press.

Knapp, K.J., Marshall, T.E., Rainer, R.K. & Ford, F.N. (2006), "Information Security: Management's Effect on Culture and Policy", *Information Management & Computer Security*, 14 (1), pp. 24-36.

Koskosas, I.V. & Pual, R.J. (2004), "Information Security Management in the Context of Goal-Setting", *Risk Management*, 6(1), pp. 19-29.

Kouzes, J.M. & Posner, B.Z. (2002), *The Leadership Challenge*, 3rd ed., San Francisco, California: John Wiley & Son Inc.

Kruger, H. & Kearney, W. (2006), "A Prototype for Assessing Information Security Awareness", *Computers & Security*, 25(4), pp. 289-296.

Kusunoki, K., Nonaka, I. & Nagata, A. (1998), "Organizational Capabilities in Product Development of Japanese Firms: A Conceptual Framework and Empirical Findings", *Organization Science*, 9 (6), pp. 699-718.

Lattin, J., Carroll, J.D. & Green, P.E. (2003), *Analyzing Multivariate Data*, Pacific Grove CA: Thomson Brooks/Cole.

Leedom, D.K. (2001), "*Final Report: Sensemaking Symposium"*, Vienna, Virginia: Command and Control Research Program (CCRP), available at http://www.dodccrp.org/files/sensemaking_final_report.pdf (accessed 2 February 2010).

MacCallum, R.C., Browne, M.W. & Sugawara, H.M. (1996), "Power Analysis and Determination of Sample Size for Covariance Structure Modeling", *Psychological Methods*, 1(2), pp. 130-149.

March, J.G. & Sutton, R.I. (1997), "Organization Performance as a Dependent Variable", *Organization Science*, 8, pp. 698-706.

Maruyama, G. (1997), *Basics of Structural Equation Modeling*, London: SAGE.

Marsh, H.W., Balla, J.R. & McDonald, R.P. (1988), "Goodness-of-Fit Indexes in Confirmatory Factor Analysis: The Effect of Sample Size", *Psychological Bulletin*, 103(3), pp. 391-410.

McCrimmon, M. (2008), "Leadership and Decision Making", *EzineArticle,*.available at: http://ezinearticles.com/?Leadership-and-Decision-Making&id=903732 (accessed February 4, 2011).

McDonald, R.P. & Ho, M.R. (2002), Principles and Practice in Reporting Structural Equation Analyses, *Psychological Methods*, 7(1), pp. 64-82.

McFadzean, E., Ezingeard, J. & Birchall, D. (2007), "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level", *Online Information Review*, 31 (5), pp. 622-660.

Mitchell, R.J. (1993), Path Analysis: Pollination, pp 211-231 in Schneider, S.M. & Gurevitch, J., Eds, Design and Analysis of Ecological Experiments, NY: Chapman and Hall.

NIST (2003), "Building an Information Technology Security Awareness and Training Program", *National Institute of Standards and Technology Special Publication 800-50*, available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (accessed 28 October 2010).

NIST (2007), "Information Security Guide For Government Executives", *National Institute of Standards and Technology, NISTIR 7359*, available at:

http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf (accessed 28 October 2010).

NIST (2008), "Draft National Institute of Standards and Technology Special Publication 800-39, Information Security - Managing Risk from Information Systems: An Organizational Perspective", available at: http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf (accessed 28 October 2010).

NIST (2010), "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans", *National Institute of Standards and Technology Special Publication 800-53A*, available at: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf (accessed 25 February 2011).

Nyanchama, M. (2005), "Enterprise Vulnerability Management and Its Role in Information Security Management", *Information Systems Security*, 14 (3), pp. 29-56.

ODNI (2008) "Vision 2015: A Globally Networked and Integrated Intelligence Enterprise", Director of National Intelligence, Washington, D.C., available at: www.dni.gov/Vision_2015.pdf (accessed 28 October 2010).

Ohab, J. (2010), "How To: Defining Your Research Questions and Hypotheses", *Armed With Science*, available at: http://science.dodlive.mil/2010/10/04/defining-the-beginning-importance-of-research-questions-hypotheses/ (accessed December 10, 2010).

Park, S. & Ruighaver, T. (2008), "Strategic Approach to Information Security in Organizations", In: *The 2008 International Conference on Information Science and Security*, Seoul, Korea, IEEE Computer Society.

Perla, P.P. et al., 2000. *Gaming and Shared Situational Awareness*, Alexandria, VA: Center for Naval Analyses, available at: http://www.cna.org/documents/D0002722.A2.pdf (accessed 2 January 2011).

Porter, M. (1985), *Competitive Advantage: Creating and Sustaining Superior Performance*, New York; London, Free Press.

Prahalad, C. & Hamel, G. (1990), "The Core Competence of the Corporation", *Harvard Business Review*, 79-91.

PricewaterhouseCoopers (2008), "PWC Global State of Information Security Survey 2008: Improving Security: An Action Plan", available at: http://www.pwc.com/gx/en/information-security-survey/index.jhtml (accessed 28 October 2010).

Pugesek, B. et al., Eds. (2003), *Structural Equation Modeling: Applications in Ecological and Evolutionary Biology*, Cambridge; New York: Cambridge University Press.

Rangone, A. (1999), "A Resource-Based Approach to Strategy Analysis In Small-Medium Sized Enterprises", *Small Bus. Econ.*, 12, pp. 223–248.

Rathnam, R.G., Johnsen, J. & Wen, H.J. (2004), "Alignment of Business Strategy and IT Strategy: A Case Study of a Fortune 500", *The Journal of Computer Information Systems*, 45(2), 1-8.

Reinard, J. (2006), *Communication Research Statistics*, Thousand Oaks Calif.: SAGE Publications.

Reymann (2007), "Strategic Alignment of IT & Security - Yield Compliance by Default", available at: http://www.tracesecurity.com/docs/whitepapers/WP_Strategic-Alignment-of-IT-Security_Reymann-Group.pdf, (accessed 28 October 2010).

Rezgui, Y. & Marks, A. (2008), "Information Security Awareness in Higher Education: An Exploratory Study", *Computers & Security*, 27(7-8), pp. 241-253.

Richard, P.J, Yip, G.S., & Johnson, G. (2009), "Measuring Organizational Performance: Towards Methodological Best Practice", *Journal of Management*, 35(3), pp. 719-804.

Salkind, N. (2009), *Exploring Research* 7th ed., Upper Saddle River N.J.: Pearson/Prentice Hall.

Saugatuck Technology (2008), "Enterprise Information Management for Competitive Advantage", available at: http://www.synaptica.com/djcs/synaptica/Enterprise%20Information%20Mgmt_DJWhitepaper033108.pdf (accessed 28 October 2010).

Schreiber, J.B. (2008), "Core Reporting Practices in Structural Equation Modeling", *Research in Social and Administrative Pharmacy*, 4, pp. 83-97.

Schreiber, J.B. et al. (2006), "Reporting Structural Equation Modeling and Confirmatory Factor Analysis Results: A Review", *The Journal of Educational Research*, 99(6), pp.323-337.

