A MODEL OF MANAGERIAL EFFECTIVENESS IN INFORMATION SECURITY: FROM GROUNDED THEORY TO EMPIRICAL TEST

Kenneth Joseph Knapp

A Dissertation

Submitted to

The Graduate Faculty of

Auburn University

in Partial Fulfillment of the

Requirements for the

Degree of

Doctor of Philosophy

Auburn, Alabama

December 16, 2005

A MODEL OF MANAGERIAL EFFECTIVENESS IN INFORMATION SECURITY:

FROM GROUNDED THEORY TO EMPIRICAL TEST

Except where reference is made to the work of others, the work described in this dissertation is my own or was done in collaboration with my advisory committee. This dissertation does not include proprietary or classified information.

_____

Kenneth Joseph Knapp

Certificate of Approval:

_____	_____
R. Kelly Rainer, Jr. George Phillips Privett Professor Management Information Systems	Thomas E. Marshall, Chair Associate Professor Management Information Systems
_____	_____
F. Nelson Ford Associate Professor Management Information Systems	Stephen L. McFarland Dean Graduate School

A MODEL OF MANAGERIAL EFFECTIVENESS IN INFORMATION SECURITY:

FROM GROUNDED THEORY TO EMPIRICAL TEST

Kenneth Joseph Knapp

_____
Author

_____
Date of Graduation

DISSERTATION ABSTRACT

A MODEL OF MANAGERIAL EFFECTIVENESS IN INFORMATION SECURITY: FROM GROUNDED THEORY TO EMPIRICAL TEST

Kenneth Joseph Knapp

Doctor of Philosophy, December 16, 2005
(M.B.A., Auburn University, 1993)
(B.S., De Sales University, 1988)

225 Typed Pages

Directed by Thomas E. Marshall

Information security is a critical issue facing organizations worldwide. In order to mitigate risk and protect valuable information, organizations need to operate and manage effective information security programs. Using a research methodology that combines qualitative and quantitative techniques, this study proposes and tests a theoretical model of managerial effectiveness in information security. Specifically, the model demonstrates the influence of top management support on perceived security effectiveness mediated by four constructs critical to successful information security programs: user training, security culture, policy relevance, and policy enforcement. Prior research has not yet

examined the mediation factors between management support and information security effectiveness.

During the qualitative phase of the study, an open-ended question was given to a sample of 220 certified information system security professionals (CISSPs). Responses were analyzed using a grounded theory strategy to develop a theoretical model as well as a survey instrument to test the model. Because of the potential sensitive nature of information security research, a special effort removed items appearing overly intrusive to the respondents. In this endeavor, an expert panel of security practitioners evaluated all proposed items on a willingness-to-answer scale. The instrument underwent further refinements through multiple pre-tests and a pilot test.

During the quantitative phase of the study, the final instrument was completed by 740 CISSPs who provided the data for empirical testing of the model. To control for common method variance, the study employed several procedural remedies during data collection. Once collected, the empirical data were analyzed using structural equation modeling with results suggesting full support for the theoretical model. An additional finding suggested strong support for an alternative, second-order factor model. Further analysis found that the alternative model might have general applicability across demographics and cultures. Overall, a high level of consistency exists between the qualitative and quantitative findings of the study.

This study also investigated how the concept of task interdependence relates to information security. Using a previously developed scale given to a sample of 936 CISSPs, the results found that effective IS security programs require high levels of task interdependence in organizations.

TABLE OF CONTENTS

Page

LIST OF TABLES xii

LIST OF FIGURES xv

CHAPTER I INTRODUCTION 1

Research Objective of the Study 4

Organization of the Dissertation 7

CHAPTER II LITERATURE REVIEW 9

Top Management Support 9

User Training 11

Security Culture 13

Information Security Policy 14

Perceived Security Effectiveness 15

Task Interdependence 17

Summary 18

CHAPTER III RESEARCH METHODOLOGY 20

Step One - Qualitative Data Collection - Open-ended Questions 22

Step Two - Qualitative Analysis - Grounded Theory 26

Step Three - Scale Development 35

Step Four - Instrument Refinement 36

Step Five - Quantitative Data Collection - Large-scale Survey 53
Step Six - Quantitative Data Analysis – Structural Equation Modeling 55
CHAPTER IV RESULTS 57
Data Preparation and Sample Demographics 57
Statistical Analysis of Each Construct 67
Analysis of the A Priori Theoretical Model 83
Analysis of Mediation Effects 86
Demographic Analysis of A Priori Model 97
Alternative, Second-order Factor Mediation Model 110
Demographic Analysis Using Second-Order Factor Model 113
Common Variance Tests 118
Task Interdependence Results 124
Summary of Empirical Results 135
CHAPTER V DISCUSSION & CONCLUSION 136
Links to Existing Theory 136
Methodological Issues 150
Implications for Research & Practice 158
Conclusion of the Study 160
REFERENCES 161
APPENDIX A List of Categories after Open Coding 182
APPENDIX B List of Categories after Axial Coding 184
APPENDIX C Results of Critical Issues in Information Security Survey 185
APPENDIX D Text Of Email Blast from $(ISC)^2$ to Constituency 189

APPENDIX E Phase One, Two, & Three Survey Instruments 190

APPENDIX F CISSP Statements from the Phase One Web Survey..... 202

APPENDIX G Standardized Residual Covariance Matrix from Alternate Model..... 206

APPENDIX H..... 208

Covariance Matrix of Second Order Factor Model - Part 1 208

Covariance Matrix of Second Order Factor Model - Part 2 210

LIST OF TABLES

Page

Table 1. *MIS Quarterly Rankings of the Security Issue* 3

Table 2. *Top Ten Information Security Issues (Knapp et al., 2004)* 4

Table 3. *Sample Characteristics of CISSPs Responding to Open-ended Question* 25

Table 4. *Formal Hypotheses* 30

Table 5. *Statements Supporting the Hypothesized Model* 31

Table 6. *Willingness-to-Answer Scale* 40

Table 7. *Intrusiveness Scores for Initial Policy Enforcement Items* 42

Table 8. *Intrusiveness Scores for Initial Perceived Security Effectiveness Items* 43

Table 9. *Country Demographics (pilot)* 45

Table 10. *Industry Demographics (pilot)* 46

Table 11. *Construct Fit Indices (pilot)* 48

Table 12. *Independent Variable Measurement Scales* 49

Table 13. *Mediating Variables Measurement Scales* 50

Table 14. *Dependent Variable Measurement Scale* 52

Table 15. *Sample Size and Response Rates by Phase* 58

Table 16. *Country Demographics* 60

Table 17. *Organization Size* 62

Table 18. *Organization Position* 63

Table 19. *Years of Information Technology & Security Experience* 64

Table 20. *Years of Experience with Organization* 64

Table 21. *Industry Demographics* 65

Table 22. *Factor Loadings* 68

Table 23. *Summary of Acceptable Cut-off Values of Reliability and Fit* 72

Table 24. *Top Management Support Construct Fit* 74

Table 25. *User Training Construct Fit* 75

Table 26. *Security Culture Construct Fit* 76

Table 27. *Policy Relevance Construct Fit* 77

Table 28. *Policy Enforcement Construct Fit* 78

Table 29. *Perceived Security Effectiveness Construct Fit* 79

Table 30. *Summary of Measurement Properties of Constructs (29-item instrument)* 80

Table 31. *Discriminate Validity Tests* 82

Table 32. *Measurement Model* 84

Table 33. *Tests of Each Mediation Variable* 90

Table 34. *Percent Mediated of Total Effect on Perceived Security Effectiveness* 92

Table 35. *Summary of Fit Statistics Comparing Two Mediation Models* 94

Table 36. *Formal Hypotheses Supported* 96

Table 37. *Demographic Tests of Partial Mediation Model* 98

Table 38. *Construct Bias Tests of Each Theoretical Construct* 105

Table 39. *Cultural Analysis of Two Questionnaire Items* 109

Table 40. *Comparison of Mediation Models* 112

Table 41. *Demographic Tests of Second-Order Factor Mediation Model* 114

Table 42. *Results of Model Comparison based on Facteau et al (1995)* 119

Table 43. *Percentage of Variance Comparison* 120

Table 44. *Percentage of Variance Comparison with Marker Variable* 122

Table 45. *Correlations of Pilot and Large-Scale Survey Data* 124

Table 46. *Task Interdependence Scale (Pearce et al, 1992)* 126

Table 47. *Task Interdependence Reliability and Fit* 127

Table 48. *Data from Studies Included in Sharma & Yetton Meta-analysis* 128

Table 49. *Results Comparison Before & After Inclusion of Present Study* 129

Table 50. *Task Interdependence Scale (Van Der Vegt et al., 2003)* 130

Table 51. *Task Interdependence Results Comparison* 131

Table 52. *Task Interdependence Results by Demographic* 133

Table 53. *Contrasting Ranking Results to Total Effect of Each Construct* 141

Table 54. *CISSP Statements on Task Cooperation and Interdependence* 145

Table 55. *The Top Ten Ranked Issues* 186

Table 56. *Top 25 Ranking Survey Results (874 respondents)* 188

LIST OF FIGURES

Page

Figure 1. *General Model of the Research Question* 5

Figure 2. *Six Methodology Steps* 22

Figure 3. *General Full Mediation Model* 29

Figure 4. *Hypothesized Partial Mediation Model* 29

Figure 5. *Data Collection Remedies to Control for Common Method Variance* 54

Figure 6. *Path Diagram of Hypothesized, Partial Mediation Model* 86

Figure 7. *Mediation Model Comparison* 89

Figure 8. *Full Mediation Model* 93

Figure 9. *Comparative Benefit of Hypothesis 6* 95

Figure 10. *A Priori, Partial Mediation Model (same as Figure 6)* 111

Figure 11. *Alternative, Second-order Factor Mediation Model* 111

Figure 12. *Moderating Effect of Task Interdependence (Sharma & Yetton, 2003)* 126

Figure 13. *Scatter Plot of Construct Correlation and Task Interdependence* 129

Figure 14. *Example of Simple Linear Function* 138

Figure 15. *Closest Theoretical Structure to the Current Study* 139

Figure 16. *General Forms of the Theoretical Models of this Study* 140

Figure 17. *Theory Y and Theory X Dichotomy* 150

Figure 18. *Phase Two Questionnaire in Excel.* 199

Figure 19. *Phase Three Web Survey in Microsoft Explorer* 200

CHAPTER I

INTRODUCTION

Information systems (IS) security is a critical issue facing organizations worldwide. With modern national economies fully dependent upon information technology for survival (President, 2003; Schou & Trimmer, 2004), the need to protect information and mitigate risk is more paramount than ever before. Multiple national surveys confirm a high number of attacks against organization information resources (Bagchi & Udo, 2003; Computer Emergency Response Team (CERT), 2004; Gordon, Loeb, Lucyshyn, & Richardson, 2004). Between 1998 and 2003, the number of reported incidents to the U.S. CERT has nearly doubled each year with 137,529 reported incidents in 2003 alone. Incidents have become so commonplace that the CERT no longer publishes incident numbers.[1] According to an Ernst and Young analysis, security incidents may cost companies between $17 and $28 million each occurrence (Garg, Curtis, & Halper, 2003). Since incidents are frequent and costly, management must take security seriously to protect their critical organizational information.

Broadly defined, security represents safety from danger and is especially important in threatening environments (Aquinas, 2003). Information security is a more recent phenomena corresponding to the rise of computers, networks, and the Internet.

---

[1] see http://www.cert.org/stats/cert_stats.html

Regardless of the enormous business benefits derived from information technology (IT), increased reliance on IT leads to increased vulnerability and danger. Since IT can encompass virtually the entire operation of the organization it serves, probably no single element has a greater potential to wipe out an entire company so quickly than a computer-related disaster (Green & Farber, 1975). For decades, security authorities have understood this danger and recognized that solving organizational IS security problems requires managerial attention (Allen, 1968; Parker, 1981; Van Tassel, 1972). Even with the recognition of increased danger, managers often did not regard security as important and many permitted their information systems to be either lightly protected or wholly unprotected (Straub, 1990).

In 1980, the *MIS Quarterly* began publishing the results of key issue surveys given to members of the Society for Information Management (SIM), a group of IT executives. Throughout the 1980s, *security* ranked as a lower-tier issue never rising higher than #12. In the 1994 survey, *security* dropped off the top 20 list entirely (Brancheau, Janz, & Wetherbe, 1996). However, in the 2003 survey, *security & privacy* surged as the third top issue among the survey participants (Luftman & McLean, 2004). Table 1 provides a summary of how the *security* issue ranked from 1980-2003. Based on the 2003 survey, it appears that IT executives now view security to be among their top issues.

Table 1. *MIS Quarterly Rankings of the Security Issue*

Year[2]	Ranking
1980	#12
1986	#18
1989	#19
1994	Dropped
2003	#3

However, even with many IT executives now considering security as one of their top issues, managerial support for organization security programs still may be insufficient. A 2004 key issues study of 874 certified information system security professionals (CISSPs) revealed that *top management support* was ranked number one from a list of 25 security issues (Knapp, Marshall, Rainer, & Morrow, 2004). This suggests that even though IT executives rank security as a high priority issue, managerial support for organizational security programs remains critical and may need improvement. Table 2 lists the top ten issues from this survey. Many of these top issues have strong managerial dimensions to include *training & awareness, organizational culture,* and *policy-related issues.* Appendix C provides the executive summary and the results of the 25-issue ranking from the *Critical Issues In Information Security Survey* report (Knapp et al., 2004).

[2] From 1980-1994, the issue was 'security & control'. In 2003, it changed to 'security & privacy.'

Table 2. *Top Ten Information Security Issues (Knapp et al., 2004)*

Rank	Information Security Issue
1	Top Management Support
2	User Awareness Training & Education
3	Malware
4	Patch Management
5	Vulnerability & Risk Management
6	Policy Related Issues
7	Organization Culture
8	Access Control & Identity Management
9	Internal Threats
10	Business Continuity & Disaster Preparation

Research Objective of the Study

Few IS studies have developed and empirically-tested theoretical models applying managerial constructs to IS security (cf., Kankanhalli, Hock-Hai, Bernard, & Kwok-Kee, 2003; Lee, Lee, & Yoo, 2004; Straub, 1990). Some IS scholars even perceive a serious lack of empirically-based information security research altogether (Bento & Bento, 2004; Kotulic & Clark, 2004). Considering the general lack of empirical research and the importance of information security to modern organizations, this study seeks to contribute to the literature by developing and empirically testing a management theory of organizational IS security. The objective of this study is to develop a theoretical model

of managerial constructs that most influence the effectiveness of information security in organizations. Figure 1 depicts the general model of the research question.

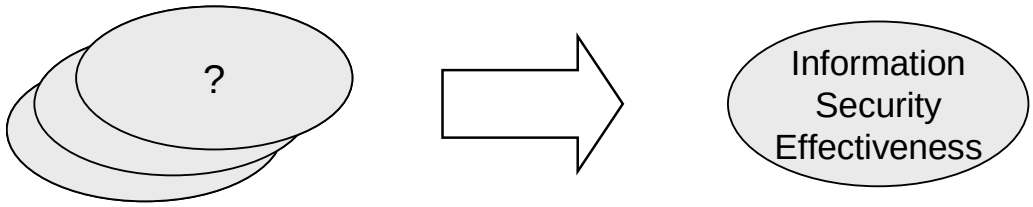


Figure 1. *General Model of the Research Question*

Due to the general lack of theory and empirical research in the IS literature about security, a grounded theory strategy is used to analyze qualitative, textual data in order to develop a theoretical model. Using a three-phased coding process consistent with developing grounded theory, open-ended question responses provided by a sample of information security professionals are analyzed to identify key issues in IS security. A theoretical model is then developed based on the relationships among key managerial issues identified in the open-ended question responses. Specifically, the model illustrates the relationship of top management support on perceived security effectiveness mediated by four managerial constructs: user training, security culture, policy relevance, and policy enforcement.

A survey instrument to test the model is developed by extracting key words and phrases from the open-ended responses to supply the questionnaire items. Because of the potential sensitive nature of information security research, a special effort is made to

remove items appearing overly intrusive to the respondents. In this endeavor, an expert panel of security practitioners evaluated all proposed items on a willingness-to-answer scale. The resulting instrument is then subjected to multiple pre-tests and a pilot test before proceeding to the large-scale empirical test.

The final instrument was completed by 740 CISSPs who are constituents of the International Information Systems Security Certification Consortium [$(ISC)^2$]. During data collection, the survey employed procedural remedies to control for common method variance that included inserting at least a three-day separation between collecting the independent, mediator, and dependent variables. After collection, the empirical data is quantitatively analyzed using structural equation modeling. The hypothesized model as well as an alternative model involving a second-order factor are tested and evaluated for general applicability across demographics and national cultures. A comparison is then made of the degree of consistency between the qualitative and quantitative findings of the study.

This study also investigates how the concept of task interdependence applies to information security. Previous IS research suggests that task interdependence moderates the relationship between management support and IS success. To see how this assertion applies to the topics of this study, the degree to which IS security requires task interdependence is investigated. The findings can help researchers better understand the relationship between required levels of management support and IS security effectiveness. Also, if the findings indicate that IS security work is highly interdependent, several related topics can be identified for future research, particularly studies about teamwork and organizational citizenship behavior.

In addition to the task interdependence literature, the theoretical constructs of this study are linked to other research streams. Topics of discussion include analyzing the effect size of each mediator variable on the dependent variable and subsequently applying the 'dilemma of the supervisor' notion to explain the findings about security policy enforcement. General forms of the two theoretical models of this study are offered as well as a commentary about viewing the models through the lens of socio-technical systems theory and the Theory X and Theory Y dichotomy.

Considering the seriousness of today's information security threats, the findings of this study can help management understand the critical areas that they can most influence in order to better protect organizational information. Prior research has not yet examined the mediation factors between management support and organizational security effectiveness. By doing so, the theoretical models proposed in this study provide timely help to practitioners and researchers alike who seek to advance the managerial effectiveness of information security programs.

Organization of the Dissertation

The lack of theory and empirical research in IS security led the researcher to use the grounded theory strategy to generate a theoretical model from qualitative data. Thus, rather than deriving the theoretical model from published studies identified in the literature review chapter, the methodology chapter describes the research approach used to produce the theoretical model and the survey instrument that tested the model.

Chapter I provides a background of the research problem under investigation. The chapter presents an overview of the qualitative and quantitative methods used in this study. The specific research question of the study is introduced.

Chapter II provides a theoretical perspective by reviewing the relevant literature regarding the key constructs involved in this study. The chapter provides a literature background for each construct of the theoretical model that is later introduced in Chapter III. Also, a section of Chapter II reviews the task interdependence literature.

Chapter III covers the research methodology of the study that produced and tested the theoretical model. This chapter describes the six methodological steps of the project from qualitative data collection to quantitative data analysis.

Chapter IV provides the empirical results of the large-scale survey. Each construct is analyzed for validity and reliability before testing the full *a priori* theoretical model using structural equation modeling. Findings pertaining to mediation effects, demographics and culture, an alternative second-order factor model, common method variance, and task interdependence are also covered.

Chapter V includes a discussion of the findings, major contributions, limitations of the study, and implications for research and practice. This discussion is followed by a conclusion to the study.

CHAPTER II

LITERATURE REVIEW

The theoretical model of this study derives from a qualitative analysis of grounded data which will be described in Chapter III of this dissertation. However, each of the variables in the model has a literature base that provides a useful theoretical perspective. This chapter reviews each of the variables from this study's theoretical model: top management support, user training, security culture, information security policy, and security effectiveness. Since there are few published studies with theoretical models illustrating key managerial constructs of IS security, this review will broadly include literature from both the IS and management bases while identifying important practitioner contributions as well. The final section in Chapter II covers the task interdependence literature.