Schultz, E. (2006), “The Changing Winds of Information Security”, *Computers & Security*, 25(5), pp. 315-316.

Schumacker, R.E. & Lomax, R.G. (2004), *A Beginner's Guide to Structural Equation Modeling* 2nd ed., Mahwah N.J.: Lawrence Erlbaum Associates.

Siponen, M.T. (2000), “A Conceptual Foundation for Organizational Information Security Awareness”, *Information Management & Computer Security*, 8(1), pp. 31-41.

Siponen, M.T. (2001), “Five Dimensions Of Information Security Awareness”, *ACM SIGCAS Computers and Society*, 31(2), pp. 24–29.

Slater, S.F. & Olson, E.M. (2001), “Marketing's Contribution to The Implementation Of Business Strategy: An Empirical Analysis”, *Strategic Management Journal*, 22(11), 1055-1067.

Smallwood, N. & Panowyk, M. (2005), “Building Capabilities”, *Leadership Excellence*, 22 (1), p. 17.

Stalk, G., Evans, P. & Shuman, L.E. (1992), “Competing on Capabilities: The New Rules of Corporate Strategy”, *Harvard Business Review*, 70 (2), pp. 54-66.

Steiger, J.H. (1998), “A Note on Multiple Sample Extensions of the RMSEA Fit Index”, *Structural Equation Modeling*, 5(4), pp. 411-419.

Stevens, S (1946), “On the Theory of Scales of Measurement”, *Science*, 103, pp. 677-680.

Straub, D.W. (1990), "Effective IS Security: An Empirical Study", *Information Systems Research*, 1 (3), pp. 255-276.

Straub D.W. & Welke R.J. (1998), "Coping With Systems Risk: Security Planning Models For Management Decision Making", *MIS Quarterly*, 22(4), pp. 441–69.

Symantec (2009), "Symantec Internet Security Threat Report Trends for 2008", available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (accessed 28 October 2010).

Tallon, P.P., Kraemer, K.L. & Gurbaxani, V. (2000),"Executives' Perceptions Of The Business Value Of Information Technology: A Process-Oriented Approach", *Journal of Management Information Systems*, 16 (4), pp. 145-173.

Tanaka, J.S. (1993), "Multifaceted Conceptions of Fit in Structural Equation Models", in Bollen, K. A. & Long, J. S (Eds.), *Testing Structural Equation Models*, Newbury Park, California [etc.]: SAGE Publications, pp. 10-39.

TechAmerica (2009),"Nineteenth Annual Survey of Federal Chief Information Officers", available at: <http://www.techamerica.org/techamerica-and-grant-thornton-release-19th-annual-survey-of-federal-cios> (accessed 28 October 2010).

Teece, D.J., Pisano, G. & Shuen, A. (1997), "Dynamic Capabilities and Strategic Management", *Strategic Management Journal*, 18(7), pp. 509-533.

Thomson, M. & Solms, R.V. (1998), "Information Security Awareness: Educating Your Users Effectively", *Information Management & Computer Security*, 6(4), pp. 167-173.

Tomarken, A.J. & Waller, N.G. (2005), Structural Equation Modeling: Strengths, Limitations, and Misconceptions, *Annual Review of Clinical Psychology*, 1(1), pp. 31-65.

Ulrich, D. & Lake, D. (1991), "Organizational Capability: Creating Competitive Advantage", *Academy of Management Executive,* 5 (1), pp. 77-92.

Ulrich, D. & Smallwood, N. (2004), "Capitalizing on Capabilities", *Harvard Business Review*, 82 (6), pp. 119-127.

Urbach, N. & Ahlemann, F. (2010), "Structural Equation Modeling in Information Systems Research Using Partial Least Squares", *Journal of Information Technology Theory and Application*, 11(2), pp. 5-40.

Valluzzi, J.L., Larson, S.L. & Miller, G.E. (2003), Indications and Limitations of Structural Equation Modeling in Complex Surveys: Implications for an Application in the Medical Expenditure Panel Survey (MEPS), in *2003 Joint Statistical Meetings - Section on Survey Research Methods*. 2003 Joint Statistical Meetings, San Francisco, California, pp. 4345-4352, available at: http://www.amstat.org/sections/srms/proceedings/y2003/Files/JSM2003-000198.pdf (accessed 13 January 2011).

Van Opstal, D. & Council on Competitiveness (2007), "The Resilient Economy: Integrating Competitiveness and Security", *Council on Competitiveness*, available at: http://www.compete.org/images/uploads/File/PDF/Files/Transform_The_Resilient_Economy_FINAL_pdf.pdf (accessed 28 October 2010).

Von Solms, B. (2006), "Information Security – The Fourth Wave", *Computers & Security*, 25 (3), pp. 165-168.

Warner, R. (2008), *Applied Statistics: From Bivariate Through Multivariate Techniques*, Los Angeles: SAGE Publications.

Weick, K.E., Sutcliffe, K.M. & Obsfeld, D. (2005), "Organizing and the Process of Sensemaking", *Organization Science*, 16(4), pp. 409-421.

Werlinger, R., Hawkey, K. & Beznosov, K. (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management", *Information Management & Computer Security*, 17 (1), pp. 4-19.

Wernerfelt, B. (1984), "A Resource-Based View of the Firm", *Strategic Management Journal*, pp. 171–180.

Wethyavivorn, P., Charoenngam, C. & Teerajetgul, W. (2009), "Strategic Assets Driving Organizational Capabilities of Thai Construction Firms", *Journal of Construction Engineering and Management*, 135 (11), pp. 1222-1231.

Wheaton, B., Muthen, B., Alwin, D. & Summers, G. (1977), "Assessing Reliability and Stability in Panel Models, Sociological Methodology, 8(1), pp. 84-136.

Willis, G. (2005), *Cognitive Interviewing: A Tool for Improving Questionnaire Design*, Thousand Oaks Calif.: Sage Publications.

Wilson, M. & Stine, K. & Bowen, P. (2009), "Information Security Training Requirements: A Role- and Performance-Based Model (Draft), Recommendations of the National Institute of Standards and Technology", *National Institute of Standards and Technology Special Publication 800-16*, Revision 1 (Draft), available http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf (accessed 28 October 2010).

Wood, C.C. (1991), "Using Information Security to Achieve Competitive Advantage", *Computers & Security*, 10 (5), pp. 399-404.

Wood, C.C. (1993), "Achieving Competitive Advantage with Information Security", *Managerial Auditing Journal*, 8 (2), pp. i-iv.

APPENDIX A

SURVEY PRETEST FINDINGS

Table A1.