Top Management Support

Applied to IS activities, top management support refers to the degree that senior leadership understands the importance of the IS function and the extent to which it is involved in IS activities (Armstrong & Sambamurthy, 1999; Ragu-Nathan, Apigian, Ragu-Nathan, & Tu, 2004). In the IS literature, the construct of top management support has been identified as the most frequently hypothesized variable contributing to IS implementation success (Markus, 1981; Sharma & Yetton, 2003). This is not surprising

since by virtue of their position, top management can significantly influence resource allocation and act as a champion of change to create a conducive environment for successful IS implementation (Thong, Yap, & Raman, 1997). Previous studies demonstrate that executive involvement in computerization often leads to IS success in small manufacturing firms (DeLone, 1988), small business environments (Thong, Yap, & Raman, 1996), e-commerce assimilation (Chatterjee & Grewal, 2002), computer aided software engineering tool assimilation (Purvis, Sambamurthy, & Zmud, 2001) and executive information systems implementation (Rainer & Watson, 1995).

In recent years, two meta-analysis studies investigated the management support construct. First, Sharma & Yetton (2003) performed a meta-analysis based on 22 previous studies involving the management support construct. Based on their examination, strong support for a model was found where task interdependence moderates the effect of management support on IS implementation success. Second, Jasperson et al (2002) conducted a meta-analysis and offered three meta-conjectures about top management support based on a review of 81 scholarly articles. The authors conjectured that:

- Top management's failure to exercise formal authority leads to more prevalent exercise of influencing behavior in IT decision by other parties,
- Top management support has more impact on project success in development environments characterized by resource conflict, and
- Top management support has more impact when there is uncertainty about the importance of IT generally or the project specifically.

Applied to security, top management support has been recognized for nearly four decades as necessary for effective computer security management (Allen, 1968; Dutta & McCrohan, 2002; Parker, 1981; Wasserman, 1969). Wasserman (1969, p.120) stated, "Computer security thus involves a review of every possible source of control breakdown…one factor that has made the job more difficult is lack of awareness by many executives of new control concepts required for computer systems." Dutta & McCrohan (2002) stated that effective organizational computer security does not start with firewalls or anti-virus software, but with top management support. Once executives place a priority on security, it takes continued effort to keep management involved (Tompkins, 2002).

Executive support can be very helpful in promoting an effective organizational IS security program. Some of the ways management can do this is by supporting user training, promoting a security-aware culture, and insisting that security policies are relevant, current, and enforced (Knapp et al., 2004). The following three sections explore the literature regarding training, culture, and policy.

User Training

Simon (1957) classifies training as a mechanism of organizational influence. Organizations train and indoctrinate its members to internalize knowledge and skill that enables the worker to make decisions consistent with organization objectives. Applied to security, the topic of training is intertwined with awareness. An organizational awareness program is often the initial phase of a broader security training program. Awareness alerts employees to the issues of IT security (Straub & Welke, 1998) and prepares users to receive the basic concepts of IT security through a formal training program. Security

awareness helps reinforce training materials through cyclical and ongoing security reminders and events (Hansche, 2002). Training and awareness programs can be used to influence the culture of an organization (Schein, 1995) by promoting favorable security practices and mindsets.

The topic of user training is a recurrent research area in the IS discipline. Previous research has investigated the role of training as a key to competitive IS strategy (James, 1992), the impact of training on IS acceptance (Lee, Kim, & Lee, 1995; Nelson & Cheney, 1987; Shaw, DeLone, & Niederman, 2002), the development of process models of end-user training (Bostrom, Olfman, & Sein, 1990; Sein, Bostrom, & Olfman, 1999), the roles of computer interface designs with training methods (Davis & Bostrom, 1993), the effectiveness of web-based learning (Piccoli, Ahman, & Ives, 1995), and the necessity of training end-users about advancing internet technologies (Aggarwal, 2003).

Earlier IS literature covering security training focused on countermeasures, deterrence, and abuse prevention (Hoffer & Straub, 1989; Parker, 1981; Straub & Nance, 1990). However, some of the earlier security management textbooks had little or no discussion about a systematic approach to employee security training or awareness (Green & Farber, 1975; Parker, 1981; Van Tassel, 1972). Yet, one of the basic steps in coping with information security risk is the establishment of a training awareness program. Such a program should require training during new employee orientation and prior to computer account issuance (Straub & Welke, 1998).

In the practitioner literature, organization's are often urged to train employees about security threats and to encourage employees to support organizational policy in the course of their daily work (ISO/IEC, 2000). Employees have been identified as an

important factor enabling IT security since security incidents are often the result of employees' lack of awareness of IT security policies and procedures (Hansche, 2002; Mitnick, 2003).

Security Culture

Culture can be defined as a set of beliefs, values, understandings, and norms shared by members of an organization (Daft & Marcic, 2001). Some researchers believe that the only thing of real importance that leaders can do is to create and manage culture; the unique talent of leaders is their ability to work with culture (Schein, 1996). Culture has been an important topic in the practitioner literature (Artner, 2000) and recently has been identified as an opportunity for future IS research in security (Kankanhalli et al., 2003)

In the management literature, culture has been described as a system of shared beliefs that is developed and sustained by organizational executives through symbolic action (Smircich, 1992). The culture construct has been explored for its role regarding the implementation of new behaviors and organizational improvement initiatives (Detert, Schroeder, & Mauriel, 2000). One study examined the linkages between organizational culture and its relationships to total control, service quality, and employee performance (Klein, Masi, & Weidner, 1995). In the IS literature, organizational culture has been examined as an opposition force resisting new technologies and transformations (Robey & Boudreau, 1999), effecting successful IT adoption (Tolsby, 1998), impacting IS policy and managerial effectiveness (Beachboard, 2004), influencing time-based manufacturing performance (Nahm, 2003), effecting information systems performance (Claver, Llopis,

Gonzalez, & Gasco, 2003), and impacting organizational security (von Solms & von Solms, 2004).

Information Security Policy

Simon (1957) defined policy as any general rule that has been laid down in an organization to limit the discretion of subordinates with the more important of these rules promulgated by top management. Much of the existing IS scholarly literature is generally about IS policy and not specifically about information security policy. Some of this research has focused on IS policy planning and its role in establishing an appropriate organizational culture favorable to information technologies (King & Zmud, 1981). Another study linked the effect of organizational culture on IS policy and managerial effectiveness (Beachboard, 2004).

In information systems, policy takes on particular importance with respect to security. Information security policy has been called the precondition to implementing all effective security deterrents (Straub, 1990) and may be more vital to reducing computer crime than devices like firewalls and intrusion detection systems (Buss & Salerno, 1984). Of all the controls necessary to protect organizational information from threats, the information security policy may be the most important one (Hone & Eloff, 2002; Whitman & Mattord, 2004).

Previous IS studies have recognized security policy as an important deterrent to ward off potential system abuse (Kankanhalli et al., 2003; Lee et al., 2004; Straub & Welke, 1998) and promote ethical conduct (Harrington, 1996; Leonard & Cronan, 2000). Other studies have invoked security policy as a useful means of controlling issues such as password effectiveness (Zviran & Haga, 1999), software piracy (Gopal & Sanders, 1997;

Peace, Galletta, & Thong, 2002), information privacy (Smith, Milberg, & Burke, 1996), computer viruses (Post & Kagan, 2000), and managing the acceptable use of IT resources at work (Boncella, 2001). Also, research topics involving computer monitoring to observe employee performance (George, 1996) and encourage policy adherence (Ariss, 2002) have been studied.

While the published academic research on security policy is somewhat limited, the number of publications available from practitioners and governmental bodies is more substantial (Barman, 2002; Howard, 2003; ISO/IEC, 2000; Lowery, 2002; Peltier, 2002; Swanson & Guttman, 1996). Wood (2003) explains that policies act as a clear statement of management intent and are central to virtually everything that happens in the information security field. Without a vital policy document, overall guidance will be lacking and managerial support called into question. The National Strategy to Secure Cyberspace (President, 2003) repeatedly references security policies and standards as an essential part of protecting networked systems. Information security policies are sometimes framed in a life-cycle context with emphasis on development, enforcement, and maintenance while advising that security policy be consistent with business objectives (Hare, 2002; Howard, 2003).

Perceived Security Effectiveness

So far, this chapter has reviewed the literature pertaining to management support and ways management can promote IS security effectiveness through training, culture, and policy. Now this review considers IS security effectiveness. Overall, there are few studies of IS security effectiveness in the literature. One study employed user perceptions of concern for security as an empirical measure of IS security effectiveness

(Straub & Goodhue, 1991). Another operationalized a perceived measure of security effectiveness using responses about overall security deterrence, prevention, as well as the protection level of computer hardware, software, data, and services (Kankanhalli et al., 2003). While both the Straub and the Kankanhalli studies contributed to the information security literature in meaningful ways, each acknowledged limitations such as a low explained variance and a low sample size.

In another study, Straub (1990) used computer abuse as a surrogate for security effectiveness. The construct was operationalized as the control of abuse through countermeasures such as deterrence and was measured through a combination of hard data and a subjective index. The study provided a general implication that computer security is more effective when organizations have active security staffs, implement effective controls, and inform users about penalties for noncompliance.

Methodological questions have been raised about the measurement of perceived effectiveness (or success) variables. Yet, constructs based on subjective judgments and perceptions can be found in both the management (e.g., Ragins, 2000) and the IS literature (e.g., Marshall & Byrd, 1998). In the current study, the perceived effectiveness variable is based on the subjective judgment of security professionals. The literature contains arguments both for and against the use of self-reported, subjective measures (Podsakoff & Organ, 1986; Spector, 1994; Straub, Boudreau, & Gefen, 2004). Some evidence suggests that perceived and objective measures are positively associated (Venkatraman & Ramanujam, 1987) while others suggest they are not positively associated (Srinivasan, 1985). Despite the debate, self-reported, subjective measures can

be an appropriate research tool for exploratory studies into a phenomena of interest (Spector, 1994).

Another issue raised in the literature is the sensitive nature of surveys that ask questions about information security effectiveness. Many companies, for example, are hesitant to provide hard data regarding computer abuse or security ineffectiveness because of the extremely sensitive nature of the topic (Kotulic & Clark, 2004; Straub & Welke, 1998). In addition, it's difficult to know if hard data (e.g. number of incidents, financial loss) is accurate and complete considering that security incidents often are undetected or underreported (Richardson, 2003). An alternative to hard data is to measure security effectiveness using professional subjective judgment. Yet it can be argued that a qualified judgment about an organization's overall security effectiveness is more sensitive than the sharing of hard data. Regardless, based on the lessons offered in the literature and due to the sensitive nature of the topic, researchers investigating information security effectiveness should proceed with caution.

Task Interdependence

A construct not directly related to the theoretical model of this study but will be investigated and analyzed in Chapter III is *task interdependence*. Task interdependence is the extent to which individuals depend upon other individuals and resources to perform a job (Van Der Vegt, Van De Vliert, & Oosterhof, 2003). High levels of task interdependence has been linked to high demands for top management support in order to improve the likelihood of IS implementation success (Sharma & Yetton, 2003). Task interdependence underpins workflow patterns and routines that involve multiple actors

whose habituated patterns of interdependent actions produce and reproduce the institutional context (Orlikowski, 1992; Sharma & Yetton, 2003).

In the IS literature, the task interdependence construct has received some research attention (Andres & Zmud, 2003; Sharma & Yetton, 2003). Most research into the topic is outside the IS domain (Bachrach, Powell, & Bendoly, 2004; Harter & Slaughter, 2003; Organ, 1988; Stanne, Johnson, & Johnson, 1999; Van Der Vegt, Eman, & Van De Vliert, 2001; Van Der Vegt et al., 2003; Wageman, 1995). The present study investigates the degree to which IS security is high in task interdependence using two previously developed scales (Pearce, Sommer, Morris, & Frideger, 1992; Van Der Vegt et al., 2003) and comparing the results to those of previous studies (Sharma & Yetton, 2003; Van Der Vegt et al., 2003). This may be useful because if IS security tasks require high levels of task interdependence, then comparing the model of the present study to related theoretical assertions can offer an analysis of the nomological validity of the present model. In addition, a number of research topics linked to task interdependence will be identified as opportunities for future study.

Summary

The theoretical model of this study derives from a qualitative analysis of grounded data and will be revealed in the following chapter. However, each of the constructs of the model has a literature base that offers a theoretical perspective into the current study. During the course of reviewing the literature, the investigator did not find a theoretical model that substantially combined these variables or one that resembles the model revealed in Chapter III of this dissertation.

The following chapter describes the research methodology used in this study. During the qualitative portion of the methodology, the theoretical model will emerge from a grounded analysis of responses to an open-ended question given to an international sample of certified information security professionals. The chapter describes the methods used during each phase of the study from qualitative data collection to empirical testing of the hypothetical model.

CHAPTER III

RESEARCH METHODOLOGY

This research study combines qualitative and quantitative techniques over a six step methodological process. Such a combined approach can provide a richer, contextual basis for interpreting and validating results (Kaplan & Duchon, 1988). Three broad benefits of linking qualitative and quantitative data are provided. First, linking can enable confirmation or corroboration of research findings. Second, it can help elaborate or develop analysis and provide richer detail. Third, it can initiate new lines of thinking and provide fresh insights into given phenomena (Miles & Huberman, 1994; Rossman & Wilson, 1984).

The qualitative portion of the methodology relied on the grounded theory research strategy (Glaser & Strauss, 1967; Orlikowski, 1993) in order to analyze open-ended question responses from 220 certified information system security professionals (CISSPs) who are constituents of the International Information Systems Security Certification Consortium [$(ISC)^2$]. This analysis generated a theoretical model depicting conceptual relationships among key managerial issues in information security. The next phase involved researchers developing measurement scales by extracting questionnaire items from the content of the open-ended question responses. An expert panel then evaluated the extracted items for construct validity and perceived intrusiveness.

An important objective of the current study is to create an instrument that exhibits not only high validity, but minimizes the respondent's perception of instrument intrusiveness. Instruments with intrusively worded questions that cover sensitive organizational issues may cause respondents to be less than forthright in their answers and can be a source of undesirable method variance (Spector, 1994). For this reason, the expert panel evaluated every item using a developed willingness-to-answer scale in order to identify potentially intrusive items and thus making the survey instrument less threatening to potential respondents.

After the multiple rounds of expert evaluation, a pre-test, and a pilot test, a large sample of data is collected to empirically test the theoretical model of this study. The data is analyzed using a structural equation modeling (SEM) approach to confirmatory factor analysis. SEM provides a comprehensive statistical approach to testing hypotheses about relations among latent variables (Hoyle, 1995) and is appropriate for this study.

A similar research study that methodologically combined grounded theory and SEM was not found in the information systems (IS) literature. However, examples of this combination in a single research project were found in the nursing and medical research domain (Larsson, Larsson, & Munch, 1998; Turkel & Ray, 2001); some of the techniques from these studies aided with the methodological strategy selected for the current project. Figure 2 illustrates the six methodological steps of the current study. The following sections describe each of the six steps in detail.

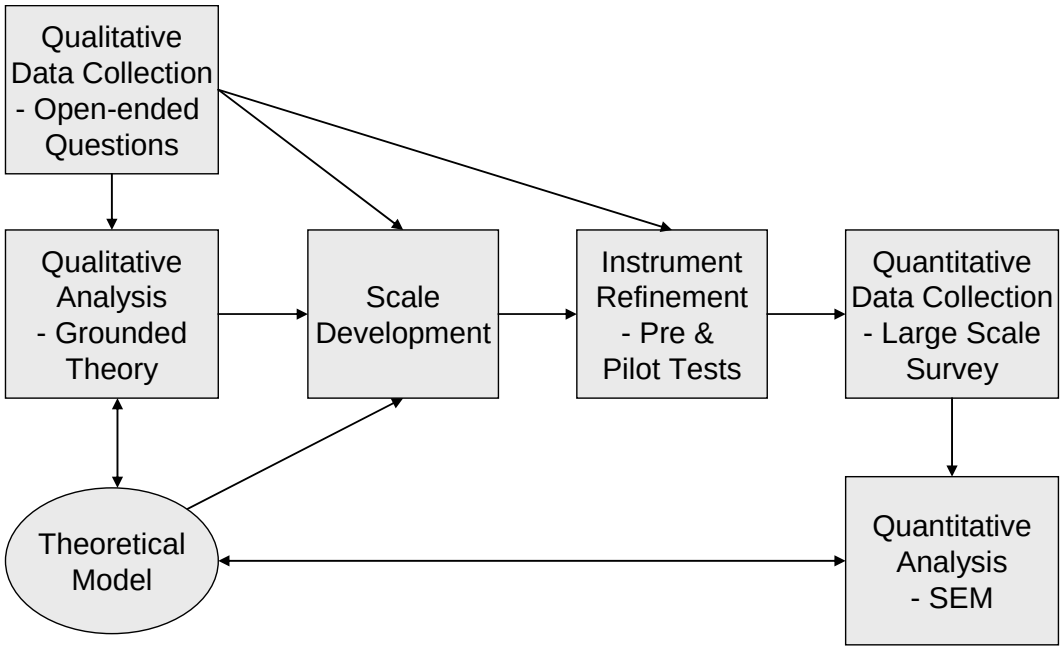


Figure 2. *Six Methodology Steps*

Step One - Qualitative Data Collection - Open-ended Questions

In September 2003, an announcement was placed on the $(ISC)^2$ home page (www.isc2.org) calling for CISSP volunteers interested in participating in this research project. $(ISC)^2$ is a non-profit organization that manages the CISSP program. Among the requirements to earn a CISSP designation, candidates must pass a comprehensive exam, agree to a code of ethics, and possess a minimum of four years of professional experience in the field or three years experience plus a college degree. To maintain certification, a CISSP must earn continuing professional education credits.

In all, 348 CISSPs responded to the web posting and subsequently received two open-ended questions. Open-ended questions have the advantage of allowing the respondent to answer in a relatively unconstrained way. Open-ended questions allow answers to include finer details to the satisfaction of the respondent and can for this

reason be more motivating (Kidder & Judd, 1986). The first open-ended question asked for the top five information security issues facing organizations today. Three weeks later, a second question asked for the top five *policy* related issues in information security. Participants answered both questions using a word processing form designed with a space for both a short-title and an accompanying rationale for each issue. Ten CISSPs pre-tested the forms. Of the 348 CISSPs, 220 returned useable responses. Electronic mail was the sole communication medium for this phase. Responses to the questions provided the qualitative data for this research.

While the sample was homogeneous to the $(ISC)^2$ constituency, a wide range of geographic regions and industries were represented. The respondent pool came from 23 countries with industry participation reflective of the types of organizations that hire information security professionals. Fifteen percent of the sample identified themselves as consultants. This group provided a valuable perspective since many of them support different-sized companies from multiple industries. Table 3 lists the demographic features of the sample.

The sample is notable for several reasons. First, the qualitative phase of the research project benefited from a large number of open-ended question responses. The first question provided 1,100 comments (220 usable responses at 5 issues each) and the second provided 990 comments (198 usable responses at 5 issues each). The total responses contained over 147,000 words, offering a collection of rich content suitable for qualitative analysis. Second, the sample of practicing security professionals allowed the acquisition of data from those who are highly knowledgeable about current organizational security issues. Third, use of the $(ISC)^2$ constituency ensured a minimum

level of professional credentials. Fourth, the $(ISC)^2$ constituency represents a sub-culture due to its rigorous admission and ongoing certification requirements. Finally, the $(ISC)^2$ constituency includes a wide variety of job types within a representative cross-section of numerous industries. Respondent comments thus provide a rich set of data containing a variety of organizational views.

Table 3. *Sample Characteristics of CISSPs Responding to Open-ended Question*

Respondents:	220 certified information system security professionals
Country:	23 countries represented including: - United States (72%) - Canada (5%) - India (4%) - Hong Kong (3%) - United Kingdom (3%)
Industry:	Largest represented include: - government (21%) - consulting (15%) - banking & finance (15%) - information technology (12%) - manufacturing (11%) - telecommunication (8%) - healthcare (7%) - energy (4%)
Job position:	- top management & business owners (11%) - middle management (34%) - professional/administrative (32%) - other management (23%)
Information Sources[3]:	- Information Security magazine (30%) - SANS Institute (29%) - Security Focus (18%) - SC Magazine (9%) - CERT web site (9%) - CSO magazine (7%) - Search Security (5%) - ISSA Journal (4%)

[3] Participants named their two primary sources of security news & information, whether electronic or print. The percent of respondents mentioning each source is provided. All sources with at least 4% are listed.