Pretest Findings, Observations and Revision Decisions

Section/ Question	Finding/Observation	Decision/Rationale
Cover Letter	Upon retrospective probing, six respondents expressed difficulties in understanding what the term "pre-condition" meant, while remaining participants indicated no problems with the language itself.	Deleted the word "pre-condition" in "…shed insight on the essential "pre-condition" or capabilities of an organization…", as it didn't seem to provide any value added but only confused respondents. By doing this, the sentence was rid of the unnecessary concept while keeping it short and to the point. The longer the statement, the more information respondents have to take in and process and the higher the likelihood for misunderstanding or misreading, and in turn could turn respondents off (Dillman et al. 2009).
Survey Overview	When asked whether a "don't know" option is necessary for questions in this section, eight respondents stated that it was not necessary as the	No changes were necessary. Among the two non-information security participants, a total of 9 "Neutral" was selected out of 74 possible options, representing an average of only 1.2% of the total. In addition, all

Section/ Question	Finding/Observation	Decision/Rationale
	"neutral" response sufficed for a "I don't know" response and was self-explained. While the remaining two participants indicated that there should be an instruction that if a respondent doesn't know an answer then check the neutral option.	participants indicated during the retrospective session that they didn't feel any burdens when answering the questions, and were able to answer all questions. Therefore, no changes were deemed necessary. Furthermore, the intended population for the survey consisted of only information security professionals who are expected to have clear answers to these questions, thus the current answer categories and instruction are sufficient.
11. Inspires workforce collaboration to protect business assets from information security attacks.	A participant desired a simpler word in lieu of "Inspires".	Changed "Inspires" to "Promotes". One way to establish legitimacy and credibility with respondents was to present them with a formalized and professional questionnaire. However, there were instances when efforts to formalize the questionnaire may lead to the use of complex words and wordy phrases (Dillman et al. 2009). This question fell under those instances. It was reasonable to replace "inspires" with an easily understood

Section/ Question	Finding/Observation	Decision/Rationale
		word such as “promotes”.
14. Deploys an integrated combination of competencies and resources to protect information assets. *(Competencies refer to knowledge, skill, and ability needed to perform a specific task.)*	One participant took a little longer than normal to answer this question. When asked during the probing session, this participant explained that the italic text was a little difficult to read.	Increased the font size. This question contained two parts: the question stem and a note used to define a term in this question. The design property of contrast was used to create separation between the question stem and the note. To create differences in contrast, the note was italicized and used smaller font. However, this small italic text seemed to create burdens for some respondents. Increasing the size of the italic text in the note would improve readability of respondents while reserving the differentiation of the two parts of the question (Dillman et al. 2009).
44. What security certification, if any, do you have? *[Select all that apply]* □ CAP □ CISA	Two participants who were not information security professionals checked the “Other” option then wrote in “None”. Upon probing, these participants stated	Two changes were deemed necessary. First was to add a “None” response category. This question contained an embedded assumption of having a security certification that may not be true for all information security professional. Adding a “None”

Section/ Question	Finding/Observation	Decision/Rationale
□ CISSP □ CISSLP □ SSCP □ Other	they didn't have any information security certification but didn't see an appropriate answer choice. One of these respondents proposed adding a "None" response option. One participant suggested in the comment section that CISA be added "to the list since it is a recognized DOD certification.	response category option would ensure this question would be applied to all respondents. Second was to add a substantive response category. CISA was a reasonable option that the researcher mistakenly omitted. Every question should include all reasonable possible answers so that every respondent can find an applicable answer (Dillman et al. 2009). Adding this answer category would minimize the chances that respondents skip questions at will (Dillman et al. 2009).
45. Do your job duties directly involve information security? *[Select one]* □ Yes □ No	Six participants selected "Yes". Four selected "No", but two of them also added the word "Indirectly" immediately following the "No" answer. Upon probing, the participants who were not information security professionals indicated that although they did not earn any security	Two changes were implemented. First was to revise the question to "Do your job duties directly or indirectly involve information security". This ensured a technically accurate question that would be applicable to all respondents. Asking a question that was not technically accurate can confuse respondents and make responding task difficult (Dillman et al. 2009). Second was to change the response options from "Yes/No" to

Section/ Question	Finding/Observation	Decision/Rationale
	certification, their job duties indirectly involved information security.	three separate answer categories, i.e., "Directly involve", "Indirectly involve", "Not involve at all", to match the question stem. Changing the answer options allowed a more comprehensive analysis of the level of involvement in information security of respondents (Dillman et al. 2009).
48. Which of the following best describes the approximate total number of people who work in your organization? *[Select one]* □ Less than 100 □ 100-499 □ 500-999 □ 1000-4,999 □ 5,000-9,999 □ 10,000 or more	One participant marked the box "5,000-9,999", but also wrote in "Don't know". Upon probing, this participant indicated that she marked the answer "5,000-9,999", although she was unsure of the accuracy of her answer. Two were left blank.	Offered an additional option, "Don't know", as some respondents may not be able to answer. Although answers of this type are wasted answers as far as the researcher is concerned, but are necessary alternatives to avoid frustrated respondents. Sometimes a "Don't Know" response represents the respondent's most honest answers to some of the questions (Dillman et al. 2009). Respondents who feel they are being coerced into giving an answer they do not want to give often do not complete the questionnaire (Dillman et al. 2009).

APPENDIX B

IRB EXEMPT APPROVAL

THE GEORGE WASHINGTON UNIVERSITY & MEDICAL CENTER
OFFICE OF HUMAN RESEARCH
INSTITUTIONAL REVIEW BOARD

EXEMPT FROM IRB REVIEW REQUEST FORM

Before completing this form, complete the Human Subject Research Determination worksheet to ensure that you are in fact required to submit your new study to the Office of Human Research. The OHR will only review studies deemed "human subject research."

INVESTIGATOR AND TEAM CONTACT INFORMATION			
IRB# *(ADMIN USE ONLY—WILL BE ASSIGNED UPON SUBMISSION)*	011012	**VERSION DATE:**	December 27, 2009
TYPE OF HIPAA AUTHORIZATION REQUESTED:		Not applicable	

PROTOCOL TITLE AND SPONSOR:
TITLE : Moderating Roles Of Organizational Capabilities Affecting Information Security Strategy Effectiveness: A Structural Equation Modeling Analysis
SPONSOR : Unfunded

PRINCIPAL INVESTIGATOR INFORMATION *(MUST BE GWU FACULTY)*				
LAST NAME:	SARKANI	**FIRST NAME:**	SHAHRAM	Degree: PH.D.
DEPARTMENT	EMSE	**SCHOOL:**	SEAS	
CAMPUS ADDRESS:	EMSE OFF-CAMPUS PROGRAMS			
PHONE:	757-269-2211	**EMAIL:**	emseocp@gwu.edu	

PRINCIPAL CONTACT IF OTHER THAN PI: *(THIS MAY BE THE STUDENT/TRAINEE)*			
LAST NAME:	HALL	**FIRST NAME:**	JACQUELINE
CAMPUS ADDRESS:	EMSE OFF-CAMPUS PROGRAMS		
PHONE:		**EMAIL:**	

Recommendation:

☒ Study Registered as Exempt. Category: 2

☐ A HIPAA waiver of research subject authorization is justified for this study under 45 CFR 46 164.512 based on the following criteria:
1. The proposed uses and disclosures of protected health information (PHI) involve no more than minimal risk to the privacy of individuals.
2. The research could not practicably be conducted without the waiver.
3. The research could not practicably be conducted without access to and use of the PHI.

Please obtain permission from the privacy officer of the health care organization in which you will access protected health information before beginning your research.

☐ This research does **NOT** meet the regulatory/institutional requirements for exemption from IRB review. To conduct this research you must complete an IRB submission package for IRB review. For more information on completing a research submission, contact OHR at 202-994-2715.

MARIA ROCHELLE S. COLANTES — Authorized Designee
Signature
4/30/2010 — Date

This Exempt Registration does not expire nor does it require renewal.

Reporting Proposed Changes in Research

This exempt from IRB review determination only applies to this form/protocol, as currently proposed. Therefore, if there are any changes that increase the risk to subjects (e.g., methodology, data gathering instruments, type of information being accessed or disclosed, etc.) the changes must be submitted to the IRB/OHR for approval *PRIOR TO* implementation.

'10 JAN 14 AM 11:57

APPENDIX C

SURVEY COVER LETTER

Invitation to Participate in Dissertation Research Survey

A Survey of Organizational Capabilities Affecting Information Security Effectiveness

December 27, 2009

Dear Information Security Professional:

I am a doctoral student at The George Washington University, School of Engineering and Applied Science. As part of my doctoral work, I am conducting a study to examine the effect of organizational capabilities on information security strategy and organizational performance. Hopefully, results from this survey will yield practical value for business management and shed insight on the essential capabilities of an organization that most influence the effective implementation of information security strategy. Additionally, there is a lack of empirical research that examines the impact of organizational capabilities in information security. Therefore, I'm writing to invite you to participate in my study to further our knowledge in this area.

Your name was selected at random from the International Information Systems Security Certification Consortium (ISC)² member directory. Inputs from information security professionals like you, who may have strong background and years of experience in information technology/information security, are crucial to the success of this important research project.

Your participation involves completing the enclosed self-administered questionnaire and some basic demographic information. The survey will take approximately 15-20 minutes to complete. Your participation in this survey is voluntary and greatly appreciated. **Please return the completed survey in the enclosed postage-paid, preaddressed envelope no later than *MMDDYYYY.***

Each survey will be assigned an arbitrary number for tracking purposes. Despite this tracking number, your responses and any comments you may have will be treated with utmost confidentiality. Information will be reported in an aggregated form, without identifying you or your organization. The results of all returned surveys will be published as a doctoral dissertation and in academic journals or trade publications. If you would like to receive a copy of the survey results, please provide your email address in the space provided on the last page of the survey form.

If you have any questions or comments concerning this study, please contact me by phone at [redacted] or email at hallj@gwmail.gwu.edu, or my dissertation advisor, Dr. Shahram Sarkani, at [redacted]

I look forward to receiving your responses. Please know that the information you provide is essential to the body of knowledge in understanding the effect of organizational capabilities on an organization's drive toward using information security to create business value.

Thank you in advance for participating in my research.

Sincerely,

Jacqueline H. Hall

Jacqueline H. Hall
School of Engineering and Applied Science
George Washington University

APPENDIX D

SURVEY INSTRUMENT

DISSERTATION RESEARCH SURVEY

SECTION 1 – INFORMATION SECURITY QUESTIONS

PART A – ORGANIZATIONAL CAPABILITIES

Please indicate the extent to which your organization has currently implemented the following capabilities by filling in the appropriate circle.

Each item is measured by a 5-point scale, in which 1 means "No Extent" and 5 means "Great Extent".

1 No Extent	2 Little Extent	3 Some Extent	4 Moderate Extent	5 Great Extent

Sense-making					
The organization I work for …	1	2	3	4	5
1. Assesses the environmental impacts (i.e., social, political and economical) on information security	☐	☐	☐	☐	☐
2. Uses a systematic process to identify potential adversary actions or reactions.	☐	☐	☐	☐	☐
3. Analyzes available information to determine risks to the enterprise.	☐	☐	☐	☐	☐
4. Keeps current on the evolving capabilities of attackers and potential attackers.	☐	☐	☐	☐	☐
5. Keeps decision makers informed of vital information security developments.	☐	☐	☐	☐	☐
6. Provides appropriate security education and awareness on information assets protection.	☐	☐	☐	☐	☐
Decision-making					
The leadership within the organization I work for…	1	2	3	4	5
7. Aligns information security objectives with the overall business goals.	☐	☐	☐	☐	☐
8. Illustrates clear intention to support information security initiatives.	☐	☐	☐	☐	☐
9. Links organizational governance structure to information security governance to provide consistency in planning, implementing, and delivering security in the organization.	☐	☐	☐	☐	☐
10. Commits appropriate resources to achieve information security objectives.	☐	☐	☐	☐	☐
11. Promotes workforce collaboration to protect business assets from information security attacks.	☐	☐	☐	☐	☐
12. Takes measures to build a more competent enterprise that can defend business against increasingly sophisticated information security threats.	☐	☐	☐	☐	☐
13. Communicates clear vision to mitigate information security risks.	☐	☐	☐	☐	☐
Competencies					
The organization I work for…	1	2	3	4	5
14. Deploys an integrated combination of competencies and resources to protect information assets. *(Competencies refer to knowledge, skill, and ability needed to perform a specific task.)*	☐	☐	☐	☐	☐
15. Recruits people with appropriate information security competencies.	☐	☐	☐	☐	☐
16. Retains a cadre of trained information security professionals.	☐	☐	☐	☐	☐
17. Uses formal mechanisms such as training, policies, procedures, processes and technologies to ensure a secure, reliable, responsive, and trusted information technology environment.	☐	☐	☐	☐	☐
18. Uses formal mechanisms such as policies, procedures, processes and technologies to enforce information security compliance.	☐	☐	☐	☐	☐
19. Implements necessary procedures to ensure effective configuration management of all changes to information related systems.	☐	☐	☐	☐	☐
20. Ensures continuity of mission-critical operations through contingency planning.	☐	☐	☐	☐	☐
21. Reviews information security policy regularly to ensure its adequacy.	☐	☐	☐	☐	☐
22. Provides a balance between security controls and access to information.	☐	☐	☐	☐	☐

PART A (Continued)

1 No Extent	2 Little Extent	3 Some Extent	4 Moderate Extent	5 Great Extent

Operations Management

The organization I work for …	1	2	3	4	5
23. Assigns all security controls needed to protect the mission/business processes to responsible parties with accountability for development, implementation, and assessment.	☐	☐	☐	☐	☐
24. Uses project management best practices to manage information security programs.	☐	☐	☐	☐	☐
25. Uses metrics to identify the achieved security performance in its operational environment.	☐	☐	☐	☐	☐
26. Uses metrics to increase accountability through the collection, analysis, and reporting of relevant performance-related data.	☐	☐	☐	☐	☐
27. Uses metrics to facilitate decision making.	☐	☐	☐	☐	☐
28. Documents incidents to provide lessons learned that help modify information security strategy.	☐	☐	☐	☐	☐

PART B - INFORMATION SECURITY STRATEGY

Please indicate the effectiveness of each of the following aspects of your organization's information security strategy by filling in the appropriate circle.

Each item is measured by a 5-point scale, in which 1 means "Very Ineffective" and 5 means "Very Effective".