Step Two - Qualitative Analysis - Grounded Theory

Grounded theory entails a series of highly structured steps involving the systematic comparison of units of data (i.e., the question responses) and the gradual construction of a system of categories describing the observed phenomena. This approach involves the discovery of emergent theory from qualitative, empirical data. The grounded theory methodology attempts to discover theory from data systematically obtained from social research (Glaser & Strauss, 1967) can be divided into three coding phases: open, axial, and selective (Gasson, 2004; Orlikowski, 1993; Strauss & Corbin, 1998). The following paragraphs provide a short description of each phase.

Open coding is a technique that uses a form of content analysis to categorized data into concepts originating from the data rather than pre-defined assumptions from an outside source. Specifically, the respondent's short-titles of each issue along with a frequency analysis of key words and phrases in the rationales were the primary means of category identification. With this open-coding approach, 57 issue categories were identified from the text of the qualitative data. Appendix A contains the list of categories after the open coding stages.

Axial coding seeks to identify a set of stable and common categories that link a number of associated concepts. It's a technique used to identify relationships between themes discovered in the open coding process to allow for the development of a more consolidated, yet comprehensive scheme (Kock, 2004; Orlikowski, 1993). In this process, a researcher reduces an original list of concepts to allow for a more select and focused analysis (Glaser & Strauss, 1967). From the 57 issues identified in open coding, a consolidated list of 25 issues developed.

There have been calls in the IS literature for a more rigorous approach to grounded theory research. Gasson (2004) presents a number of quality measures to improve rigor in grounded theory research including the process of regularly justifying emerging constructions to critical colleagues. To act on this, the list of 25 identified issues along with a definition of each category was returned to the 220 participants requesting critical feedback. This request had two purposes. The first was to validate the issue categories by asking the participants to provide feedback about the issues and associated definitions. The second was to obtain a preliminary ranking of the 25 issues. Of the 220 CISSPs, 115 responded. Of the 115 responses received, ten included critical comments with their rankings. The remaining 105 ranked the issue list without comment. The comments helped to further refine some of the issue categories.

This validation round was an important process. It subjected the list of 25 issue categories to a round of critical feedback from content area experts while providing the investigator with an initial list of prioritized security issues. The validation round enhanced the soundness and relevancy of the 25 issues. This prioritized list was useful since many of these issues represent potential constructs in a theoretical model. Appendix B contains the list of 25 issues prioritized by the 115 CISSPs. [4]

Following open and axial coding, selective coding is a grounded theory technique used to group interrelated categories into theoretical models (Strauss & Corbin, 1998). Within this study, selective coding consisted of an iterative process of examining the 25 categories and reevaluating the responses from the two open-ended questions. This

[4] A summary report of this process including a subsequent ranking of the 25 issue categories by 874 CISSPs is provided in Appendix C.

process surfaced patterns in the qualitative responses suggesting theoretical relationships among the issues revealed from the axial coding phase. In addition, the prioritized list of 25 issues aided in theoretical development by identifying the most critical issues for consideration in a theoretical model. The selective coding approach of analyzing the open-ended responses led to a theoretical model containing six constructs.

Theoretical model of this study. The theoretical model of this project emerged from studying the qualitative text and looking for relationships among and between the identified managerial constructs. After this iterative process of model construction and then comparing the model back to the qualitative data and modifying it as necessary, a final model with six constructs emerged. The model suggests that the relationship between top management support and perceived security effectiveness is partially mediated by user training, security culture, policy relevance and policy enforcement. Additionally, user training is positively associated with security culture.

A mediator is defined as a variable that explains the relation between an independent and dependent variable. Mediation is a mechanism through which an independent variable, such as top management support, influences a dependent variable, such as security effectiveness (Baron & Kenny, 1986; Frazier, Barron, & Tix, 2004). Figure 3 provides a general, full mediation model. Figure 4 illustrates the hypothesized partial mediation model. Table 4 contains formal statements of hypothesis. Table 5 provides twenty examples of respondent statements from the open-ended questions that support the six hypotheses. Underlined words refer to the independent and mediating variables of the hypothesized model. The selected statements are typical of the larger body of responses. Each statement provides some support for at least one of the

hypothesized paths in the theoretical model. To the highest degree possible, the statements are sequentially ordered based on the hypotheses they support (e.g. responses supporting H1 and H2 are toward the beginning of Table 5).

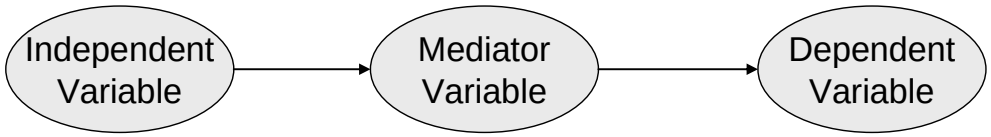


Figure 3. *General Full Mediation Model*

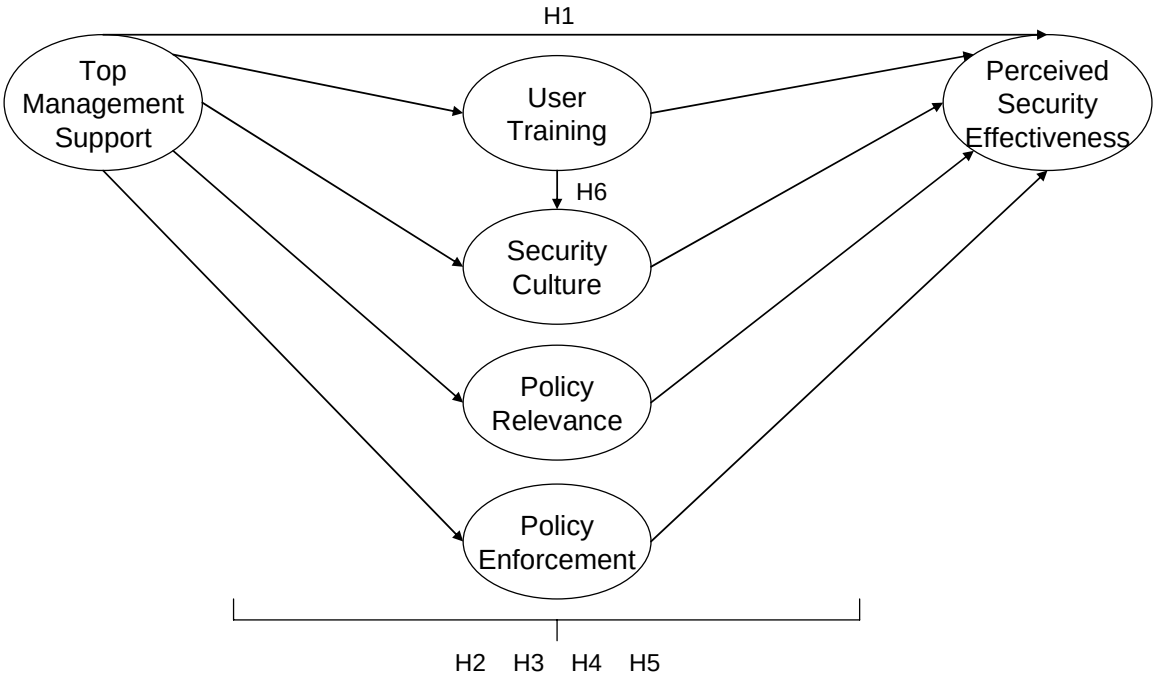


Figure 4. *Hypothesized Partial Mediation Model*

Table 4. *Formal Hypotheses*

H1	*Top management support is positively associated with perceived security effectiveness.*
H2	*Top management support and perceived security effectiveness is partially mediated by user training.*
H3	*Top management support and perceived security effectiveness is partially mediated by security culture.*
H4	*Top management support and perceived security effectiveness is partially mediated by policy relevance.*
H5	*Top management support and perceived security effectiveness is partially mediated by policy enforcement.*
H6	*User training is positively associated with security culture.*

Table 5. *Statements Supporting the Hypothesized Model*

Qualitative statements from the CISSP sample that support the six hypotheses of this study.	*H 1*	*H 2*	*H 3*	*H 4*	*H 5*	*H 6*
"It is imperative to have top management support all security programs…If there's no management support, real or perceived, all INFOSEC programs will fail."	√	√	√	√	√	
"The bottom line is senior management must accept ownership for all information security decisions and the corresponding policies along with them."	√	√	√	√	√	
"The importance of information security by the company's leadership permeates throughout the organization resulting in either successful or poor information security programs."	√	√	√	√	√	
"It is part and parcel of the security lifecycle to constantly keep management involved in security as it is from their approval and understanding which matters most in a successful security implementation"	√	√	√	√	√	
"In most enterprises' cultures, security or risk management is not included in the normal training process with any depth or impact. The primary cause of this is little or no senior management recognition"		√	√			√

Qualitative statements from the CISSP sample that support the six hypotheses of this study.	*H 1*	*H 2*	*H 3*	*H 4*	*H 5*	*H 6*
"Obviously, without top management support and involvement, the creation, training and enforcement of the organization's security policies…would not be taken seriously by the employees. Top management support must happen first if the other issues are to be handled effectively."		√		√	√	
"Management buy-in and increasing the security awareness of employees is key. Technology is great, but without the culture change that embraces security and Management's backing, all the bits in the world won't help."		√	√			√
"Lack of awareness among the users will always hinder the right attitude towards a secure business practice."		√	√			√
"Awareness training will do more for security effectiveness than any new firewall or intrusion prevention system."		√				√
"Information security is not just about technical controls; it encompasses the whole culture of the organization. The cultural improvement can only be made by strategies involving user awareness and constant reminders."		√	√			√

Qualitative statements from the CISSP sample that support the six hypotheses of this study.	*H 1*	*H 2*	*H 3*	*H 4*	*H 5*	*H 6*
"Is the user and the entire organization trained on a recurring basis? Every user in the organization needs to learn how to be an information security steward."		√	√			√
"Awareness training or education is important to build the security culture"		√	√			√
"Without an established and widespread awareness and education effort it is difficult if not impossible to integrate security into the corporate culture."		√	√			√
"There needs to be a master plan that identifies realistic training requirements, identifies resources needed to implement the plan, and has management support to ensure that the program is carried out effectively."		√				
"[T]he senior leadership example…can foster an institutional culture that recognizes the importance of information to the survival of the organization and the criticality of protecting this information."			√			
"Executive management must take an active role in the…enforcement of all corporate policies. Without this support from the organization's leadership, any policies that do get distributed will not be totally effective."				√	√	

Qualitative statements from the CISSP sample that support the six hypotheses of this study.	*H 1*	*H 2*	*H 3*	*H 4*	*H 5*	*H 6*
"Senior management support is critical to foster an environment where security policies can be initiated, discussed, approved, and implemented at all levels in the organization."			√	√	√	
"Policy development, enforcement, and ultimately support, is too often relegated to lower-level management where it sits in the queue … ultimately diminishing the … effectiveness of the security organization."				√	√	
"Frequent security policy updates need to happen in a timely manner…we see policy updates as an important task."				√		
"Enforcement (and) policy violations may also be an excellent indicator for security staffs on the effectiveness of their policies, …, and the general security state of the organization."					√	

Step Three - Scale Development

Considering the limited empirical studies in information security (Bento & Bento, 2004; Kotulic & Clark, 2004), the scarcity of existing scales that apply to the research question, and the substantial content obtained from the qualitative data in this study, the researcher began development of new measurement scales. The scales were developed through an iterative process of extracting words and phrases from the open-ended question responses to develop candidate questionnaire items. This approach assured that both the content and the language of the questionnaire items would be familiar to the likely sample and thus reduce possible construct bias (Karahanna, Evaristo, & Srite, 2004).

Psychometricians emphasize that the validity of a measurement scale is built in from the outset. Careful construction of the initial scale items helps to assure that they will representatively cover the specified domain of interest, and thus possess content validity (Nunnally, 1978). While it is impossible to specify the optimum number of items to be included in an item pool (DeVellis, 2003), researchers should anticipate that less than one half of the extracted items will be retained in the final scales (Hinkin, 1998).

The grounded theory technique of theoretical saturation (Gasson, 2004; Strauss & Corbin, 1998) was extended and applied as a guide to help determine the number of items appropriate for the item pool. Theoretical saturation implies that when adding items to the pool contributes little marginal value to the scale or seems counterproductive, the construct scale may be theoretically saturated. This approach links the size of the candidate item pool to the assessed content domain.

Using this approach, the researcher generated construct items until the addition of new items contributed little to the scale, indicating that theoretical saturated was reached for a particular construct. Using various word combinations from the existing items, the size of the item pool was then doubled (Hinkin, 1998) to ensure that an adequate number of items would be available in the final scales after instrument refinement. At this stage of scale development, many items appeared redundant. However, redundant items can be a desired quality and many scales require a level of redundancy (DeVellis, 2003) for acceptable reliability. Testing for instrument construct validity began once the quality and quantity of the item pool seemed satisfactory with theoretical saturation and acceptable redundancy.

Step Four - Instrument Refinement

Expert panel evaluation. This step had two major focal areas. The first concerned the construct validity of the candidate survey items. The second concerned the perceived sensitive nature of the questions asked. A panel of twelve experts evaluated each candidate item from these two perspectives (construct validity and intrusiveness). The researcher handpicked the twelve panelists from the 220 CISSP participants of the open-ended question based on the high quality and critical skills displayed in their previous responses.

For construct validity, expert panelists matched each item in the item pool to one of seven constructs in two separate evaluation rounds. The seven constructs in the scale included the independent and mediating variables used in this study (top management support, security culture, policy enforcement, policy relevance, and user training) plus two additional choices (policy development and organizational governance). Panelists

were given definitions of each construct to reference during the evaluation. The panelists were encouraged to comment and make suggestions for improvement to the items. In total, the twelve expert panelists provided over 50 comments on specific items.

Items that obtained at least a 75% agreement rate among the panelists were retained for the survey (Hinkin, 1995, 1998). If the agreement rate was less than 75% the item was dropped or modified. In the first round, 65% of the items produced the required 75% panelist agreement. While this round produced a sufficient number of items for five of the intended constructs, it did not produce sufficient items for the security culture construct. Thus, the primary goal of the second round was to produce a sufficient number of security culture items. To do so, the open-ended responses and literature were consulted (Detert et al., 2000; Klein et al., 1995) to generate additional items. In the second round, 84% of the new and refined questions produced the required 75% agreement including a sufficient number of items for the culture construct.

Although this item-to-construct matching process is not a guarantee of construct validity, this refinement effort produced a list of 70 content-oriented questionnaire items that exhibited preliminary evidence of construct validity (Segars & Grover, 1998) for the constructs of this study. This important step helped minimize potential problems such as cross-loading of items across constructs.

The second focus area was concerned with the problem of the perceived sensitive nature of security-related questions. In-part because of the intrusive nature of the subject, many previous studies in information security have experienced poor response rates (Kankanhalli et al., 2003; Kotulic & Clark, 2004). Some consider information security research an extremely sensitive topic (Straub & Welke, 1998) and recommend a cautious

approach when attempting studies because of a general mistrust by practitioners of any attempt to gain data about the practices and behaviors of security professionals (Kotulic & Clark, 2004). This recommendation by Kotulic & Clark is based on the results of a follow-up questionnaire given to a sample of survey non-respondents. Responses from 74 'non-respondent' firms showed that 23% did not participate because they do not share any information about computer security policies with outside entities. Another 10% stated the questionnaire appeared to contain items that require answers revealing proprietary information.

Overly sensitive questions are also a potential source of undesirable method bias because they can influence the assessment of particular traits (Spector, 1994). For this reason, development of a non-intrusive instrument is important to reduce this form of method variance by encouraging subjects to respond thoroughly and candidly to the research questions. This notation of method variance is different from the better known notion that method variance is inherent in a particular method, like a questionnaire, because two or more measures come from the same source, and a defect in that source contaminates all traits assessed by that method (Campbell & Fiske, 1959).[5]

To minimize the problem of unacceptably high levels of perceived intrusiveness, the same expert panel of 12 CISSPs evaluated each item using a developed willingness-to-answer scale provided in Table 6. While a certain level of perceived intrusiveness is unavoidable, only items with acceptable intrusive scores were retained. This step is critical especially in the domain of security because items perceived to be unacceptably

[5] The present study will attempt to control for both forms of method variance.

intrusive may discourage or influence survey completion. The following guideline to help evaluate the perceived intrusiveness of each item was established. An acceptable item should:

- be rated as either slightly (3) or not intrusive (4) by at least 70% of the panelists and
- have a mean score from all the panelists of at least a 2.75 on a 4.0 scale.

In addition to scoring every item by the willingness-to-answer scale, some of the feedback from the expert panel addressed the more intrusive items in the pool. For instance, a panelist commented about one problem item, "(I) find it hard to believe you would get an honest or accurate answer" and subsequently rated the item as *unacceptably intrusive*. Based on this and other feedback, the item was dropped. Combining both the intrusiveness scores with the expert feedback from the panel helped with the evaluation of problematic items and with the instrument refinement process overall.

Table 6. *Willingness-to-Answer Scale*

Scale		Definition
1.	Unacceptably Intrusive	Many respondents may be unwilling to answer; a problem question.
2.	Moderately Intrusive	Some respondents may be unwilling to answer.
3.	Slightly Intrusive	A small number of respondents may be unwilling to answer.
4.	Not Intrusive	Respondents should be willing to answer; the question is OK

Based on the expert panel results, perceived intrusiveness problems did not surface with four of the six constructs in the theoretical model. All of the initial items developed to measure the top management support, security culture, user training, and policy relevance constructs met the above two guidelines. However, 22% of the initial policy enforcement and 33% of the perceived security effectiveness items did not. Table 7 and Table 8 contain the twelve panelist's intrusiveness scores for all the policy enforcement and perceived effectiveness questions from the initial item pool, respectively.

A final guideline was established that the overall instrument may be judged acceptable if each item passes the above two conditions and the mean of all the items on the instrument exceeds 3.5 out of a 4.0. In all, intrusiveness scores provided by the expert panel led to the removal or modification of 13% of the initial candidate items. The

mean score of the remaining questions, after removal of intrusive questions, was a 3.64, suggesting that the survey instrument was not overly intrusive.

Table 7. *Intrusiveness Scores for Initial Policy Enforcement Items*

Proposed Survey Question (Item)		Slightly or Not Intrusive	Mean Score (4.0 max)
Security policies have no teeth. [Reverse Code (RC)]	*dropped*	50%	2.75
There is conflict between security staff and employees regarding policy enforcement. (RC)	*dropped*	67%	3.00
Policies are selectively enforced. (RC)	*dropped*	67%	3.00
Computer security abuses often go unpunished. (RC)	*dropped*	67%	2.75
Policies are consistently enforced on senior management.		75%	3.17
Employees caught violating important security policies are appropriately corrected.		92%	3.50
Security policies are properly monitored for violations.		92%	3.42
Security staff has adequate automated tools to enforce policy.		92%	3.67
Security officers have the necessary authority to enforce policy.		92%	3.58
Information security policies are appropriately enforced on external parties (contractors, suppliers, etc.).		92%	3.58
Employee computer practices are properly monitored for policy violations.		92%	3.42
Information security policy is properly enforced.		100%	3.67
Employees clearly understand the ramifications for violating security policies.		100%	3.67
Policies are consistently enforced across the organization.		100%	3.50
Discovered security policy violations are reported to the proper authority.		100%	3.58
Information security rules are enforced by sanctioning the employees who break them.		100%	3.75
Repeat security offenders are appropriately disciplined.		100%	3.58
Termination is a consideration for employees who repeatedly break security rules.		100%	3.75

Table 8. *Intrusiveness Scores for Initial Perceived Security Effectiveness Items*

Proposed Survey Question (Item)		Slightly or Not Intrusive	Mean Score (4.0 max)
Sensitive information is sufficiently protected.	*dropped*	45%	2.42
Valuable information is effectively secured.	*dropped*	64%	2.58
Our organization has adequate computer security.	*dropped*	64%	2.67
The information security program has kept security losses to a minimum.		73%	2.75
The information security program is successful.		73%	2.75
The information security program achieves most of its goals.		92%	3.67
Generally speaking, information in the organization is sufficiently protected.		92%	3.17
Overall, the information security program is effective.		92%	3.67
The information security program accomplishes its most important objectives.		100%	3.75

The willingness-to-answer scale was not the only consideration for reducing perceived intrusiveness. Other factors may influence a potential respondent's participation more than simply perceived intrusiveness of the questionnaire's items. Some of these possible factors include the visible sponsorship of a research project by a reputable organization such as $(ISC)^2$, clearly written survey instructions, approval of a university human subjects office, implementation of secure sockets layer encryption at the survey web site, a posted privacy policy, and a general impression of professionalism. This study addressed all of these factors in an effort to minimize the perception of intrusiveness.