1 Very Ineffective	2 Somewhat Ineffective	3 Neutral	4 Somewhat Effective	5 Very Effective

Over the last two years, the organization I work for …	1	2	3	4	5
29. Maintains appropriate protection of information assets.	☐	☐	☐	☐	☐
30. Achieves information security compliance with legislation, regulatory or industry requirements.	☐	☐	☐	☐	☐
31. Upholds information security policies and standards.	☐	☐	☐	☐	☐
32. Responds promptly to information security attacks.	☐	☐	☐	☐	☐
33. Recovers quickly following system failure or interruption.	☐	☐	☐	☐	☐
34. Keeps information security risks to a minimum.	☐	☐	☐	☐	☐
35. Sustains continuity of mission-critical operations.	☐	☐	☐	☐	☐
36. Prevents damages to information assets.	☐	☐	☐	☐	☐
37. Allows for better control of information assets.	☐	☐	☐	☐	☐

PART C - ORGANIZATION PERFORMANCE

Please indicate the extent to which you agree or disagree with the following aspects of your organization's performance by filling in the appropriate circle.

Each item is measured by a 5-point scale, in which 1 means "Strongly Disagree" and 5 means "Strongly Agree".

1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree

Over the last two years, the organization I work for …	1	2	3	4	5
38. Increases customer trust.	☐	☐	☐	☐	☐
39. Prevents costly legal action from government agencies, stockholders, or others.	☐	☐	☐	☐	☐
40. Preserves public's perception of brand strength or company reputation.	☐	☐	☐	☐	☐
41. Improves customer service.	☐	☐	☐	☐	☐
42. Preserves market valuation.	☐	☐	☐	☐	☐
43. Maintains business resiliency in the face of a constantly changing risk environment	☐	☐	☐	☐	☐

SECTION 2 – DEMOGRAPHIC QUESTIONS

This section contains seven questions used to compare the demographic distributions among information security professionals. Please respond to each question by filling in the appropriate circle.

44. What security certification, if any, do you have? *[Select all that apply]*

o CAP o CCP o CISA o CISSP o CPP o SSCP
o None
o Other (please specify): _____

45. Do your job duties directly or indirectly involve information security?

o Directly involve
o Indirectly involve
o Do not involve at all

46. How many years of experience do you have in information technology/information security?

o Less than 5 years
o Between 5-8 years
o Between 8-15 years
o More than 15 years

47. Which of the following best describes your current job function?

o Architecture and Engineering
o Budget, Finance or Accounting
o Human Resources
o Management /Strategic Planning
o Information Technology/Information Security
o Operations or Production
o Sales and Marketing
o Other (please specify): _____

48. Which one of the following best describes your organization?

o Aerospace/ Engineering
o Agriculture/Chemicals
o Consumer Products/Retail/Wholesale/Distributor
o Education/Training
o Energy/Utilities
o Government/Non-profit (Federal, state, local, military, police, etc.)
o Healthcare/Medical/Pharmaceuticals
o Information, Communications and Technology
o Insurance/Financial/Banking Services
o Manufacturing/Industrial
o Oil/Gas/Consumable Fuels
o Real Estate Services
o Transportation/Warehousing/Logistics
o Other (please specify): _____

PART 2 (Continued)

49. Which of the following best describes the approximate total number of people who work in your organization?

- o Less than 100
- o 100 - 499
- o 500 - 999
- o 1,000 - 4,999
- o 5,000 - 9,999
- o 10,000 - 14,999
- o 15,000 or more

50. Which of the following ranges best describes the approximate annual revenues of your organization?
(For government, educational and non-profit institutions please use your organization's operating budget, that is, its annual expenditures.)

- o Less than $1 million
- o $1 million - $4.99 million
- o $5 million - $9.99 million
- o $10 million - $49.99 million
- o $50 million - $99.99 million
- o $100 million - $499.99 million
- o $500 million - $999.99 million
- o $1 billion or more
- o Don't know

If you would like to receive a copy of the survey results, please provide your email address below:

_____

Please share any additional thoughts about any of the above topics or the survey itself in the space provided below.

Please return the completed survey in the enclosed self-addressed stamped envelope.

Jacqueline H. Hall

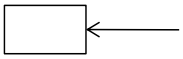
Thanks again for completing the survey!

APPENDIX E

PATH DIAGRAM NOTATIONS

Table E1.

Summary of Path Diagram Notations

	Observed Variable, Measured Variable, Indicator
	Latent Variable, Unobserved Variable, Construct, Factor
	Causal Relationship
	Correlation, Covariance
	Residual to a Variable

APPENDIX F

ASSESSMENT OF NORMALITY

Table F1.

Univariate Skewness and Kurtosis Descriptive Statistics (N=428)

	Skewness			Kurtosis		
	Statistic	Standard Error	Standard Value	Statistic	Standard Error	Standard Value
SM2	-.315	.118	-2.671	-.836	.235	-3.550
SM3	-.790	.118	-6.700	-.120	.235	-.511
SM4	-.825	.118	-6.993	.090	.235	.382
SM5	-.560	.118	-4.746	-.456	.235	-1.937
SM6	-.480	.118	-4.071	-.648	.235	-2.753
DM1	-.328	.118	-2.779	-.659	.235	-2.799
DM2	-.547	.118	-4.633	-.658	.235	-2.796
DM3	-.154	.118	-1.306	-1.006	.235	-4.273
DM4	-.108	.118	-0.916	-.831	.235	-3.531
DM5	-.168	.118	-1.428	-.887	.235	-3.769
DM6	-.394	.118	-3.340	-.664	.235	-2.822
DM7	-.175	.118	-1.485	-.830	.235	-3.525
OA1	-.518	.118	-4.392	-.571	.235	-2.425
OA2	-.398	.118	-3.373	-.681	.235	-2.892
OA3	-.399	.118	-3.379	-.858	.235	-3.644
OA4	-.424	.118	-3.591	-.621	.235	-2.638
OA5	-.568	.118	-4.817	-.483	.235	-2.051
OA6	-.368	.118	-3.119	-.591	.235	-2.509
OA7	-.595	.118	-5.045	-.262	.235	-1.114

	Skewness			Kurtosis		
	Statistic	Standard Error	Standard Value	Statistic	Standard Error	Standard Value
OM2	-.123	.118	-1.042	-.719	.235	-3.053
OM3	-.166	.118	-1.406	-.787	.235	-3.342
OM4	-.027	.118	-0.226	-.919	.235	-3.903
OM5	-.084	.118	-0.708	-.866	.235	-3.677
OM6	-.489	.118	-4.144	-.513	.235	-2.180
IS1	-.780	.118	-6.612	.086	.235	.367
IS2	-1.003	.118	-8.502	.565	.235	2.399
IS3	-.822	.118	-6.964	.248	.235	1.054
IS4	-1.159	.118	-9.820	.864	.235	3.669
IS5	-.752	.118	-6.375	.067	.235	.285
IS6	-.556	.118	-4.709	-.462	.235	-1.961
IS7	-.993	.118	-8.415	.606	.235	2.572
IS8	-.761	.118	-6.450	.149	.235	.634
IS9	-.399	.118	-3.381	-.316	.235	-1.343
OP1	-.522	.118	-4.421	-.174	.235	-.739
OP2	-.536	.118	-4.544	-.063	.235	-.269
OP3	-.758	.118	-6.425	.238	.235	1.010
OP4	-.477	.118	-4.045	-.326	.235	-1.384
OP5	-.193	.118	-1.635	-.455	.235	-1.933
OP6	-.646	.118	-5.478	.127	.235	.538

APPENDIX G

ADDITIONAL SEM ANALYSIS OUTPUTS

Table G1.