Using the results from the expert panel, a web-based questionnaire was developed. To reduce the potential for order bias, the content items appeared in random order for each respondent. Nine CISSPs and nine academics pre-tested the survey resulting in some minor format changes to the web survey to enhance readability. After this, the survey was prepared for the pilot-test.

Pilot test results. A convenience sample of 68 CISSPs, who did not participate in the open-ended questions, pilot tested the instrument. The characteristics of the sample are contained in Tables 9 and 10.

Table 9. *Country Demographics (pilot)*

Country	Count	Percent	Country	Count	Percent
			United		
United States	34	50.0	Kingdom	2	2.9
Canada	5	7.4	Australia	1	1.5
Other[6]	5	7.4	Korea (South)	1	1.5
Germany	3	4.4	Malaysia	1	1.5
India	3	4.4	Portugal	1	1.5
Brazil	2	2.9	Saudi Arabia	1	1.5
Finland	2	2.9	South Africa	1	1.5
Hong Kong	2	2.9	Sweden	1	1.5
New Zealand	2	2.9	Turkey	1	1.5
			Total	68	100%

[6] Countries with fewer than 10 CISSPs are listed as 'other'.

Table 10. *Industry Demographics (pilot)*

Industry	Count	Percent			
Government-central, local, military, etc.	23	19.7	Industrial Tech	3	2.6
Consulting	21	17.9	Utilities	3	2.6
Info Tech-Security-Telecomm	21	17.9	Education/Training	2	1.7
Finance, Banking & Insurance	10	8.5	Energy	2	1.7
Manufacturing	8	6.8	Travel/Hospitality	2	1.7
Medical/Healthcare - public or private	6	5.1	Entertainment	1	0.9
Consumer Products/Retail/Wholesale	5	4.3	Non-profit	1	0.9
Professional Service (legal, marketing, etc.)	4	3.4	Real Estate	1	0.9
Other	4	3.4	Total	117[7]	100%

An important goal of this phase was continued scale refinement through item reduction. Hinkin (1998) recommends analyzing inter-item correlations. While there are no hard-and-fast rules on this, items that did not correlate above .45 with other items were deleted. This benchmark is slightly above the .40 figure referenced by Hinkin. Using this method, about 10% of the items were deleted because they did not correlate well with other items.

Since factor analysis is a large sample technique, the sample size of the pilot test (N=68) did not allow for a reliable test of the full theoretical model. However, a confirmatory approach tested each individual construct. Hinkin (1995) states a confirmatory approach is recommended over an exploratory (e.g., principal axis

[7] Respondents could select more than more industry.

factoring) because a confirmatory allows the researcher more precision in evaluating the measurement model. Table 11 presents each of the measurement scales with selected fit indices and reliability scores. Table 12 through Table 14 lists all the items for each of the independent, mediating, and dependent variables in the proposed model, respectively. Later in Chapter IV is an appropriate description of each of the fit indices and measures provided in the tables.

Table 11. *Construct Fit Indices (pilot)*

Construct	# of Items	χ^2	df	*p*	Adj χ^2	GFI	RMSEA	CFI	Alpha
Top Mgt Support	6	10.20	9	.334	1.13	.95	0.045	.99	.94
User Training	6	10.60	9	.298	1.19	.95	0.053	.99	.93
Security Culture	6	5.94	9	.746	0.66	.97	0.000	1.00	.94
Policy Relevance	8	22.91	19	.241	1.21	.93	0.055	.99	.91
Policy Enforcement	4	0.97	2	.616	0.48	.99	0.000	1.00	.91
Perceived Effectiveness	5	5.49	5	.359	1.10	.97	0.038	.99	.91

Table 12. *Independent Variable Measurement Scales*

Concept: Top Management Support of Organizational Security Program

Construct Name: Top Management Support

Aliases: Executive Support, Senior Management Championship

Code & Items:

TM1	Top management considers information security an important organizational priority.
TM2	Top executives are interested in security issues.
TM3	Top management takes security issues into account when planning corporate strategies.
TM4	Senior leadership's words and actions demonstrate that security is a priority.
TM5	Visible support for security goals by senior management is obvious.
TM6	Senior management gives strong and consistent support to the security program.

Table 13. *Mediating Variables Measurement Scales*

Concept: Organizational Security Training and Awareness

Construct Name: User Training

Aliases: Security Training, Security Awareness, Security Education, Employee Training

Code & Items:

UT1	Necessary efforts are made to educate employees about new security polices.
UT2	Information security awareness is communicated well.
UT3	A variety of business communications (notices, posters, newsletters, etc.) are used to promote security awareness.
UT4	An effective security awareness program exists.
UT5	A continuous, ongoing security awareness program exists.
UT6	Users receive adequate security refresher training appropriate for their job function.

Concept: Organizational Security Culture

Construct Name: Security Culture

Aliases: Culture, Security Culture, Organization Culture, Security Attitude, Climate

Code & Items:

SC1	Employees value the importance of security.
SC2	A culture exists that promotes good security practices.
SC3	Security has traditionally been considered an important organizational value.
SC4	Practicing good security is the accepted way of doing business.
SC5	The overall environment fosters security-minded thinking.
SC6	Information security is a key norm shared by organizational members.

Table 13. *Mediating Variables Measurement Scales* (continued.)

Concept: Organizational Security Policy Relevance

Construct Name: Policy Relevance

Aliases: Policy Alignment, Policy Currency, Policy Maintenance, Policy Review

Code & Items:

PR1	Information security policy is consistently updated on a periodic basis.
PR2	Information security policy is updated when technology changes require it.
PR3	Policy is updated when legal & regulatory changes require it.
PR4	An established information security policy review and update process exists.
PR5	Security policy is properly updated on a regular basis.
PR6	Information security policies are aligned with business goals.
PR7	Information security policies reflect the objectives of the organization.
PR8	Risk assessments are conducted prior to writing new security polices.

Concept: Organizational Security Policy Enforcement

Construct Name: Policy Enforcement

Aliases: Policy Monitoring, Policy Auditing, Security Enforcement

Code & Items:

PE1	Employees caught violating important security policies are appropriately corrected.
PE2	Information security rules are enforced by sanctioning the employees who break them.
PE3	Repeat security offenders are appropriately disciplined.
PE4	Termination is a consideration for employees who repeatedly break security rules.

Table 14. *Dependent Variable Measurement Scale*

Concept: Organizational Security Program Effectiveness

Construct Name: Perceived Security Effectiveness

Aliases: Security Success, Security Adequacy, Perceived Effectiveness

Code & Items:

EF1	The information security program achieves most of its goals.
EF2	The information security program accomplishes its most important objectives.
EF3	Generally speaking, information is sufficiently protected.
EF4	Overall, the information security program is effective.
EF5	The information security program has kept risks to a minimum.

Step Five - Quantitative Data Collection - Large-scale Survey

An email notification was sent by $(ISC)^2$ to its member CISSPs inviting them to participate in this research project. Data was collected in three-phases through a secure web site and spreadsheet attachment sent by email. The three-phased approach is described in this section.

Control of common method variance. Common method variance is a type of method bias where variable correlations are vulnerable to artificial inflation (or deflation) due to the method used during data collection. Common method variance is one of the main sources of measurement error and can threaten the validity of empirical research conclusions (Campbell & Fiske, 1959; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). It can be a particular concern with self-reported questionnaire surveys where predictor and criterion variables are gathered from the same source. Investigators can strengthen their research studies by taking steps to control for this validity threat. However, one analysis of 116 IS published studies that potentially had a problem with common method bias revealed that only 12 specifically mentioned this issue at all (Whitman & Woszczynski, 2004). This is unfortunate considering that anecdotes on how to minimize the problem of common method variance have been available in the literature (Podsakoff & Organ, 1986; Straub, 1989).

The key to controlling method variance is to identify what the measure of the predictor and criterion variables have in common and to minimize it through the design of the study. A number of procedural and design remedies to reduce common method variance are used in this project (Podsakoff et al., 2003; Podsakoff & Organ, 1986) and are illustrated in Figure 5. First, at least a three-day hiatus separated the collection of the

independent, mediator, and dependent variables. Second, different response formats were used through modified Likert scales and changed media. Third, given *H6* in the hypothesized theoretical model (see Figure 4), the collection of the user training variable on the web survey is separated from the collection of the security culture, policy relevance and policy enforcement variables. This separation is illustrated as Block A and Block B in Figure 5. Between the blocks is the Van Der Vegt et al *task interdependence* scale and one open-ended question.

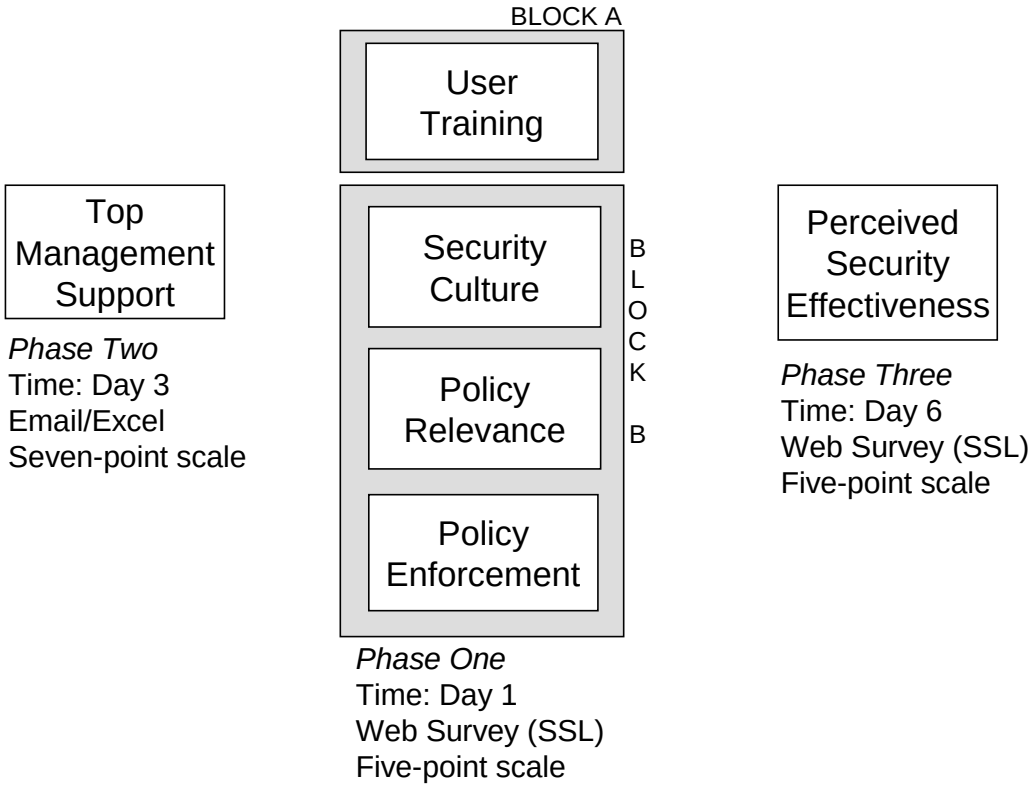


Figure 5. *Data Collection Remedies to Control for Common Method Variance*

Procedural remedies such as inserting temporal lags in the data collection process helps to control common method variance by mitigating the problems such as *transient*

mood states, consistency motifs, and *hypothesis guessing*. *Transient mood states* of respondents produced from any of a number of events (e.g. receiving a compliment from a boss, interacting with a disgruntled customer, hearing rumors about layoffs) may inflate artifactual covariance in self-report measures because the respondent answers questions about independent and dependent variables while in the same mood (Spector, 1992). The *consistency motif* suggests that people try to maintain consistency between their cognitions and attitudes. Respondents may answer questions in a way to appear consistent and rational. The consistency motif is likely to be problematic when respondents are asked to provide retrospective accounts of their attitudes and perceptions (Podsakoff et al., 2003). *Hypothesis guessing* occurs when respondents recognize the thrust of the questionnaire items, and then begin to answer in a manner that confirms (or disconfirms) researcher expectations (Orne, 1979; Straub, Limayem, & Karahanna-Evaristo, 1995). Hypothesis guessing could especially be a problem when the sample is highly educated, such as the case with CISSPs. In addition to the temporal separation of variables, the title of the survey will be worded in a manner as not to reveal the intention or goal of the research (e.g. *Critical* Issues in Information Security instead of *Managerial* Issues in Information Security).

Step Six - Quantitative Data Analysis – Structural Equation Modeling

In the following chapter, a detailed analysis is conducted on the data collected in step 5. Confirmatory factor analysis (CFA) techniques using the Amos 5.0 software program tests for important statistical validities (Straub et al., 2004). The instrument is tested for reliability as well as construct, convergent, and discriminant validity.

Mediation effects and common variance sources are tested. Demographic sub-samples are evaluated. Moreover, an alternative theoretical model is proposed and tested.

Summary

This research study involves six methodological steps combining both qualitative and quantitative techniques. The qualitative portion of the methodology relies on the grounded theory research strategy to generate a theoretical model depicting conceptual relationships among key managerial constructs in information security. Rigorous standards are applied to scale development including the use of an expert panel to evaluate the items for construct validity and perceived intrusiveness. The methodology applies procedural remedies to control for common method variance. Overall, the methods used in this study combine grounded theory with structural equation modeling in a way to provide a richer, contextual basis for interpreting and validating results.

Chapter IV provides the results of the large-scale empirical survey.

CHAPTER IV

RESULTS

This chapter presents a quantitative analysis of the large-scale survey data collected for this study. The chapter is divided in nine parts. First, data preparation and sample demographics are described. Second, statistical analysis and validities of each construct are provided. Third, the *a priori* measurement and path models are evaluated. Fourth, mediation effects are tested. Fifth, a demographic analysis of the data using the *a priori* model is presented. Sixth, an alternative, second-order factor mediation model is considered. Seventh, a demographic analysis of the data using the alternative model is provided. Eighth, an examination of common variance is conducted. Finally, results of the *task interdependence* scales are analyzed.

Data Preparation and Sample Demographics

Survey invitation to the research sample. A single email notification was sent to approximately 30,000 constituents of the $(ISC)^2$ organization inviting them to participate in the research survey. The message was an official 'e-blast' containing one other unrelated item of constituency business. Considering that $(ISC)^2$ constituents were invited to participate in at least four other survey questionnaires in the past year, a monetary incentive was offered to encourage participation. No follow-up emails were sent to non-respondents. Appendix D provides the text of the email invitation. Table 15

lists the survey response rates by phase and the average time for respondents to complete each of the phases.

Table 15. *Sample Size and Response Rates by Phase*

	Phase 1	Phase 2	Phase 3	Usable
N	936	760	743	740
Response Rate	3% of 30,000	81% of Phase 1	79% of Phase 1	79% of Phase 1
Actual Mean of Temporal Separation	Day 1	Day 4.5	Day 9	---

Initial data preparation. 743 CISSPs completed all three phases of the survey. This sample size is considered large for the purposes of this study. In multivariate analyses and interpretation, when sample size is in excess of 400, the researcher should be cautious by examining all significant results to ensure that they have practical significance due to the increased statistical power from the larger sample size (Hair, Anderson, Tatham, & Black, 1998).

Data preparation included standardizing the phase two, seven-point Likert scale to a five-point scale. Mean imputation was used to fill missing values; however, only two-tenths of one per cent of the total values were missing. Three outliers were removed based on a frequency bar chart of Mahalanobis Distance values, leaving a final data set of 740 responses. Additionally, no evidence of unacceptable skewness, kurtosis, or

multicollinearity was found. Among the variables in the study, the data met the conditions of multivariate normality.

Sample demographics. Table 16 through Table 21 provides the demographics of the sample (N = 740).

Table 16. *Country Demographics*

Country	Count	Percent	Country	Count	Percent
United States	402	54.3%	Ireland	4	0.5%
Canada	60	8.1%	Mexico	4	0.5%
United Kingdom	36	4.9%	Nigeria	4	0.5%
Hong Kong	20	2.7%	Israel	3	0.4%
Australia	18	2.4%	Japan	3	0.4%
India	17	2.3%	Philippines	3	0.4%
Netherlands	16	2.2%	Spain	3	0.4%
Other[8]	13	1.8%	Turkey	3	0.4%
Finland	12	1.6%	United Arab Emirates	3	0.4%
Singapore	12	1.6%	Bermuda	2	0.3%
China	9	1.2%	Croatia	2	0.3%
South Africa	8	1.1%	Greece	2	0.3%
Russian Federation	7	0.9%	Luxembourg	2	0.3%
Brazil	6	0.8%	Portugal	2	0.3%
Korea, South	6	0.8%	Switzerland	2	0.3%
Malaysia	6	0.8%	Taiwan	2	0.3%

[8] Countries with fewer than 10 CISSPs are listed as 'other'.

Country	Count	Percent	Country	Count	Percent
Sweden	6	0.8%	Thailand	2	0.3%
Italy	5	0.7%	Columbia	1	0.1%
New Zealand	5	0.7%	Egypt	1	0.1%
Saudi Arabia	5	0.7%	Hungary	1	0.1%
Belgium	4	0.5%	Kuwait	1	0.1%
Denmark	4	0.5%	Pakistan	1	0.1%
France	4	0.5%	Slovakia	1	0.1%
Germany	4	0.5%	not provided	3	0.4%
			Total	740	100%

Table 17. *Organization Size*

Employees	Count	Percent
less than 500	193	26%
between 500-2,499	122	16%
between 2,500-7,499	120	16%
between 7,500-15,000	60	8%
greater than 15,000	245	33%
Total	740	100%

Table 18. *Organization Position*

Organization Position	Count	Percent
Owner/Partner	23	3.1%
Senior manager/Executive (e.g. CEO, CIO)	31	4.2%
Department manager/supervisor/director	98	13.2%
Other managerial	21	2.8%
MIS/IS/IT/technical management	241	32.6%
Other IT/technical/scientific/professional	324	43.8%
Not provided	2	0.3%
Total	740	100%

Table 19. *Years of Information Technology & Security Experience*

Years	Count	Percent
less than 8	161	21.8%
between 8 and 15	326	44.1%
greater than 15	251	33.9%
not provided	2	0.3%
Total	740	100%

Table 20. *Years of Experience with Organization*

Years	Count	Percent
less than 1	114	15.4%
between 1 and 4	305	41.2%
greater than 4	317	42.8%
not provided	4	0.5%
Total	740	100%

Table 21. *Industry Demographics*[9]

Industry	Count	Percent
Info Tech, Security, Telecommunications	201	27.2%
Finance, Banking, Insurance	187	25.3%
Government	184	24.9%
Consulting	166	22.4%
Manufacturing	69	9.3%
Healthcare	63	8.5%
Other	50	6.8%
Consumer Products, Retail, Wholesale	47	6.4%
Education, Training	47	6.4%
Professional Services (legal, marketing, etc.)	30	4.1%
Utilities	29	3.9%
Energy	24	3.2%
Transportation, Warehousing	15	2.0%

[9] Respondents were free to indicate multiple industries

Industry	Count	Percent
Industrial Technology	14	1.9%
Non-Profit	13	1.8%
Travel & Hospitality	11	1.5%
Entertainment	6	0.8%
Publishing	5	0.7%
Real Estate, Rental, Leasing	4	0.5%

Statistical Analysis of Each Construct

Exploratory factor analysis. A factor analysis of the 35-item instrument was conducted using the SPSS 13.0 program. Table 22 illustrates the factor loadings using principal components analysis with varimax rotation. When sample sizes are in excess of 100, loadings above .50 are considered practically significant (Hair et al., 1998, p.112). For this study, each of the 35 items had a loading of at least .50 on its primary factor, indicating practical significance. However, a few items (i.e. SC2, PR6, PR7) had high cross-loads. Each of the six factors had an eigenvalue above 1.0, together accounting for 72% of the systematic variance.

Table 22. *Factor Loadings*[10]

Item #	Policy Relev (PR)	Top Mgt Support (TM)	User Train (UT)	Sec Cult (SC)	Per Effect (EF)	Policy Enforce (PE)
SC1	0.08	0.26	0.31	0.59	0.21	0.24
SC2	0.16	0.30	0.36	0.56	0.31	0.24
SC3	0.10	0.32	0.22	0.70	0.13	0.15
SC4	0.20	0.29	0.30	0.64	0.24	0.18
SC5	0.16	0.32	0.32	0.66	0.23	0.18
SC6	0.22	0.31	0.27	0.66	0.22	0.21
EF1	0.23	0.28	0.25	0.17	0.72	0.17
EF2	0.27	0.28	0.19	0.15	0.73	0.17
EF3	0.18	0.17	0.19	0.26	0.71	0.12
EF4	0.25	0.31	0.30	0.25	0.68	0.18
EF5	0.27	0.17	0.20	0.20	0.71	0.14
PE1	0.19	0.19	0.19	0.19	0.18	0.77
PE2	0.18	0.20	0.22	0.17	0.11	0.74
PE3	0.19	0.21	0.13	0.19	0.18	0.76
PE4	0.17	0.11	0.16	0.12	0.11	0.77
PR1	0.81	0.14	0.23	0.10	0.14	0.16
PR2	0.70	0.17	0.17	0.10	0.19	0.16
PR3	0.63	0.11	0.15	0.14	0.26	0.17

[10] Intended construct loadings are outlined.

Item #	Policy Relev (PR)	Top Mgt Support (TM)	User Train (UT)	Sec Cult (SC)	Per Effect (EF)	Policy Enforce (PE)
PR4	0.77	0.13	0.24	0.06	0.16	0.13
PR5	0.83	0.14	0.22	0.10	0.15	0.11
PR6	0.52	0.19	0.07	0.54	0.18	0.12
PR7	0.54	0.17	0.08	0.55	0.19	0.09
PR8	0.56	0.16	0.19	0.24	0.11	0.15
UT1	0.27	0.15	0.68	0.22	0.26	0.20
UT2	0.23	0.22	0.74	0.26	0.26	0.15
UT3	0.25	0.26	0.67	0.15	0.13	0.20
UT4	0.28	0.25	0.75	0.27	0.22	0.17
UT5	0.29	0.20	0.76	0.20	0.17	0.13
UT6	0.22	0.19	0.66	0.30	0.23	0.22
TM1	0.17	0.77	0.15	0.28	0.18	0.18
TM2	0.13	0.77	0.14	0.20	0.21	0.14
TM3	0.18	0.72	0.20	0.26	0.14	0.16
TM4	0.22	0.74	0.23	0.26	0.22	0.15
TM5	0.20	0.75	0.29	0.22	0.20	0.16
TM6	0.19	0.64	0.24	0.26	0.30	0.23
Eigenvalue	17.25	2.30	1.60	1.52	1.34	1.16
% Variance	49.3	6.6	4.6	4.3	3.8	3.3
Cumulative	49.3	55.9	60.4	64.8	68.6	71.9

Confirmatory factor analysis. Covariance-based structural equation modeling (SEM) with the Amos 5.0.1 program was used to test the model presented in Chapter III. The method of estimation is maximum likelihood. A process was followed where each of the measured factors were modeled in isolation, then in pairs, and then as a collective network (Segars & Grover, 1998). The measurement properties for the final constructs each modeled in isolation are presented in Table 24 through Table 29. Each of the measures presented in the tables are first briefly described.

Scale Reliability. Reliability is the pre-condition for validity. A Cronbach's alpha of .70 is considered the minimum acceptable standard for demonstrating internal consistency (Nunnally, 1978). Yet, through the use of factor analysis in aiding the decision to delete particular items that fail to adequately capture the sampling domain, reliability should be considerately higher than .70 (Hinkin, 1998). In the present study, the scales demonstrated acceptable reliability as evidenced by the Cronbach's alpha scores ranging from .87 to .93.

Measures of model fit. The most fundamental measure of overall fit is the chi-squared (χ^2) statistic. A large chi-square value relative to the degrees of freedom signifies that the observed and estimated matrices differ. Thus, we are looking for a non-significant p-value to indicate that the proposed model fits the observed covariances and correlations adequately. A recommended cutoff value for adjusted chi-square ranges from 2.0 (Im & Grover, 2004) to 5.0 (Jöreskog, 1970). However, use of the chi-square and the adjusted chi-square statistic is appropriate for sample sizes between 100 and 200 and can become less reliable with sample sizes outside this range. Because of this, researchers should combine chi-square with other goodness of-fit measures (Hair et al.,

1998). In the current study, because of the large sample (N=740), we complement the chi-square measure with other goodness-of-fit measures.

The Goodness-of-Fit (GFI) and Adjusted GFI (AGFI) indices represent an overall degree of fit. GFI values close to 1.0 indicate an overall good fit of the data to the proposed model with a generally accepted cut-off value of .90. However, some GFI tests indicate that the index behaves more consistently at sample sizes of 250 or greater (Hu & Bentler, 1995). The AGFI adjusts GFI by the ratio of degrees of freedom for the proposed model to the degrees of freedom for the null model. A recommended cut-off is .80 (Straub et al., 2004)

The Comparative Fit Index (CFI) and Normed Fit Index (NFI) are incremental fix measures that compare the proposed model to a baseline model, usually a single construct, null model. The CFI has been found to be more appropriate in a model development strategy and takes sample size into account (Byrne, 2001). With NFI and CFI, a recommended cut-off is .90 with values closer to 1.0 indicating a good fit (Hair et al., 1998).

The Root Mean Square Error of Approximation (RMSEA) attempts to correct for the tendency of the chi-square statistic to reject any specified model when the sample size is large. One study found the RMSEA was best suited in a competing models environment with larger sample sizes (Rigdon, 1996). A recommended cut-off is .08 with .05 indicating a close fit and .00 indicating an exact fit (Browne & Cudeck, 1993).

Convergent and discriminant validity. To support convergent validity, all item loadings should be statistically significant and above .707 indicating that over half the variance is captured by the latent construct (Straub et al., 2004). Supporting both

convergent and discriminant validity, acceptable GFI, NFI, AGFI, CFI and RMSEA should be within acceptable ranges (Im & Grover, 2004). A summary of acceptable cut-off values of these key measures are provided in Table 23.

Table 23. *Summary of Acceptable Cut-off Values of Reliability and Fit*

Measure	Cut-Off Value
Cronbach's alpha	≥ .70
Item loadings	significant ≥ .707
Adjusted chi-square	≤ 3.0
GFI	≥ .90
AGFI	≥ .80
CFI	≥ .90
NFI	≥ .90
RMSEA	≤ .08

As shown in Table 24 through Table 29, with the exception of the *policy relevance* scale, little adjustment to the scales was required. In the initial phase of isolated construct estimation, five items were deleted from the *user training, security*

culture, and *policy relevance* constructs. Specifically, the items SC2, PR6, PR7, and PR8 were deleted due to high cross-loads with other constructs. UT3 was deleted due to a lack of item reliability. During tests for unidimensionality based on procedures from Gefen (2003), PR3 was deleted due to high levels of residual covariance with indicators in other constructs. The three scales for constructs *top management support, policy enforcement*, and *perceived security effectiveness* remained unchanged from the scales used during the pilot test. Table 30 summarizes the measurement properties for the six final constructs each modeled in isolation.

Table 24. *Top Management Support Construct Fit*

Item	Std ML Estimate	ML Estimate	Critical ratio	p-level	Est of Variance	SMC	Mean	Std Dev
TM1	.843	.903	31.33	p <.001	.299	.710	3.65	1.02
TM2	.787	.846	27.52	p <.001	.395	.620	3.60	1.02
TM3	.784	.896	27.32	p <.001	.454	.614	3.22	1.09
TM4	.875	.989	33.81	p <.001	.271	.765	3.43	1.07
TM5	.881	1.000	--	--	.261	.775	3.29	1.08
TM6	.847	.904	30.12	p <.001	.340	.684	3.58	1.04

Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
2	6	.93	4.98 *0.00*	.98	.95	.99	.99	.073

Refinements from initial scale: None.

Table 25. *User Training Construct Fit*

Item	Std ML Estimate	ML Estimate	Critical ratio	p-level	Est of Variance	SMC	Mean	Std Dev
UT1	.814	.852	31.38	p <.001	.382	.814	3.37	1.06
UT2	.882	.912	37.56	p <.001	.246	.882	3.25	1.05
UT4	.924	1.00	--	--	.177	.924	3.16	1.10
UT5	.847	.953	34.77	p <.001	.368	.847	3.34	1.14
UT6	.811	.841	31.20	p <.001	.379	.811	2.84	1.05

Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
1	5	.93	3.95 *0.01*	.99	.97	1.00	.99	.063

Refinements from initial scale: UT3 deleted due to lack of item reliability.

Table 26. *Security Culture Construct Fit*

Item	Std ML Estimate	ML Estimate	Critical ratio	p-level	Est of Variance	SMC	Mean	Std Dev
SC1	.752	.815	23.54	p <.001	.415	.565	3.28	0.97
SC3	.769	1.024	24.52	p <.001	.588	.592	3.37	1.20
SC4	.827	.890	27.12	p <.001	.296	.685	3.48	.969
SC5	.848	1.097	28.35	p <.001	.354	.719	3.37	1.12
SC6	.839	1.00	--	--	.343	.703	3.33	1.06

Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
1	5	.90	2.33 *.040*	.99	.98	1.00	1.00	.042

Refinements from initial scale: SC2 deleted due to high cross-loads with three other factors.

Table 27. *Policy Relevance Construct Fit*

Item	Std ML Estimate	ML Estimate	Critical ratio	p-level	Est of Variance	SMC	Mean	Std Dev
PR1	.904	1.00	34.34	p <.001	.177	.818	3.49	.988
PR2	.720	.715	23.62	p <.001	.379	.518	3.68	.887
PR4	.795	.923	27.78	p <.001	.394	.633	3.62	1.04
PR5	.900	1.00	--	--	.187	.810	3.55	.993

Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
1	4	.90	.379 *.684*	1.00	1.00	1.00	1.00	.000

Refinements from initial scale: PR6, PR7, and PR8 deleted due to high cross-loads with the *security culture* construct. PR3 later deleted due to low reliability and high levels of residual covariance with indicators in other constructs.

Table 28. *Policy Enforcement Construct Fit*

Item	Std ML Estimate	ML Estimate	Critical ratio	p-level	Est of Variance	SMC	Mean	Std Dev
PE1	.849	1.00	--	--	.254	.721	3.53	.954
PE2	.777	.888	23.78	p <.001	.338	.604	3.26	.925
PE3	.834	1.071	26.32	p <.001	.329	.695	3.43	1.04
PE4	.715	.958	21.29	p <.001	.573	.512	3.64	1.08

Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
1	4	.87	1.55 *.212*	.99	.99	.99	1.00	.027

Refinements from initial scale: None.

Table 29. *Perceived Security Effectiveness Construct Fit*

Item	Std ML Estimate	ML Estimate	Critical ratio	p-level	Est of Variance	SMC	Mean	Std Dev
EF1	.847	.962	31.35	p <.001	.218	.717	3.48	.888
EF2	.835	.968	30.70	p <.001	.244	.697	3.59	.907
EF3	.745	.880	25.31	p <.001	.370	.555	3.56	.921
EF4	.877	1.00	--	--	.162	.786	3.46	.883
EF5	.773	.960	26.85	p <.001	.370	.598	3.42	.969

Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
3	5	.91	1.32 *.256*	1.00	.99	1.00	1.00	.020

Refinements from initial scale: None.

Table 30. *Summary of Measurement Properties of Constructs (29-item instrument)*

Construct	Phase Collected	Items	Alpha	χ^2/df *p-value*	GFI	AGFI	CFI	NFI	RMSEA
Top Mgt Support	2	6	.93	4.98 *0.00*	.98	.95	.99	.99	.073
User Training	1	5	.93	3.95 *0.01*	.99	.97	1.00	.99	.063
Security Culture	1	5	.90	2.33 *.040*	.99	.98	1.00	1.00	.042
Policy Relevance	1	4	.90	.379 *.684*	1.00	1.00	1.00	1.00	.000
Policy Enforcement	1	4	.87	1.55 *.212*	.99	.99	.99	1.00	.027
Perceived Effectiveness	3	5	.91	1.32 *.256*	1.00	.99	1.00	1.00	.020

Two specific tests of discriminant validity were conducted. Discriminant validity refers to the distinctiveness of the factors measured by different sets of indicators. For

the first test, if the estimated correlations between the factors are not excessively high (e.g., > .85), evidence for discriminant validity exists (Kline, 1998, p.60). This test is provided in Table 31, column 4. For this study, all correlations between the constructs were under the .85 benchmark. For the second test, a chi-square comparison of an original two-construct model with an alternative model is made (Segars & Grover, 1998, p.153). In the alternative model (column 5), the two constructs in the test are constrained into one united construct. If the chi-square value is significantly smaller in the original, unconstrained model (column 6), discriminant validity between the tested constructs has been shown (Straub et al., 2004). Column 7 shows the chi-square differences between each construct. All tests showed significant differences ($p < .001$) suggesting the six constructs are distinct conceptual entities.

Table 31. *Discriminate Validity Tests*[11]

Test	Covariance Est	Critical Value	Correlation Est	Constrained Model χ^2 (df)	Unconstrained Model χ^2 (df)	χ^2 Difference
(1)	(2)	(3)	(4)	(5)	(6)	(7)
Top Management Support						
Training	.668	13.98***	.68	149.44 (44)	117.28 (43)	32.17***
Culture	.684	14.62***	.80	143.62 (44)	113.16 (43)	30.45***
Policy Enf	.468	12.36***	.61	176.88 (35)	82.59 (34)	94.30***
Policy Rel	.441	11.32***	.52	194.79 (35)	95.60 (34)	99.12***
Per Effect	.536	14.10***	.72	208.23 (44)	131.53 (43)	76.70***
User Training						
Culture	.706	14.63***	.77	112.03 (35)	86.37 (34)	25.65***
Policy Enf	.500	12.51***	.61	142.40 (27)	61.84 (26)	80.53***
Policy Rel	.57	13.24***	.63	117.68 (27)	61.10 (26)	56.59***
Per Effect	.574	14.38***	.72	138.26 (35)	75.32 (34)	62.94***
Security Culture						
Policy Enf	.469	12.48***	.64	133.68 (27)	38.25 (26)	94.43***
Policy Rel	.427	11.25***	.53	168.00 (27)	62.54 (26)	105.50***
Per Effect	.515	13.82***	.73	137.44 (35)	53.27 (34)	84.17***
Policy Enforcement						
Policy Rel	.369	10.90***	.51	164.73 (20)	23.41 (19)	141.32***
Per Effect	.376	12.08***	.60	177.88 (27)	24.70 (26)	153.18***
Policy Relevance						
Per Effect	.412	12.47***	.60	185.99 (27)	54.57 (26)	131.42***

[11] Note: *** $p < .001$

Analysis of the A Priori Theoretical Model

In the preceding sections, each construct was modeled in isolation and then in pairs during tests for discriminant validity. Now the full, *a priori* theoretical model as a collective network is tested. Table 32 provides the standardized factor loadings, critical value (z-statistic), and squared multiple correlation (SMC) for each of the 29 indicators from the finalized instrument. Together, the significant loadings, item loadings above .707, and acceptable fit indices demonstrate construct validity: discriminant, convergent, and factorial (Straub et al., 2004, p.410). The SMC is the percentage of explained variance for each indicator. For example, it is estimated that the predictor of TM1, which is the latent construct *top management support*, explains 71 percent of the TM1 variance and the error variance is approximately 29 percent of the variance of TM1 itself (Arbuckle, 2003).

Figure 6 presents the standardized causal path findings, selected fit indices, and SMC values. All hypothesized paths are significant with indices indicating a good overall fit of the model to the data. Overall, the data is consistent with the hypothesized model.

Table 32. *Measurement Model*

Constructs	Indicators	Loadings[12]	Critical Value	SMC
Top Management Support alpha = .93	TM1	.84	31.33	0.71
	TM2	.79	27.53	0.62
	TM3	.78	27.34	0.62
	TM4	.87	33.83	0.77
	TM5	.88	---	0.78
	TM6	.83	30.13	0.68
Employee Training alpha = .93	UT1	.81	31.39	0.66
	UT2	.88	37.56	0.78
	UT4	.92	---	0.85
	UT5	.85	34.77	0.72
	UT6	.81	31.20	0.66
Security Culture alpha = .90	SC1	.75	23.54	0.57
	SC3	.77	24.52	0.59
	SC4	.83	27.12	0.69
	SC5	.85	---	0.72

[12] All loadings significant at $p < .001$.

Constructs	Indicators	Loadings[12]	Critical Value	SMC
	SC6	.84	28.35	0.70
Policy Relevance alpha = .90	PR1	.90	34.98	0.81
	PR2	.73	24.01	0.53
	PR4	.80	27.98	0.64
	PR5	.90	---	0.81
Policy Enforcement alpha = .87	PE1	.85	---	0.72
	PE2	.78	23.78	0.60
	PE3	.83	26.32	0.70
	PE4	.72	21.29	0.51
Perceived Security Effectiveness alpha = .91	EF1	.85	31.36	0.72
	EF2	.83	30.69	0.70
	EF3	.75	25.31	0.56
	EF4	.89	---	0.79
	EF5	.77	26.84	0.60

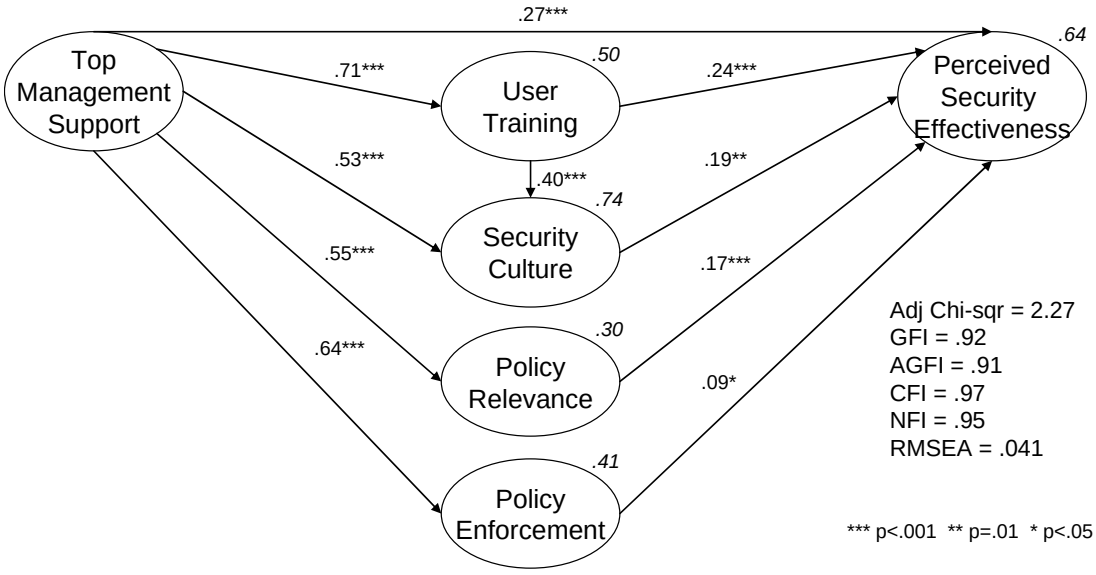


Figure 6. *Path Diagram of Hypothesized, Partial Mediation Model*[13]

Analysis of Mediation Effects

The hypothesized model is a partial mediation model. With such a model, a number of tests are necessary to check the appropriateness of the mediator variables. Four steps can help establish whether a variable mediates the relation between an independent and dependent variable (Frazier et al., 2004, p.125).