Squared Multiple Correlations of the Fitted Model

Variable	Estimate	Variable	Estimate
IS	0.75	OM2	0.49
OP	0.54	OM3	0.81
SM2	0.53	OM4	0.85
SM3	0.69	OM5	0.77
SM4	0.57	OM6	0.50
SM5	0.54	IS1	0.68
SM6	0.60	IS2	0.51
DM1	0.61	IS3	0.65
DM2	0.64	IS4	0.53
DM3	0.67	IS5	0.42
DM4	0.62	IS6	0.72
DM5	0.67	IS7	0.50
DM6	0.66	IS8	0.64
DM7	0.73	IS9	0.67
OA1	0.73	OP1	0.63
OA2	0.52	OP2	0.59
OA3	0.60	OP3	0.69
OA4	0.68	OP4	0.60
OA5	0.63	OP5	0.63
		OP6	0.67

Table G2.

Covariances of the Fitted Model

Variable		Variable	Estimate	Standard Error	Critical Ratio	*P*
SM	<-->	DM	.631	.063	9.993	***
DM	<-->	OA	.705	.064	11.060	***
OA	<-->	OM	.530	.055	9.580	***
DM	<-->	OM	.499	.053	9.438	***
SM	<-->	OM	.477	.054	8.856	***
SM	<-->	OA	.680	.066	10.261	***
e_is8	<-->	e_is7	.121	.021	5.810	***
e_sm6	<-->	e_sm3	-.119	.027	-4.416	***
e_sm5	<-->	e_sm4	.077	.028	2.791	.005
e_dm2	<-->	e_dm1	.192	.030	6.495	***
e_dm7	<-->	e_dm6	.092	.024	3.899	***
e_dm6	<-->	e_dm5	.099	.025	3.909	***
e_cs4	<-->	e_cs5	.142	.026	5.481	***
e_op5	<-->	e_op4	.091	.020	4.471	***
e_is1	<-->	e_is2	.076	.020	3.910	***
e_is5	<-->	e_is4	.136	.024	5.615	***
e_is8	<-->	e_is9	.077	.017	4.449	***
e_is2	<-->	e_is3	.104	.021	4.952	***
e_cs3	<-->	e_cs2	.316	.039	8.121	***
e_op6	<-->	e_op3	-.058	.018	-3.182	.001
e_om2	<-->	e_om4	-.090	.025	-3.668	***
e_is5	<-->	e_is7	.056	.022	2.612	.009
e_cs3	<-->	e_cs4	.066	.021	3.179	.001

Note: *** p< .001 (two-tailed)

Table G3.

Correlations of the Fitted Model

Variable		Variable	Estimate
SM	<-->	DM	.833
DM	<-->	OA	.877
OA	<-->	OM	.743
DM	<-->	OM	.765
SM	<-->	OM	.710
SM	<-->	OA	.822
e_is8	<-->	e_is7	.316
e_sm6	<-->	e_sm3	-.292
e_sm5	<-->	e_sm4	.161
e_dm2	<-->	e_dm1	.399
e_dm7	<-->	e_dm6	.232
e_dm6	<-->	e_dm5	.222
e_cs4	<-->	e_cs5	.359
e_op5	<-->	e_op4	.272
e_is1	<-->	e_is2	.207
e_is5	<-->	e_is4	.304
e_is8	<-->	e_is9	.247
e_is2	<-->	e_is3	.270
e_cs3	<-->	e_cs2	.514
e_op6	<-->	e_op3	-.211
e_om2	<-->	e_om4	-.253
e_is5	<-->	e_is7	.121
e_om2	<-->	e_om6	.074
e_cs3	<-->	e_cs4	.142

Table G4.

Variances of the Fitted Model

Variable	Estimate	Standard Error	Critical Ratio	*P*
SM	.780	.092	8.506	***
DM	.735	.078	9.424	***
OA	.879	.082	10.657	***
OM	.578	.073	7.907	***
D	.161	.020	8.127	***
E	.267	.030	8.907	***
e_is1	.314	.025	12.515	***
e_is2	.433	.032	13.692	***
e_is3	.340	.027	12.695	***
e_is8	.325	.026	12.738	***
e_is6	.307	.025	12.077	***
e_is5	.483	.034	13.994	***
e_is4	.412	.031	13.465	***
e_is7	.453	.033	13.838	***
e_sm6	.522	.045	11.496	***
e_sm5	.515	.040	12.831	***
e_sm4	.449	.036	12.639	***
e_sm3	.317	.031	10.197	***
e_sm2	.680	.052	12.965	***
e_dm7	.366	.031	11.830	***
e_dm2	.491	.039	12.677	***
e_dm6	.431	.035	12.236	***

Variable	Estimate	Standard Error	Critical Ratio	*P*
e_dm5	.461	.037	12.550	***
e_dm4	.479	.037	13.009	***
e_dm3	.480	.039	12.365	***
e_dm1	.473	.037	12.891	***
e_cs3	.585	.047	12.381	***
e_cs2	.645	.050	12.978	***
e_cs1	.328	.031	10.416	***
e_cs4	.374	.032	11.507	***
e_cs5	.420	.035	12.006	***
e_om2	.613	.047	13.099	***
e_om3	.251	.023	10.895	***
e_om4	.206	.022	9.178	***
e_om5	.316	.027	11.585	***
e_om6	.634	.047	13.570	***
e_op1	.342	.028	12.062	***
e_op6	.289	.026	10.989	***
e_op5	.303	.025	12.198	***
e_op4	.366	.029	12.571	***
e_op3	.257	.024	10.715	***
e_op2	.353	.028	12.756	***
e_is9	.299	.024	12.509	***

Note: ***p<.001 (two-tailed)