- Step one: show that there is a significant relation between the independent and dependent variable.
- Step two: show that the independent variable is related to the mediator.
- Step three: show that the mediator is related to the dependent variable.
- Step four: show that the relation between the independent and dependent variable is significantly reduced when the mediator is added to the model.

[13] Each endogenous variables' estimate of SMC is to the upper-right of each construct (e.g. Perceived Security Effectiveness SMC=.64)

The results of each of the four steps is provided in Figure 7 and Table 33. Figure 7 illustrates the form of Model A, no mediation, and Model B, partial mediation with one variable.

In Table 33, step one is demonstrated in test 1. In this test, a significant relationship is shown between the independent variable, *top management support*, and the dependent variable, *perceived security effectiveness* (column C). Step two is demonstrated in tests 2 through tests 5 (column D). For each test, a significant relationship is demonstrated between the independent variable and each of the four mediator variables. Step three is demonstrated in tests 2 through 5 (column E). For each test, a significant relationship is demonstrated between each of the four mediator variables and the dependent variable. Step four is demonstrated by examining the relationship between the independent and dependent variable in tests 1 through 5 (column C). When each mediator is included, the relationship is smaller, but greater than zero.

In addition, Table 33 shows selected model fit statistics for each of the tests (column H). The results of the chi-square comparisons between model A in test 1 and each of the four versions of model B in tests 2 through 5 is provided (column G). Each of the mediation models provides a significantly different chi-square value except for model B4, the *policy enforcement* mediation model. In this case, the chi-square difference between models A and B4 cannot be distinguished from zero, suggesting that the variable is not a mediator. However, because the chi-square statistic is very sensitive to sample size, researchers are encouraged to consider other more appropriate fit measures when the sample size is large (Hair et al., 1998). Three alternate measures are considered. First, model B4 has a low RMSEA value of .037 (column H). Second, when the *policy*

enforcement mediator is added to the model, the relation between the independent and dependent variable is reduced from .72 to .57, $p < .001$ (column C). Third, the paths between policy enforcement and both the independent and dependent variables are both highly significant (columns D and E). Thus, based on the results provided in Table 33, sufficient support exists that all four variables including *policy enforcement,* are appropriate mediator variables.

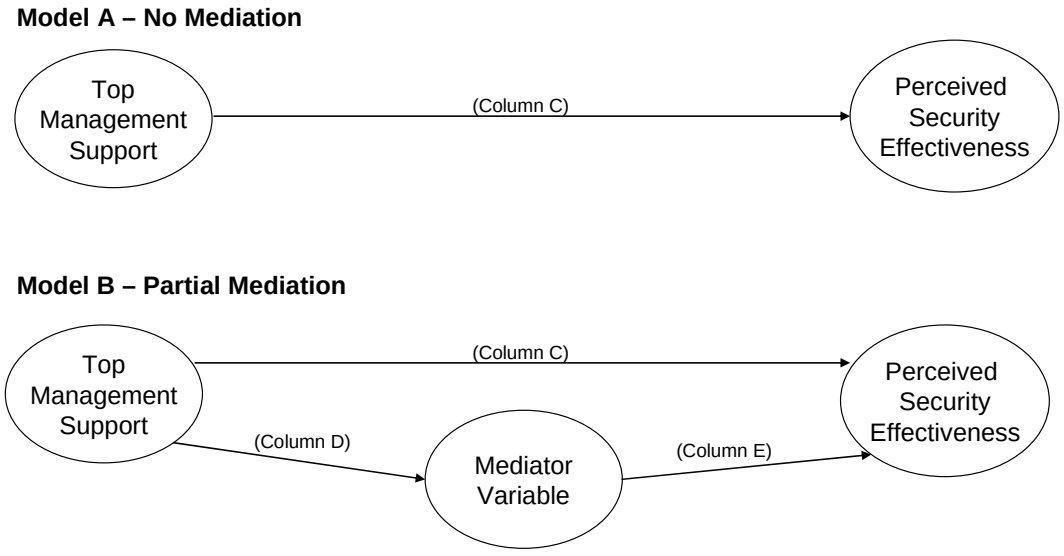


Figure 7. *Mediation Model Comparison*

Table 33. *Tests of Each Mediation Variable*[14]

		Standardized Path Coefficients			Model Fit		
Test #	Mediator Variable	TM→ EF	TM→ Mediator Variable	Mediator Variable → EF	χ^2 (df) χ^2/df	$\Delta\chi^2$ (Δdf) *from Model A*	GFI CFI RMSEA
(A)	(B)	(C)	(D)	(E)	(F)	*(G)*	(H)
1	Model A. No Mediation	.72***	---	---	131.5 (43) 3.06	---	.97 .99 .053
2	Model B1: Training	.42***	.68***	.43***	242.8 (101) 2.40	*111.3 (58)* *p<.001*	.96 .99 .044
3	Model B2: Culture	.38***	.80***	.43***	226.7 (101) 2.24	*95.2 (58)* *p< .01*	.96 .99 .041
4	Model B3: Policy Relev	.56***	.52***	.31***	214.5 (87) 2.46	*83 (44)* *p< .001*	.96 .99 .045
5	Model B4: Policy Enfor	.57***	.61***	.25***	173.9 (87) 2.00	*42 (44)* *N.S.*	.97 .99 .037

[14] Notes: TM: Top Management Support. EF: Perceived Security Effectiveness. *** p<.001; **p=.001; *p<.05

The percentage of the effect of each mediational pathway on the dependent variable, *perceived security effectiveness*, is now assessed. The percentage of the total effect of each mediator variable provides information on how much of the total effect is attributable to each mediator (MacKinnon, Krull, & Lockwood, 2000). From Table 34, the mediated effect represents 60.5% of the total effect on the dependent variable *perceived security effectiveness* whereas the direct effect of *top management support* represents 39.5% of the total effect. This implies support for a partial mediation model since both the mediational and direct effect provides substantial effects.

Table 34. *Percent Mediated of Total Effect on Perceived Security Effectiveness*[15]

A	B	C	D	E
Mediated Effects	Path From Top Mgt Spt	Path To Effectiveness	Effect (B*C)	Percent of Total Effect
Training	0.708***	0.243***	0.172	24.8%
Culture	0.528***	0.193**	0.102	14.7%
Relevance	0.550***	0.166***	0.091	13.2%
Enforcement	0.639***	0.085*	0.054	7.8%
Total Mediated Effects			0.420	60.5%
Direct Effect				
Top Mgt Support to Effectiveness			0.274***	39.5%
Total Effects Direct & Mediated			0.694	100%

Notes: *** p<.001; **p=.001; *p<.05

[15] The percentage mediated is the mediated effect divided by the total effect. For example, the value of the mediated effect of the variable *user training* was .172. The total effect of *user training* was calculated by adding all the mediated effects of the four variables (.420) and the direct effect (.274) which summed up to .694. The percentage mediated by the *user training* mediator was about 25% (MacKinnon et al., 2000).

Full versus partial mediation. In SEM, a full mediation model can be supported if the model with the direct path between the independent and dependent variables does not provide a better fit to the data than the model without the direct path. If, however, the model with the direct path from the independent to the dependent variable provides a better fit to the data, partial mediation is supported (Frazier et al., 2004). Figure 8 illustrates the results of the full mediation version of the *a priori* model.

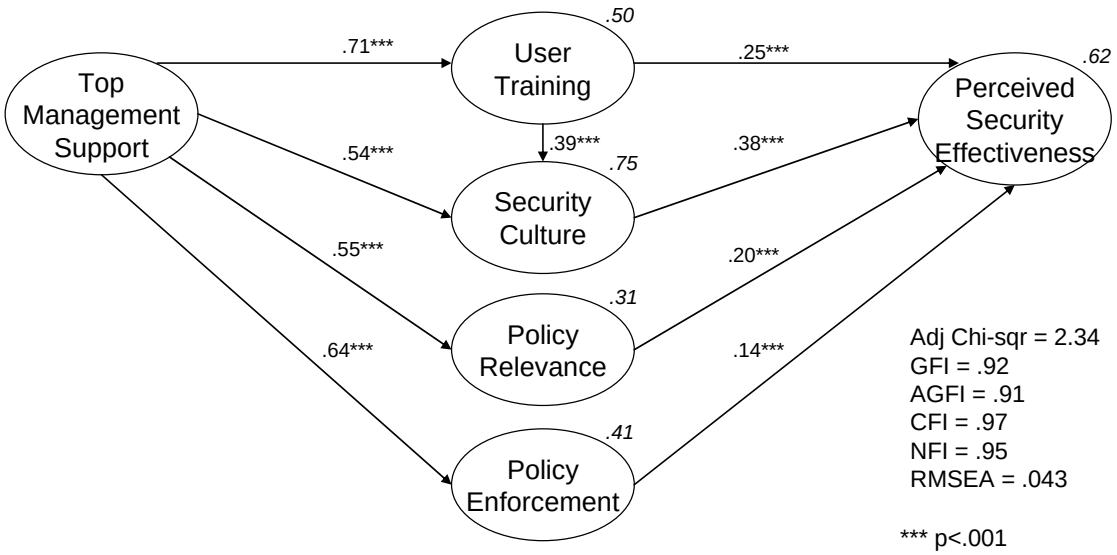


Figure 8. *Full Mediation Model*

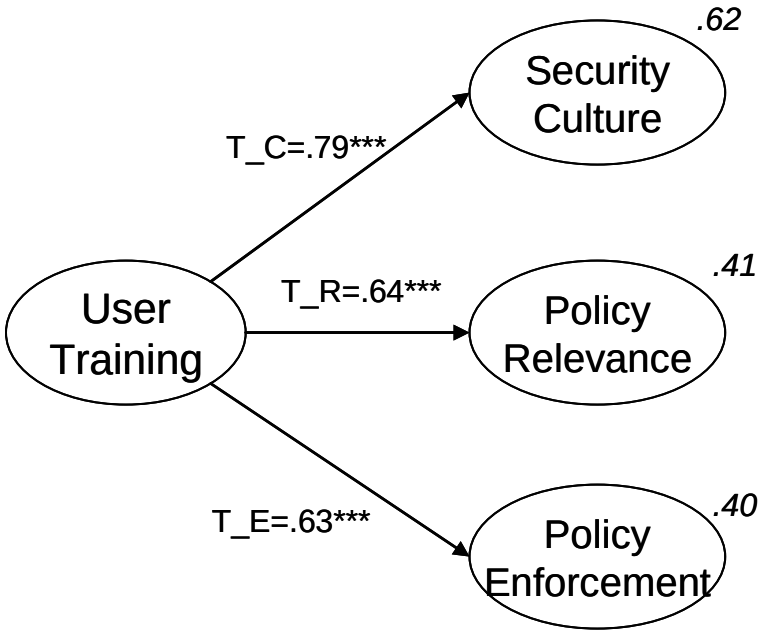
When comparing the full mediation model to the partial mediation model, the statistical evidence suggests that partial mediation is the better model. First, in the partial mediation model (Figure 6), the direct effect path between *top management support* and *perceived security effectiveness* is highly significant (p<.001). Second, partial mediation has a small, but improved model fit. Table 35 compares some of the fit statistics between the two models. Based on these two statistical results and considering that the *a priori*,

partial mediation model was theoretically justified from the qualitative analysis of the CISSP open-ended responses, partial mediation is the better of the two models.

Table 35. *Summary of Fit Statistics Comparing Two Mediation Models*

Model	RMSEA	χ^2	df	χ^2/df	Δdf	$\Delta\chi^2$	*p-value*
Full Mediation	.043	859.3	368	2.34			
					1	25.2	*.000*
Partial Mediation	.041	834.1	367	2.27			

Test of Relative Benefit of Hypothesis 6. Hypothesis 6 theorizes that the mediator variable *user training* is positively associated with the mediator variable *security culture*. This hypothesis resulted from the qualitative evaluation of the CISSP open-ended responses. Chapter III, Table 5, provides example statements that illustrate this relationship. This same analysis of the open-ended responses did not support similar paths between *user training* and *policy relevance* and *enforcement*. Thus, if H6 is theoretically appropriate, the *user training* → *security culture* path (T_C) should have a stronger relationship than the *user training* → *policy relevance* (T_R) and *policy enforcement* (T_E) paths. Similarly, constraining T_C to equal zero should have the most adverse affect on overall model fit than likewise constraining T_R or T_E. Figure 9 illustrates the SEM results of a four variable test model. The results support the *a priori*, qualitative assertion that the relationship between *user training* and *security culture* is theoretically appropriate.



	Chi-sqr/df	GFI	CFI	RMSEA
Unconstrained Full Model	2.34	.95	.98	.036
When T_C = 0	6.49	.91	.93	.086
When T_R = 0	4.77	.92	.95	.071
When T_E = 0	4.55	.93	.95	.069

Test of comparative benefit of Hypothesis 6, *User Training → Security Culture (T_C).* The path model shows the coefficients and the construct SMC of the unconstrained, four variable model. The table shows the fit comparisons after each path is constrained to equal zero. Model fit suffers the most when T_C is constrained to zero.

Figure 9. *Comparative Benefit of Hypothesis 6*

Statements of Formal Hypothesis.

In Chapter III, Table 4 presented formal statements of hypothesis. All the paths in the *a priori*, partial mediation model are statistically significant and the data is consistent to the model. During mediation tests, each mediator variable showed to be appropriate. Additionally, tests demonstrated that H6 was theoretically appropriate. Based on the quantitative analysis presented in this chapter, each of the hypotheses listed in Table 36 is thus supported.

Table 36. *Formal Hypotheses Supported*

H1	*Top management support is positively associated with perceived security effectiveness.*	Supported
H2	*Top management support and perceived security effectiveness is partially mediated by user training.*	Supported
H3	*Top management support and perceived security effectiveness is partially mediated by security culture*	Supported
H4	*Top management support and perceived security effectiveness is partially mediated by policy relevance.*	Supported
H5	*Top management support and perceived security effectiveness is partially mediated by policy enforcement.*	Supported
H6	*User training is positively associated with security culture.*	Supported

Demographic Analysis of A Priori Model

In the survey, respondents were asked various demographic questions to aid the researcher in sub-sample analysis and in tests for construct bias. Differences in factor structures can point to possible construct bias among demographic sub-samples. Construct bias may also be detected by embedding the construct in a nomological set of relationships. If the construct antecedents and consequents differ across demographic variables, then construct bias may be suspected (Karahanna et al., 2004). This analysis can be especially useful for detecting differences among demographics such as countries, organizational size, and industry. Table 37 provides results of testing the partial mediation model using demographic sub-samples with an $n > 100$. Because of low statistical power, interpretations of the some of the sub-samples should be made with caution (i.e. $n < 200$).

Table 37. *Demographic Tests of Partial Mediation Model*

Sample N	Top Mgt Support[16]					UT	UT	SC	PR	PE	Fit
	EF[17]	UT	SC	PR	PE	SC	Perceived Security Effectiveness				GFI CFI RMSEA
Full Sample 740	***	***	***	***	***	***	***	**	***	*	.92 .97 .041
Demographics About Evaluated Organization:											
US & Canada 462	***	***	***	***	***	***	***	**	**	.091	.91 .97 .042
US & Canada - No Consultants 371	***	***	***	***	***	***	***	*	**	NS	.90 .97 .043
Other than US & Canada 277	**	***	***	***	***	***	**	*	***	NS	.87 .96 .049

[16] Note: ***p<.001; **p<.01; *p<.05; .### p<.10; N.S. Not Significant

[17] EF: perceived security effectiveness; UT: user training; SC: security culture; PR: policy relevance; PE: policy enforcement

Sample N	Top Mgt Support[16]					UT	UT	SC	PR	PE	Fit
	EF[17]	UT	SC	PR	PE	SC	Perceived Security Effectiveness				GFI CFI RMSEA
Europe 121	*	***	***	***	***	***	NS	.010	**	NS	.79 .96 .051
Asia-Pacific 104	*	***	***	***	***	**	.065	NS	NS	.082	.76 .93 .065
Government Sector 184	N.S	***	***	***	***	***	***	*	*	NS	.84 .97 .046
Finance, Banking, Insurance Sector 187	**	***	***	***	***	***	NS	NS	*	**	.84 .96 .050
Info Tech (IT) Sector 201	*	***	***	***	***	***	**	.089	*	NS	.84 .96 .052
Small (< 500 employees) 193	NS	***	***	***	***	***	**	*	**	**	.84 .96 .049

Sample N	Top Mgt Support[16]					UT	UT	SC	PR	PE	Fit
	EF[17]	UT	SC	PR	PE	SC	Perceived Security Effectiveness				GFI CFI RMSEA
Medium (500-15,000 employees) 302	***	***	***	***	***	***	.079	.054	***	NS	.88 .97 .048
Large (> 15,000 employees) 245	*	***	***	***	***	***	***	.095	NS	NS	.85 .95 .054
No Top Security Officer (e.g. CSO) 267	***	***	***	***	***	***	NS	*	**	*	.87 .96 .044
Yes Top Security Officer 460	**	***	***	***	***	***	***	*	***	NS	.91 .97 .041
Demographics About Evaluating Respondent:											
In a Technical Position 324	**	***	***	***	***	***	**	***	**	NS	.89 .97 .043

Sample N	Top Mgt Support[16]					UT	UT	SC	PR	PE	Fit
	EF[17]	UT	SC	PR	PE	SC	Perceived Security Effectiveness				GFI CFI RMSEA
In a Managerial Position 414	***	***	***	***	***	***	***	NS	***	*	.89 .97 .046
IT Experience < 8 years 161	NS	***	***	***	***	**	NS	NS	***	NS	.82 .94 .060
IT Experience 8-15 years 326	***	***	***	***	***	***	**	NS	**	NS	.89 .97 .042
IT Experience > 15 years 251	*	***	***	***	***	***	***	**	*	NS	.85 .96 .053
Only Consultants 166	**	***	***	***	***	**	NS	.070	NS	NS	.82 .96 .053
Only Non Consultants 574	***	***	***	***	***	***	***	*	***	.070	.92 .97 .041

Sample N	Top Mgt Support[16]					UT	UT	SC	PR	PE	Fit
	EF[17]	UT	SC	PR	PE	SC	Perceived Security Effectiveness				GFI CFI RMSEA
Remove less than one year at organization 622	***	***	***	***	***	***	***	**	***	.079	.92 .97 .041
Lower reported levels of task interdep.[18] 368	***	***	***	***	***	***	*	***	**	.071	.88 .96 .052
Higher reported levels of task interdep. 372	***	***	***	***	***	***.	***	NS	***	NS	.91 .98 .036

[18] Note: Lower (or upper) half of summed scores from the Van Der Vegt et al task interdependence scale.

A few consistencies in Table 37 are worth highlighting. First, regardless of the demographic sub-sample, all paths between *top management support* and the four mediator variables is highly significant ($p < .001$). Second, every *user training – security culture* path is significant (at least $p < .05$). Third, regardless of the demographic, the data has a good overall fit to the model: all CFI and RMSEA measures are within the accepted cut-off values. Many of the GFI values suggest a poor or moderate fit (e.g. Asia-Pacific = .76), but this may be attributed to a small sub-sample size.

Five demographic differences are now highlighted. First, while the direct effect from *top management support* to *perceived security effectiveness* was not significant for small-sized organizations, the path was highly significant ($p < .001$) for medium-sized organizations. Second, for respondents working in technical positions, the *security culture – perceived security effectiveness* path was highly significant whereas for respondents working in management positions, the path was not significant. Third, for respondents with less than eight years of IT experience, the *user training – perceived security effectiveness* was not significant whereas for respondents with fifteen years or more the path was highly significant. Fourth, only two of the twenty-three total demographic sub-samples had the *policy enforcement - perceived security effectiveness* path significant ($p < .01$): respondents working in small organizations and respondents working in the financial, banking, and insurance industry. Otherwise, for most sub-samples, this path had little or no statistical significance. Finally, for respondents requiring higher levels of task interdependence to accomplish their job well, the path between *security culture* and *perceived security effectiveness* was not significant. However, for respondents requiring lower levels of task interdependence to accomplish

their job well, the *security culture* and *perceived security effectiveness* path was highly significant.