APPENDIX H

FEEDBACK FROM RESPONDENTS

Respondent's Optional Comment
In the last 10 years in the government I have seen the trend to enforce information security to the extent that it is now decreasing workers ability to do their job in a timely & effective manner. I am a proponent of IS but believe there are reason to not enforce all rules. For example, in [my organization] no user can add a printer to their system. This slows down user productivity while they wait for an IT person to fix it on an unclassified system. This is a wasted security precaution.
It would be interesting to correlate ITIL, PRINCEL, or Cobit adoption with their result.
There is a risk of skewing the data by focusing only on a single point of operations. It's like throwing a dart at the list of 100 functions the company performs to decide "what is most important" today. Outside of the few companies who sell security related products, nobody "does" security because it is the most important thing. A business must pay its bills, which comes from selling its goods or services at a profit. Without profit, the business must close its doors. Security for most companies is a necessary cost of doing business, but not the objective.
In my humble opinion, the information security professional community is just beginning to realize the importance of information to the business enterprise and most importantly determining methods to metrically measure and manage for a continuous improvement model. Additionally, we have very little knowledge of the risk/threat environment.
Costs of implementation of IA controls might have been addressed in survey. Cost/benefit analyses are critical as the costs of information security should be considered. Good luck!
You need to address the "appropriate" level of security - you don't want to "overspend" but based on risk's best practices to respond at a correct, but not over-

aggressive level.
Would be interesting to see a companion of IS strategy and execution effectiveness versus IS communication effectiveness.
In large companies, the drive is there to bring security to a high awareness. Smaller companies are significant less driven to have info security at any level of awareness. Unless there is a contract requiring awareness, then there is a rush.
Some key trends that are gaining significance are the use of metrics and the impact of regulatory changes (real or expected).
The key challenge for security in my company stems from an organization structure that is focused on cost cutting and has conflicts of interested. Security doesn't get visibility unless something bad happens. Security and Audit departments report to Operations and don't have influence with the executives. Our VP of Operations has the attitude that "We sell green beans, why would a hacker target us" and has pillaged our budgets for years.
Since I work in a Government environment we are governed by many regulations so I would be curious to see the results of this survey for non-government entities.
Size and type of the company matters when information security governance and support are implemented and provided. In private (non-public) company (midsize - small) is really difficult to apply security best practices rather than in big enterprises and regulated industries.
Perhaps it would be nice to include option for an organization that is improving in an area or areas that need improvement. For an organization as large as the one I work for, there are many levels where decisions are made where improvements can be made, but this survey does not account for this. Also certifications are nice, but what about asking about college education where IT skills are also taught or developed.

Interesting data could possibly have been gathered if there were 3-5 questions about organization's security management practices' impact by economic downturn.
This has been designed with a med-large org in mind. I work for a small company that consults on behalf of med-large companies. I answered these questions with my small org in mind, rather than my customers.
We're very driven by regulations and regulatory requirements. Best practice is often to cost justify.
Reliability is important to security. Network layers have to become more secure. Intrusion attacks via applications are becoming standard.
Compliance ≠ Security
The biggest problem in secure software development is the ability to get funds for individual developer training. My company has a limited budget for training making it hard to beef up with the day job and new technologies' vulnerabilities.
We're a very large clinic + must meet several guidelines specifically AIPAA/HITech/ARRA. (A CIO respondent)
Some of the questions regarding "formal mechanisms" are a little tricky. I know of companies who might have tons of security policies, but might follow a handful!
You should have asked about the respondent's specific job function and seniority… because a CTO is different than a system admin.
In my 16+ years in InfoSec the biggest problems I see today are: - A focus on "compliance" and security. Instead of taking the recommendations to improve security management now (….) to be told what they should do by outside agencies. - Lack of communication between InfoSec & Business Management. The economy recently has also been a major factor with little ROC on the implementation of new products. Down-sizing is also having a crippling effect on

the organization. "Bottom line" is the mantra, but does it make business sense in all situations?
Basically, security controls are extremely tight to the point where it feels like we are working in quicksand because everything is so highly classified, plus because we do insider threat monitoring as well (cyber counter-espionage). In terms of the CIA triad, availability is way low, confidentiality is high and I would assess our requirements for data integrity is medium/medium high. I answered "3-some extent" to that question, focused on the word "balance". However, I would say that in a way, it is not balance because often controls + compartmentalization that are way tighter than necessary, so access to info is low due to so many security controls, but I was unsure which side of the spectrum to lean toward given my situation.
Good self-assessment survey for internal improvement of security practices.
Executive management always asks: "How much security is enough". Global risks outside the U.S. are likely underestimated and under protected. Legal compliance, like Sarbanes-Oxley, gets more management attention and resources than any other risk assessment or presentation, including audit.
The word "threat" was hard to get my hands around. FISMA compliance is a threat because it takes professionals away from worthwhile work. Security is high; compliance not so good.
Infosec initiatives are driven by 2 factors: 1) Those of us in operations who understand the gap. 2) External requirements (PCI, customer request) that force us to do it. There is little "top down" direction to improve or have any security.
This is a very good survey. Good luck.
I work for a network security vendor. So we have a bunch of highly educated & trained security professional; some of the best. However, our IT department is small and may not be security professionals like engineering, product management, sales, etc. So it may be an unusual perspective. The other thing is that this survey

seems to target folks with a lot of visibility into the organizations IT operations. If you're not in IT, some of these questions are tough to answer.
I would like to see security as an integrated part of system development - not as something added later. Would like to see unannounced security system evaluation and penetration testing. Evaluation and examination that sensitive data are stored in encrypted format - including data backups. All portable devises (laptop, PDA, blackberry etc.) should be randomly checked to see if sensitive data reside in encrypted format.
Consider targeting responses from Information Assurance evaluators. Their input may provide a different perspective as well as a more accurate depiction of the overall security posture.
My organization (which I have only been a member of for 3 years) does not have direct Internet facing servers. I was hired to support and direct the internal systems support group to handle new projects with a higher security consciousness. This org was ISO 9001 + ISO27001 certified before I was hired, however, there isn't a good communication between the internal systems group and the community we support, and that is why feel there is a lack of good security practices (system wise). Corporate is starting to bring in good risk mgmt tools, however, there is a disconnect between corporate & orgs like mine. As a security contact, I am working to marry the corporate tools/resources into the organization's practices, a slow (and sometimes painful) process!
Your survey questions accurately identified the current issues with information security programmes. Good luck with your research.
I appreciate the random opportunity to participate in your doctoral work, and offer these additional comments.

First, my responses reflect my Federal government (i.e., Department of Defense) bias. There really is a significant difference between the information assurance I live each day in my position versus someone like me in a commercial or university environment. My environment has a rigid hierarchical structure in which issues such as incident response, intrusion detection, intrusion prevention, malicious software defense, and networking are not the responsibility of local leaders. Therefore, locally the buy-in of local management is a minimal issue.

Second, the mantra in the thirty-five years of my association with computer security, information system security, and now information assurance has echoed around the "need for management support". Policy and strategic statements within government, the commercial sector, and private organizations have incessantly restated this requirement. I can testify based on experience within dozens of military organizations that one can have an effective information assurance program, validated by independent parties, without direct management support. One requires on a laissez-faire management attitude to build and to maintain a credible program. Given the right mix of individuals possessing the applicable enthusiasm and talents, excellent IA program can and do flourish. I would argue that, if managers simply do not impede the process, the right people can maintain an effective program.

Third, money does not guarantee an effective information assurance program; rather it is the individuals who devise, manage and implement it. Therefore, recruitment of those individuals is of paramount importance.

Infosec can target IT and focus on compliance - losing sight of the customer and business process. Some of your questions can be viewed through different perspectives, IT, Infosec, or the business - then some of the answers would change. Note: there is also a very large group of so called experts who really do not know who would provide very different answers. I am always trying to educate them but it could skew the sample population.