Cultural differences and tests for construct bias. Construct bias occurs when a measured construct is not equivalent across cultures both at a conceptual and at an operational level. This can result from different definitions of the construct across cultures, incomplete construct coverage, or poor sampling (van de Vijver & Poortinga, 1997). Table 38 shows test results by looking for statistical inappropriateness in each of the six constructs for countries with at least twenty participants in the study.

Table 38. *Construct Bias Tests of Each Theoretical Construct*

$\Delta\chi^2$/df *p-value*
GFI CFI
RMSEA alpha
loadings ≥ .707?
(exceptions)
items p < .05?
(exceptions)

Sample n	Top Mgt Support	User Training	Security Culture	Policy Relevance	Policy Enforcement	Perceived Effectiveness
US 402	2.72 *.004* .98 .99 .066 α=.94 Yes Yes	2.60 *.024* .99 .99 .063 α=.93 Yes Yes	1.11 *.351* .99 1.0 .017 α=.91 Yes Yes	3.53 *.029* .99 .99 .079 α=.90 Yes Yes	2.35 *.096* .99 1.0 .058 α=.88 Yes Yes	.538 *.748* 1.0 1.0 .000 α=.92 Yes Yes
Canada 60	.944 *.485* .95 1.0 .000 α=.92 Yes Yes	5.92 *.000* .83 .89 .29 α=.91 No *(UT6=.68)* Yes	2.02 *.072* .93 .97 .132 α=.87 No *(SC3=.60)* Yes	7.25 *.001* .90 .89 .325 α=.83 No *(PR2=.51, PR4=.60)* Yes	.148 *.863* 1.0 1.0 .000 α=.90 Yes Yes	.449 *.814* .99 1.0 .000 α=.93 Yes Yes
UK 36	2.16 *.022* .84 .92 .18 α=.90 No *(TM3=.62)* Yes	2.67 *.534* .97 1.0 .000 α=.88 No *(UT6=.66)* Yes	1.04 *.395* .95 1.0 .032 α=.88 No *(SC3=.65)* Yes	.030 *.971* 1.0 1.0 .000 α=.87 No *(PR2=.51)* Yes	.752 *.471* .98 1.0 .000 α=.87 No *(PE4=.68)* Yes	1.36 *.236* .94 .97 .10 α=.85 No *(EF3=.58)* Yes

$\Delta\chi^2$/df	*p-value*
GFI	CFI
RMSEA	alpha
loadings ≥ .707?	
(exceptions)	
items p < .05?	
(exceptions)	

Sample n	Top Mgt Support	User Training	Security Culture	Policy Relevance	Policy Enforcement	Perceived Effectiveness
Hong Kong 20	1.22 *.280* .84 .97 .11 α=.84 No *(TM2=.39,* *TM6=.50)* No *(TM4 p<.10)*	2.12 *.052* .85 .89 .251 α=.89 No *(UT2=.64)* Yes	2.33 *.040* .99 1.0 .042 α= .91 No *(SC2=.65,* *SC4=.67)* Yes	1.52 *.219* .93 .98 .165 α= .92 Yes Yes	3.60 *.027* .87 .82 .37 α=.80 No *(PE1=.54;* *PE3=.57)* Yes	.861 *.506* .93 1.0 .000 α=.89 No *(EF5=.66)* Yes
Australia & New Zealand 23	1.84 .056 .81 .94 .195 α=.95 Yes Yes	3.95 *.001* .99 .99 .063 α=.94 Yes Yes	2.33 *.040* .99 .99 .043 α=.95 Yes Yes	.379 *.684* 1.0 1.0 .000 α=.94 Yes Yes	1.79 *.167* .94 .97 .19 α=.87 No *(PE4=.61)* Yes	1.31 *.256* 1.0 1.0 .020 α=.88 No *(EF5=.54,* *EF3=.63)* Yes
Europe 121	2.28 *.015* .94 .98 .103 α=.91 Yes Yes	1.34 *.246* .98 1.0 .053 α=.93 Yes Yes	2.20 *.051* .97 .98 .100 α=.88 Yes Yes	1.56 *.209* .99 .99 .069 α=.89 No *(PR2=.59)* Yes	.429 .651 1.0 1.0 .000 α=.88 Yes Yes	1.28 *.268* .98 .99 .049 α=.88 No *(EF3=.66)* Yes

$\Delta\chi^2$/df *p-value*
GFI CFI
RMSEA alpha
loadings ≥ .707?
(exceptions)
items p < .05?
(exceptions)

Sample n	Top Mgt Support	User Training	Security Culture	Policy Relevance	Policy Enforcement	Perceived Effectiveness
Asia-Pacific 104	2.33 *.013* .94 .97 .11 α=.92 Yes Yes	2.03 .071 .96 .99 .10 α=.92 Yes Yes	.676 .646 .99 1.0 .000 α=.89 Yes Yes	1.876 .153 .98 .99 .092 α=.90 Yes Yes	2.85 *.058* .98 .98 .13 α=.82 No *(PE2=.62; PE4=.64)* Yes	1.48 *.191* .97 .99 .069 α=.90 Yes Yes.

Based on the confirmatory factor analysis of each individual construct presented in Table 38, a few of the sub-samples indicate possible construct bias. First, Hong Kong respondents may not have construct equivalence for *top management support, user training,* and *policy enforcement. Top management support*, for example, had two items well below the .707 factor loading cut-off indicating that the construct was capturing less than half of the variance of those two items. However, other indicators such as the significant chi-square value of .280 and a CFI of .97 suggest that the data fit well. For the top management support construct, the TM2 item may not be appropriate from a cultural context, which is explored further in Table 39. Perhaps the most suspect construct is *policy enforcement* as it pertains to Hong Kong respondents. All the indicators suggest a problematic fit (e.g. CFI of .82), however the reliability is within the cut-off and all the items loaded significantly on the construct. The item PR2 demonstrated possible construct bias with Europe, UK, and Canadian sub-samples and also is further analyzed in Table 39.

Table 39. *Cultural Analysis of Two Questionnaire Items*

Item	Hong Kong (n=20)	Full Sample (N=740)
"Top executives are interested in security issues" (TM2)	Std Loading: .39 Mean: 3.73 Std Dev: 0.88 SMC: 0.15	Std Loading: .80 Mean: 3.60 Std Dev: 1.02 SMC: 0.64

Item	Canada (n=60)	Full Sample (N=740)
"Information Security Policy is updated when technology changes require it." (PR2)	Std Loading: .51 Mean: 3.40 Std Dev: 0.91 SMC: 0.26	Std Loading: .72 Mean: 3.68 Std Dev: 0.89 SMC: 0.52

It is difficult to draw reliable conclusions about potential construct bias when some of the sub-samples are very small even for single construct factor analysis (e.g. Hong Kong n=20). However, the data suggests that construct bias among the seven geographic sub-samples presented in Table 38 is not serious. A number of results support this assertion. First, all reliability alphas are at least .80. Second, the vast majority of factor loadings are above .707 and are significant, even for small sub-samples

from Hong Kong, United Kingdom, and Australia-New Zealand. Third, the majority of model fit indices are within acceptable ranges. There are only two instances where no fit indices for a particular construct were within acceptable ranges. The first concerns *user training* for Canadian respondents and the other is *policy enforcement* for Hong Kong respondents. However, in both cases the Cronbach's alpha were acceptable and all items had significant loadings. Overall, reliable conclusions about these two instances cannot be made due to the lack of statistical power of the smaller sub-samples.

Alternative, Second-order Factor Mediation Model

Illustrated in Figure 11, an alternative model posits a second-order factor governing the correlations among *user training*, *security culture*, *policy relevance*, and *policy enforcement*. This model provides an additional prospective on the factor analytic structure of the *a priori* model reproduced in Figure 10. The theoretical interpretation of the second-order factor is *managerial practice* in information security. The findings of the second-order factor analysis reveal that the four mediator variables can be expressed by one overall *managerial practice* trait. Table 40 provides a comparison of the two models.

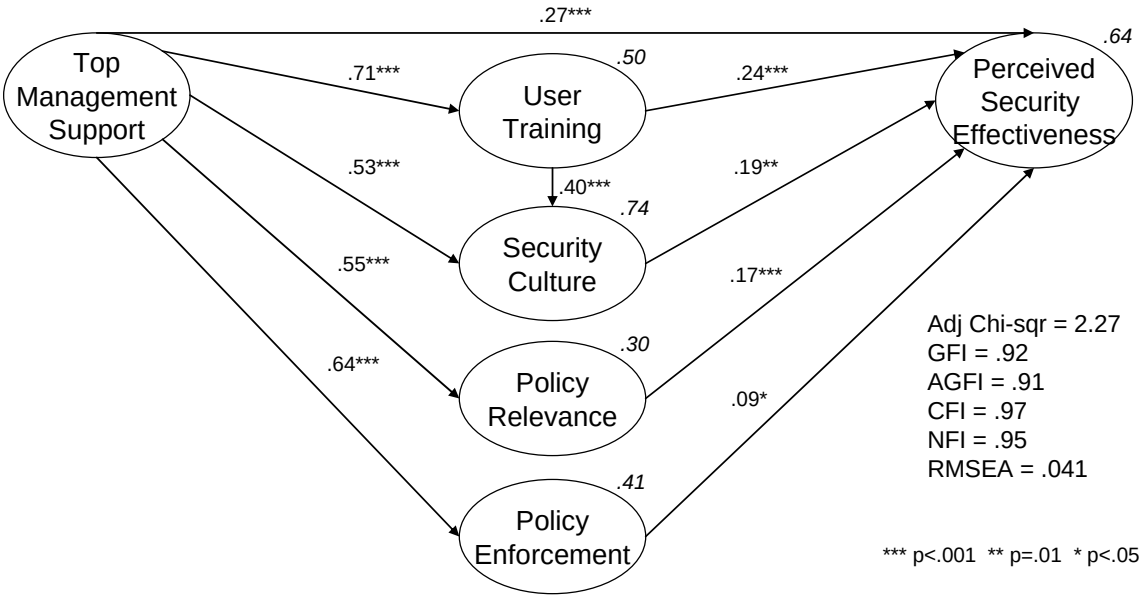
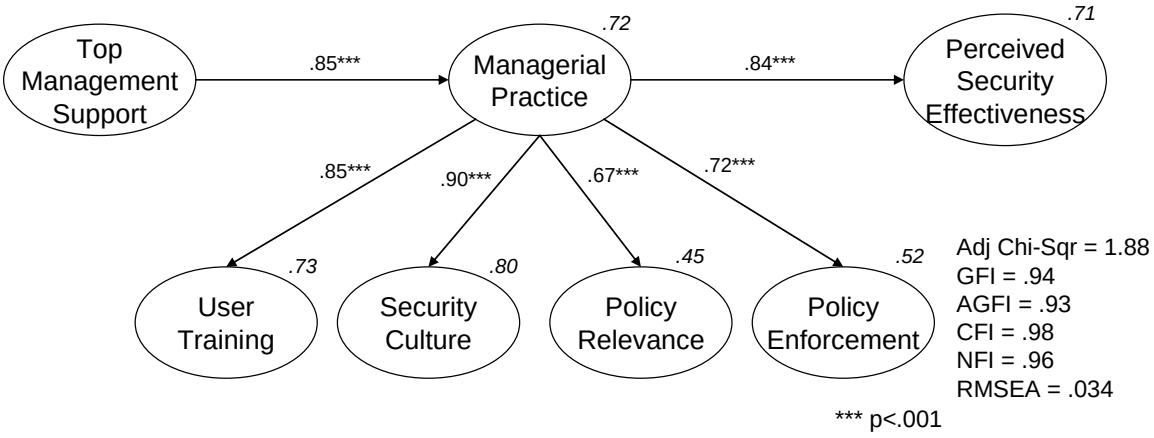


Figure 10. *A Priori, Partial Mediation Model (same as Figure 6)*



Note:
• Partial Mediation (adding Top Mgt Spt → Effectiveness path) not supported. Path not distinguished from zero.
• H6 path (Training → Culture) not supported. Path not distinguished from zero.

Figure 11. *Alternative, Second-order Factor Mediation Model*

Table 40. *Comparison of Mediation Models*

Measure	Partial Mediation (*a priori*)	2nd Order Factor Mediation (alterative)
Number of Paths	10	6
Path significance	Eight paths *p<.001* One path *p<.01* One path *p<.05*	Six paths *p<.001*
Chi-square	834.1	699.1
df	367	371
Chi-square/df	2.27	1.88
GFI	.92	.94
AGFI	.91	.93
CFI	.97	.98
NFI	.95	.96
RMSEA (two-sided 90% confidence interval)	.041 (.038, .045)	.035 (.031, .039)
Squared Multiple Correlations:		
User Training	.50	.73
Security Culture	.74	.80
Policy Relevance	.30	.45
Policy Enforcement	.41	.52
Perceived Security Effectiveness	.64	.71
Managerial Practice	---	.72

The alternative, second-order factor is a more parsimonious representation of the observed covariance (six paths versus ten paths in the *a priori* model). Empirical support

of the second-order factor model is found in the magnitude and significance of the estimated parameters as well as the amount of variance explained by the structural equations (Segars & Grover, 1998). Unlike the *a priori* model, all paths in the alternative model are highly significant ($p < .001$). The amount of explained variance measured by SMC is higher in each variable in the alternative model. Every model fit index improved in the alternative model. Additionally, unidimensionality tests on the alternate model revealed only three instances where the standardized residual covariances exceeded 2.58 (Gefen, 2003; Jöreskog, 1970). Each involved questionnaire item PR2 as it covaried with EF2, EF4, and UT1. Appendix G provides a table of standardized residual covariances.

Based on empirical grounds that is fully consistent with theory,[19] the conceptualization of managerial practice as a multi-dimensional measure of user training, security culture, policy relevance, and policy enforcement seems justified.

Demographic Analysis Using Second-Order Factor Model

Table 41 illustrates the results of running the alternative model by the same demographic sub-samples from Table 37. In the alternate model, every path is highly significant ($p < .001$) including the smaller samples such as from Asia-Pacific respondents. The model-fit generally improved for each sub-sample. Thus, results indicate that the more parsimonious, alternative model may have general applicability across countries, industries, and organizational sizes.

[19] Based on the open-ended, qualitative responses from the CISSPs

Table 41. *Demographic Tests of Second-Order Factor Mediation Model*

Sample N	Top Mgt Support	Managerial Practice				Mgt Practice	Fit	
	Mgt Practice	UT	SC	PR	PE	Per Effect	$\Delta\chi^2$/df	GFI CFI RMSEA
Full Sample 740	***	***	***	***	***	***	1.88	.94 .98 .034
Demographics About Evaluated Organization:								
US & Canada 462	***	***	***	***	***	***	1.56	.92 .98 .035
US & Canada & No Consultants 371	***	***	***	***	***	***	1.49	.91 .98 .036
Other than US & Canada 277	***	***	***	***	***	***	1.51	.88 .97 .043
Europe 121	***	***	***	***	***	***	1.24	.80 .96 .045
Asia-Pacific 104	***	***	***	***	***	***	1.40	.77 .94 .062
Government sector 184	***	***	***	***	***	***	1.37	.84 .97 .045

Sample N	Top Mgt Support	Managerial Practice				Mgt Practice	Fit	
	Mgt Practice	UT	SC	PR	PE	Per Effect	$\Delta\chi^2$/df	GFI CFI RMSEA
Finance, Banking, Insurance sector 187	***	***	***	***	***	***	1.47	.84 .96 .050
Info Tech (IT) sector 201	***	***	***	***	***	***	1.40	.85 .97 .045
Small (< 500 employees) 193	***	***	***	***	***	***	1.40	.84 .97 .045
Medium (500-15,000 employees) 302	***	***	***	***	***	***	1.50	.89 .97 .041
Large (> 15,000 employees) 245	***	***	***	***	***	***	1.58	.87 .96 .049
No Top Security Officer (e.g. CSO) 267	***	***	***	***	***	***	1.40	.88 .97 .039
Yes Top Security Officer 460	***	***	***	***	***	***	1.56	.92 .98 .035
Demographics About Evaluating Respondent:								
In a Technical Position 324	***	***	***	***	***	***	1.43	.90 .98 .036

Sample N	Top Mgt Support	Managerial Practice				Mgt Practice	Fit	
	Mgt Practice	UT	SC	PR	PE	Per Effect	$\Delta\chi^2$/df	GFI CFI RMSEA
In a Managerial Position 414	***	***	***	***	***	***	1.66	.91 .97 .040
IT Experience < 8 years 161	***	***	***	***	***	***	1.51	.82 .95 .056
IT Experience 8-15 years 326	***	***	***	***	***	***	1.46	.90 .98 .037
IT Experience > 15 years 251	***	***	***	***	***	***	1.52	.87 .97 .046
Only Consultants 166	***	***	***	***	***	***	1.36	.83 .97 .047
Only Non Consultants 574	***	***	***	***	***	***	1.68	.93 .98 .034
Remove less than One Year at Org 622	***	***	***	***	***	***	1.73	.93 .98 .034
Lower reported levels of task interdependence 368	***	***	***	***	***	***	1.73	.89 .97 .045

Sample N	Top Mgt Support	Managerial Practice				Mgt Practice	Fit	
	Mgt Practice	UT	SC	PR	PE	Per Effect	$\Delta\chi^2$/df	GFI CFI RMSEA
Higher reported levels of task interdependence 372	***	***	***	***	***	***	1.37	.92 .99 .031

Common Variance Tests

Tests were conducted to estimate the amount of common variance in the collected data (N=740). Whereas the pilot test collected data from a single source at one point in time, the large-scale survey collected from a single source but employed procedural remedies to control method bias. Foremost, data was collected in three timed increments with forced gaps of at least three days each phase that actually averaged over four days each (Conger, Kanungo, & Menon, 2000; Podsakoff et al., 2003). Additionally, different scales and collection formats were used to help maximize the difference in data collection between the independent and other variables of the study (Podsakoff et al., 2003). Three different tests for common variance follow: a common latent factor analysis, a marker variable assessment and a pilot versus large-scale survey comparison.

Common latent factor analysis. The empirical data of this study were analyzed using procedures developed to test for common method variance (Facteau, Dobbins, Russell, Ladd, & Kudisch, 1995; Williams, Cote, & Buckley, 1989). Five models are presented in Table 42. Model 1 is a null model with zero factors and contains all 29-items from the research instrument. Model 2 posits a single, latent *common variance* factor. Model 3 is the measurement model without any paths among the six constructs of the study. Model 4 adds to Model 3 the common variance factor so that items could load on their theoretical constructs as well as on the latent common factor. For comparison purposes, Model 5 is the second-order factor mediation model.

If a common variance factor exists, Model 2 should fit the data better than Model 1 and Model 4 should fit the data better than Model 3. An assessment of Table 42 reveals that while Model 2 provides significant fit, it fits the data poorly (e.g. GFI is .57). Also,

the gain in fit provided by Model 4 over Model 3 is relatively small (e.g. GFI improves from .94 to .96). Thus, confirmatory factor analysis shows that a single factor model did not fit the data well; the alternate six-factor model provides a significantly better fit than a single-factor model in the sampled data ($\Delta\chi^2(6\ df) = 4598.4$, $p < .001$) (Koh, Ang, & Straub, 2004).

Table 42. *Results of Model Comparison based on Facteau et al (1995)*

Model		χ^2	df	χ^2/df	GFI	AGFI	CFI	RMSEA
1	Null	17518.4	406	43.15	.13	.07	.00	.239
2	Single Latent Factor	5297.5	377	14.05	.57	.51	.71	.133
3	Measurement Model	717.4	390	1.84	.94	.93	.98	.034
4	Measurement Model + Single Latent Factor	500.3	333	1.50	.96	.94	.99	.026
5	Second-order Factor Mediation Model	699.1	371	1.89	.94	.93	.98	.035

Table 43 presents the results of partitioning the variation accounted by Model 4 into trait, common variance, and unique (i.e. error) components (Facteau et al., 1995; Williams et al., 1989). The standardized factor scores are squared to indicate the percentage of variance due to the theoretical trait factor and to the single latent factor. This test indicated that 38% of the total variance is attributed to the single latent factor.