As a direct-report to the Director of IT (CIO), I was an ISO (Information Security Officer) that instituted a risk-management-based security program that balances organizational objectives with mandated-compliance, protection (confidentiality, integrity, and availability), and governance as defined by the business (GRC). Developed staff into very proficient security professionals which resulted in the establishment of an advanced security organization. Created, designed, developed, organized, and executed security functions including:

Risk Management Processes: Established classification and prioritization models for data and services. Also established organizational protection requirement criteria based on risk.

Vulnerability Management: Managed/performed vulnerability assessments, penetration testing, and application security testing. Provided and managed mitigation recommendations.

Application Security: Led the efforts to have programming staff develops more secure application code leveraging OWASP (OWASP "Development Guide" and the OWASP "Top 10"). Integrated application security into their SDLC. Performed vulnerability assessments on custom developed applications and COTS solutions. Collaborated with third parties (Ounce Labs) to perform static analysis, black box testing, and provide remediation recommendations.

Security Awareness: Created security Intranet site, streaming videos, newsletter publications, and presentations

Incident Response: Developed and executed incident handling procedures (tied to risk). Also created, training, and development Interdepartmental CIRT (Computer Incident Response Team).

Forensic Services: Forensic analysis, investigation, monitoring, chain of custody, data recovery, and evidence handling.

Security Monitoring: IDS/IPS, SEM integration/monitoring and rogue

wireless detection/location.

Security Policy: Created, developed, managed, and enforced security policy and procedures for the organization.

The development of the security program resulted in mature/repeatable processes which were integrated into existing IT departmental processes and newly-developed ITIL processes. Finally, ISO 27001, ISO 27002, and NIST standards were leveraged by my department to research, study, identify gaps, and mitigate gaps for the organization.

The effect of organizational capabilities on information security strategy and organizational performance, in my opinion, will vary depending upon the maturity level of the IT governance process, and whether or not the Information Security function is perceived as an enabler of the business process or viewed as a road block. Additionally, a decentralized, federated security model will have significantly more challenges in implementing strategic security policy than a centralized security model. What appear to be missing in the above survey are the following questions:

1. What is the maturity level of information technology governance?

2. What percent of the organizations budget is allocated to information security?

3. What level does compliance/regulatory issues drive information security strategy?

I work for a great organization. I was brought on board a little more than a year ago to establish a new office to help change a culture which did not understand the threats, vulnerabilities and information security risks that were unknowingly being accepted. We are making significant progress but we still have far to go.

I see many organizations increasing their security posture through policy and technology due to the various regulations out there, however I am curious as to how many organizations actually view security as a business driver that increases value as

opposed to a strict, must have, that increases operational costs
Short term government budgetary challenges frequently impact IA projects in my organization. The policies, procedures, and staff are mostly in place but the projects are often not appropriately funded; or the IA components of the projects are cut to reduce overall project costs. For example, enterprise patching often is lacking because the larger systems typically have an annual update cycle contracted...if that. Keeping up with urgent and monthly patching is too expensive because the regression testing and dissemination to all enterprise systems is in the millions of dollars in cost each year. Secondly, senior government leaders are still very IA risk averse--from a project management perspective. This zero-risk approach prevents the organization from deploying newer processes, technologies, or approaches that could save money and improve customer access. Government program managers are very tightly restricted by organizational and Congressional oversight. As a result, slow moving steady incremental programs with little disruption that stay on budget are the desired norm--don't rock the boat. Third, data ownership continues to challenge my organization. Several external organizations "own" the data we use. The impact is that external organizations often influence internal security architectures driving up costs. "My data is special and can only be put on an isolated server and workstations in this one locked room." With multiple data providers each thinking that their data is "more" special than others, and few of the external organizations trusting each other to maintain separation of data, the IA architecture, policy issues, and environment creates some significant information sharing challenges.
The metrics are collected. The problem is that they are not useful. They are numbers that make executives happy. They reflect what is done daily, not lead to what should be done to make things better. The questions don't ask if the metrics are

helpful.
I received your survey and unfortunately I must decline to participate. You are familiar with the CIA principles of ISC2, confidentiality, integrity and assurance. I have been unemployed for over a year and cannot answer any of the questions as they are all from "The organization I work for..." I have found that with a BS in computer science, a MA in Information Systems Management, a CISSP, CISA and ITIL certifications, 20 years experience (with the last 13 years in management) I cannot even get an interview for a helpdesk position. When I was employed in the Pharmaceutical industry, we were more concerned about product quality and meeting FDA guidelines than security, as that was a role left to the Risk management type group in the headquarter location. The most responsibility I had was to verify the physical person, the user ID, and the systems authorities they were given to perform the job function they were hired to do. The Risk managers regularly employed consultants to enact industry "best practices". We often joked that the "best practice" was the budgeted amount. The company saw IT security more like a necessary cost of doing business than risk prevention. Since the product purchaser or end consumer was an institutional customer where product was paid via bank or wire transfers, we never had to worry about credit cards (PCI compliance) or privacy issues. Just SOX compliance, even internal IT audits were a joke. I wish you well in your research and am actually interested in your findings. If you can put me on your list to electronically receive them I would appreciate that. (email address). Please consider submitting your paper for publishing in the ISC or ISACA journals. It's a good forum to get your name out there.
1) Working in government organization: government employees demonstrate

less alignment to business and security strategies than the contractors who are tasked with executing the tactical aspects. 2) Communication channels are fragmented and usually one-way (top to bottom).
Your question is wrong on this. The questions should be directed as follows: PART A: Rank & file of organizations PART B: All of IT in same orgs PART C: CFO & Marketing in same orgs This makes section 2 unnecessary. By polling security purists you will receive an inflated view of proficiency. My answers are not going to help your cause, as security best practice is my job. You do not account for consulting in your mix. This insight will come with experience.
Large companies have broad security strategies based on division, mission, products and customers. This was very general and many questions per division might have been answered differently. IT/Corp security doesn't always set policy or standards across InfoSec, development, etc. I answered the question as I see the organization, but there are holes in security where execs, divisions, mission of the company, etc. diverge from the security strategy.
What was not covered is the over tightening of controls to the point that it makes the accomplishment of the business mission difficult to achieve. This situation is something we encounter very often. The worker will use other equipment to get the job done, but circumvent the control due to its poorly thought out implementation. Good luck on your project! It is needed.

I am the only security guy in my company. While I am involved in decision making process, I do not have enough support to effectively implement all measures that I would like to. Also - Workload … - prohibit me from implementing such controls. Fly by night and hope for the best that has to be my mantra. Security is mostly an afterthought in my organizations. While required, it is often merely a "checkbox" for compliance reasons. People don't care about security. Good luck.
Have you considered the role or affect of legacy systems that cannot be upgraded to security standards but are too critical or expensive to replace on the risk posture of an organization.
The gaming industry (casinos) is just waking up to Technology Security and has a long way to go. It seems like if they still have not disconnected from the "Physical" Security (surveillance) to step into the realm of Information Security.
As IT Manager I am of course responsible for the technical aspects of information security. I think we do a very good job knowing and covering the fundamentals (patches, least privileges, etc.) at a reasonable cost. I really wish we did a better job at real-time analysis and response, and plan to contract for some of that. Company management has little interest in security policy, classifying information, awareness no one wants to touch it. They just want to be told good news no matter what.