Table 43. *Percentage of Variance Comparison*

N=740	Phase Collected	Trait Factor Variance	Common Factor Variance	Unique Variance
Measurement model + single latent factor	---	31%	38%	31%
Top Management Support	Two	39%	32%	29%
User Training	One	19%	56%	26%
Security Culture	One	23%	43%	34%
Policy Relevance	One	45%	25%	30%
Policy Enforcement	One	34%	29%	37%
Perceived Effectiveness	Three	26%	42%	32%
Second-order factor measurement + path model	---	68%	---	32%

The results from the previous two tables suggest that the measurement model benefits from a common variance factor, although the model fit gain is small, and that common variance accounts for a sizable percentage (38%) of the overall variance. However, the percent of common variance also varies considerably by theoretical construct. *User training*, *security culture*, and the dependent variance *perceived security effectiveness* have more common variance than trait variance. However, *policy relevance*, *policy enforcement*, and the independent variable *top management support* have more trait variance than common variance. This suggests that that the 38% common variance is not equally 'common' or systematic to all the theoretical constructs

of the study. Of note, the three constructs with the most common or shared variance also have higher construct correlations: *user training–security culture (*0.77), *user training–perceived effectiveness* (0.72), and *security culture–perceived effectiveness (*0.73).

Marker variable assessment. Another technique to analyze common variance is the use of a marker variable (Lindell & Whitney, 2001). If a variable can be identified on theoretical grounds that it is not related to at least one other variable from the study, then it can be used as a marker. Any observed relationship between it and any of the other variables in the study can be assumed to be due to common method variance. This method, however, has limitations in that it cannot be relied upon to identify all types of common method variance. For instance, the technique assumes that common variance can only inflate, not deflate, the observed relationships between the independent and dependent variables (Podsakoff et al., 2003).

Nevertheless, for this study, the five items from the Van Der Vegt *task interdependence* scale (alpha = .75; GFI = 0.98; CFI = 0.95) were used as a marker variable to test for possible systematic inflation of variance. Table 44 presents the results of including the *task interdependence* construct to Model 4 from the previous analysis. Confirmatory factor analysis partitioned the variation into trait, common variance, and unique (i.e. error) components (Facteau et al., 1995; Williams et al., 1989). The standardized factor scores are squared to indicate the percentage of variance due to the theoretical trait factor and to the common factor. This test indicated that only 1.2% of the *task interdependence* variance was attributed to the common latent factor.

Table 44. *Percentage of Variance Comparison with Marker Variable*

N=740	Phase Collected	Trait Factor Variance	Common Factor Variance	Unique Variance
Measurement model with single latent factor	---	31%	34%	35%
Top Management Support	Two	38%	33%	29%
User Training	One	15%	59%	25%
Security Culture	One	23%	43%	34%
Policy Relevance	One	45%	25%	30%
Policy Enforcement	One	34%	29%	37%
Perceived Effectiveness	Three	26%	42%	32%
Task Interdependence	One	41%	1%	58%

These results do not represent a complete solution for gauging the source of common variance; yet, it provides some confirmation that the common variance was not systematic across all constructs measured in the survey instrument.

Pilot versus large-scale survey comparison. Another technique for analyzing the source of common variance in this study is to compare the results of the pilot test to the large-scale survey. During the pilot test (N = 68), all the variables were collected on the same questionnaire at the same point in time, making the pilot data more vulnerable to problematic common method variance than the large-scale survey data, which employed a longitudinal design involving time lags (Sanchez & Viswesvaran, 2002). Comparing the levels of common variance from the pilot and large-scale survey may provide insight

into the origin of the common variance. Particularly, if the correlations are artificially high because of common *method* variance, we should see a difference in the correlations; the constructs from the pilot data would show 'artificially' higher (or lower) levels of correlation. If, however, the constructs are highly correlated *theoretically*, we should see consistency in the correlations from the pilot and large-scale survey data. In other words, if the 38% common variance is valid and predictable variance, then a necessary but insufficient proof of this validity is for the construct correlations to be about the same from the pilot to the large-scale survey data. Since phase two employed the least similar conditions in data collection compared to phases one and three, the pilot versus large-scale comparison is most useful for the phase two variable *top management support*. As Table 45 demonstrates, the correlations between *top management support* and the other variables of the study changed very little from the pilot to the large-scale survey data. Additional discussion of common method variance is provided in Chapter V.

Table 45. *Correlations of Pilot and Large-Scale Survey Data*

	N = 68 Pilot survey Correlations	N = 740 Large-scale survey Correlations
Top Management Support (Independent Variable):		
User Training	.61	.68
Security Culture	.79	.80
Policy Enforcement	.62	.61
Policy Relevance	.54	.52
Perceived Effectiveness	.68	.72

Task Interdependence Results

Task interdependence is the extent to which individuals depend upon other individuals and resources to perform a job (Van Der Vegt et al., 2003). High levels of task interdependence has been demonstrated to lead to high demands for top management support for IT implementation success (Sharma & Yetton, 2003). Thus, if IS security tasks show evidence of high levels of task interdependence, then comparing the theoretical model of the present study to the Sharma & Yetton model can provide a degree of nomological validity of the present model. Nomological validity refers to the making of a comparison with previous theoretical networks often using patterns of

correlation and regression (Straub et al., 2004, p.385). Nomological validity examines the robustness of the constructs as they interrelate with one another and can be confirmed within a wider theoretical context or network of constructs (Smith et al., 1996).

Pearce et al task interdependence scale. Sharma & Yetton (2003) conducted a meta-analysis of 22 studies that operationalized *IS implementation success* and *management support*. In the present study, we extend the Sharma & Yetton analysis to observe the extent that IS security effectiveness is reliant on management support moderated by task interdependence.

Sharma & Yetton (2003) included a variety of dependent variables for *IS implementation success* such as *user satisfaction* where the key managerial challenges include overcoming various forms of end-user resistance, motivating end users to adopt a new IS, and developing new behaviors among end users. The dependent variables in the Sharma & Yetton study "represent the success of various managerial interventions designed to promote end-user adoption. Hence, these variables are accepted here as the most appropriate proxies for implementation success" (Sharma & Yetton, 2003, p.543). Considering that the operationalized variable *perceived security effectiveness* in the present study is consistent with the Sharma & Yetton scope of *IS implementation success*, extending the meta-analysis to IS security seems justified for comparative purposes. Figure 12 illustrates the theoretical model of the Sharma & Yetton meta-analysis study.

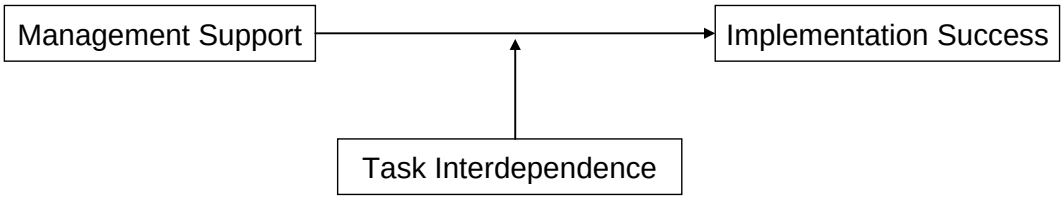


Figure 12. *Moderating Effect of Task Interdependence (Sharma & Yetton, 2003)*

Table 46. *Task Interdependence Scale (Pearce et al, 1992)*

TI1	Security-related tasks can be performed fairly independently of others. (Reverse Code)
TI2	Security-related tasks can be planned with little need to coordinate with others. (RC)
TI3	It is rarely required to obtain information from others to complete security-related tasks. (RC)
TI4	Information security-related tasks are relatively unaffected by the performance of others individuals or departments. (RC)
TI5	Information security-related tasks require frequent coordination with the effort of others.
TI6	Performance on information security-related tasks is dependent on receiving accurate information from others.

During the pilot test, 68 CISSPs completed the scale provided in Table 46. The alpha and fit indices resulting from a confirmatory factor analysis provided in Table 47 demonstrate high levels of scale reliability and fit. The mean score of the scale was 22.9. The estimated correlation between *top management support* and *perceived security*

effectiveness was 0.68. Table 48 compares other IS tasks provided in the Sharma & Yetton study with the results provided by the pilot test. Based on the table, IS security has the third highest *task interdependence* score and the second highest estimated correlation between the constructs of concern. Figure 13 illustrates a scatter plot of the construct correlation between management support and implementation success against task interdependence (Sharma & Yetton, 2003, p.546). Table 49 compares the results of a weighted least squares (WLS) regression analysis of the Sharma & Yetton data before and after the inclusion of the data from the present study. Based on these results, the findings of the current study are consistent with the findings of the meta-analysis.

Table 47. *Task Interdependence Reliability and Fit*

Data Collected	Items	Overall Mean	Alpha	$\Delta\chi 2$ (df) *p-value*	$\Delta\chi 2$/df	GFI	CFI	NFI	RMSEA
Pilot N=68	6	22.9	.87	11.2 (9) *.253*	1.26	.95	.99	.94	.062

Table 48. *Data from Studies Included in Sharma & Yetton Meta-analysis*

Application	Task Interdependence	Correlation	Sample Size
Info Engineering using CASE tools	26.3	0.69	56
CASE tools	24.7	0.28	59
Information systems security *(present study)*	22.9	0.68	68
DSS - Financial analysis & planning	20.7	0.45	132
DSS - Financial analysis & planning	20.7	0.33	156
DSS - Financial analysis & planning	20.7	0.39	90
OR/MS Projects	20.0	0.13	53
Sales forecasting model	19.7	0.30	92
Executive information systems	19.6	0.06	65
Telework	17.2	0.39	120
MLS Realty	14.4	0.11	106
Management information system	13.7	0.19	58
Expert system	13.2	0.20	88
Expert systems	12.7	0.27	69
SW testing & debugging tool	12.6	0.44	30
Office automation system	12.0	0.30	348
Customer record system	11.0	0.31	66
Micro computing	10.0	0.17	102
Portfolio management system	9.8	-0.15	34
PC applications	8.7	0.31	212
Interactive video instruction	7.7	0.18	344
Faculty computer use	7.7	0.12	422

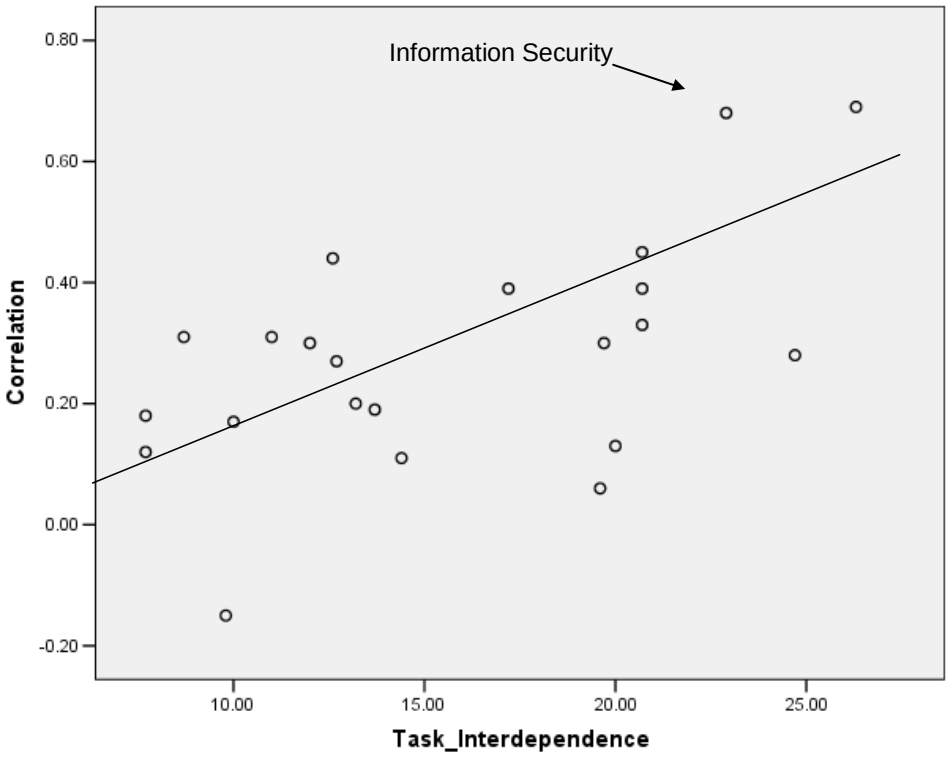


Figure 13. *Scatter Plot of Construct Correlation and Task Interdependence*

Table 49. *Results Comparison Before & After Inclusion of Present Study*

	Sharma & Yetton (2003)	Inclusion of present study
R-Squared	0.36, F = 10.5, $p \leq .05$	0.39, F = 12.56, $p \leq .05$
Slope	0.60, t = 3.2, $p \leq .05$	0.62, t = 3.5, $p \leq .05$
Intercept	0.06, t = .097, *N.S.*	0.04, t = .66, *N.S.*

Van Der Vegt et al task interdependence scale. A second task interdependence scale was applied. This scale was taken by 936 CISSPs during phase 1 data collection. The items with resulting mean, standard deviation, and possible range are provided in Table 50. The items refer to typical information security tasks performed in organizations.

Table 50. *Task Interdependence Scale (Van Der Vegt et al., 2003)*

Item		Mean	S.D.	Range
TI1	I have a one-person job; I rarely have to check or work with others. (RC)	1.94	.98	1-5
TI2	I have to work closely with my colleagues to do my work properly.	4.05	.85	1-5
TI3	In order to complete our work, my colleagues and I have to exchange information and advice.	4.23	.73	1-5
TI4	I depend on my colleagues for the completion of my work.	3.56	1.03	1-5
TI5	In order to complete their work, my colleagues have to obtain information and advice from me.	3.86	.86	1-5
TI6	Indicate the percentage of your tasks for which you have to exchange information or cooperate with others in your organization.	62.43	24.87	0-100
TI7	Indicate the total number of hours per day you have to exchange information or cooperate with others to do your job well.	4.11	2.25	0-10

Because the answers to the task interdependence items are on different scales, all seven items are standardized before combined into a single measure for the demographic analysis. Reliability of the five Likert-type items is .75 and for the seven standardized items is .79. Table 51 compares the results from the Van Der Vegt study to the present one. Based on an examination of the results, additional evidence is provided that IS security is a task that exhibits high levels of task interdependence.

Table 51. *Task Interdependence Results Comparison*

	Van Der Vegt et al (2003, p.719)	Present Study
Task	Telecommunications	Information Systems Security
Sample	129 members of 20 multidisciplinary teams from company in Netherlands; 70% of the teams work in software development	936 certified information systems security professionals (CISSPs) located world-wide in multiple industries.
TI6	Mean = 32.10; S.D. = 28.8	Mean = 62.43 ; S.D.= 24.87
TI7	Mean = 2.27; S.D. = 2.59	Mean = 4.11; S.D.= 2.25

Table 52 provides detailed task interdependence results by demographic sub-sample. The analysis uses the sum of the standardized items from the scale to include standard deviation, t-statistics and a 95% confidence interval of the mean.

An examination of the table reveals some notable results, of which four are mentioned. First, respondents from the Asia-Pacific region reported significantly lower levels of task interdependence than respondents from the United States and Canada. Second, Singapore respondents reported the lowest levels of any single country with more than 17 respondents in the study. Third, as expected, there is an incremental increase in the mean based on the organizational size: the larger the organization, the higher the task interdependence scores. Finally, respondents in managerial positions reported significantly higher levels of task interdependence than respondents in technical positions.

Table 52. *Task Interdependence Results by Demographic*

	Critical value	df (n-1)	Mean	S.D.	95% C. I. Lower	Upper
Country:						
Netherlands	32.06	17	3.44	0.46	3.22	3.67
UK	42.61	43	3.78	0.59	3.60	3.96
Australia & New Zealand	31.39	28	3.69	0.63	3.45	3.93
Canada	59.64	72	3.68	0.53	3.55	3.80
Hong Kong	29.90	26	3.67	0.64	3.42	3.92
USA	125.60	513	3.61	0.65	3.55	3.66
India	29.22	23	3.48	0.58	3.23	3.72
Singapore	23.33	24	3.21	0.69	2.92	3.49
Geographic Region:						
Asia-Pacific	61.02	141	3.44	0.67	3.33	3.55
Middle East	18.35	18	3.24	0.77	2.87	3.61
Europe	60.16	140	3.54	0.70	3.42	3.66
USA & Canada	137.54	586	3.61	0.64	3.56	3.67
South-Central America	22.21	13	3.57	0.60	3.22	3.92
Number of Employees:						
less than 500	75.57	230	3.41	0.69	3.33	3.50
Between 500 and 2,499	69.11	159	3.49	0.64	3.39	3.59
Between 2,500 and 7,499	67.25	141	3.58	0.63	3.47	3.68
Between 7,500 and 14,999	47.18	78	3.63	0.68	3.48	3.78
greater than 15,000	105.00	322	3.68	0.63	3.61	3.75
Industry (Sector):						
Utilities	40.55	31	3.82	0.53	3.63	4.01
Energy	29.67	27	3.64	0.65	3.39	3.89
Travel, Hospitality	17.46	12	3.64	0.75	3.18	4.09
Manufacturing	52.25	81	3.64	0.63	3.50	3.77
Professional Services (Legal, Marketing, etc.)	43.96	41	3.63	0.54	3.46	3.80

	Critical value	df (n-1)	Mean	S.D.	95% C. I. Lower	Upper
Government - federal, local, military, etc.	83.53	216	3.62	0.64	3.54	3.71
Industrial Technology	21.33	21	3.62	0.80	3.26	3.97
Finance, Banking, Insurance	86.88	237	3.59	0.64	3.51	3.67
Healthcare, Medical	51.12	79	3.59	0.63	3.45	3.73
Retail, Consumer Products, Wholesale	47.38	55	3.54	0.56	3.39	3.69
Transportation, Warehousing	19.43	19	3.53	0.81	3.15	3.91
IT & Telecommunications	81.44	253	3.52	0.69	3.44	3.61
Consultants	71.81	208	3.47	0.70	3.37	3.56
Non-Profit	25.24	13	3.42	0.51	3.13	3.72
Education	36.95	59	3.41	0.71	3.22	3.59
Does the organization have a top security position (e.g. Chief Security Officer)?						
Yes	134.17	584	3.63	0.65	3.58	3.69
No	96.60	331	3.43	0.65	3.36	3.50
Does the organization have a dedicated office responsible for IS security issues?						
Yes	152.63	759	3.61	0.65	3.56	3.66
No	66.90	169	3.35	0.65	3.25	3.45
Organizational Position:						
Senior Mgt	48.83	36	3.80	0.47	3.64	3.95
Owner-Partner	24.59	29	3.47	0.77	3.18	3.76
Dept manager, supervisor, director	64.14	121	3.72	0.64	3.61	3.84
Other Manager	34.18	27	3.80	0.59	3.57	4.02
MIS, IS, IT, technical	103.20	295	3.55	0.59	3.48	3.62
Other IT, technical, scientific, professional	102.14	419	3.50	0.70	3.43	3.56
Job Type:						
Technical	142.98	715	3.52	0.66	3.47	3.57
Managerial	86.29	216	3.71	0.63	3.63	3.79

	Critical value	df (n-1)	Mean	S.D.	95% C. I. Lower	Upper
IT-experience of respondent:						
less than 8 years	73.61	223	3.41	0.69	3.32	3.50
Between 8 and 15 years	115.58	410	3.58	0.63	3.52	3.64
greater than 15 years	96.47	298	3.65	0.65	3.57	3.72

Summary of task interdependence finding. The results from the two task interdependence scales suggests that IS security is a highly interdependent task. As such, the results of the present study are consistent with a well established meta-analysis study that suggests that tasks requiring high levels of interdependence require high levels of top management support for IS success (Sharma & Yetton, 2003). This affirms the conclusion that management support is a critical component for a successful implementation strategy when task interdependence is high.

Summary of Empirical Results

Based on the empirical results presented in this chapter, the *a priori*, partial mediation model is supported. An alternate, second-order factor mediation model was considered and also supported. Based on an analysis of demographic sub-samples, evidence for construct and cultural bias was not problematic. In addition, the second-order factor model showed evidence of general applicability across all demographics and cultures in the survey. Finally, based on the results of two separate scales, information security organizational tasks demonstrate high levels of task interdependence. The next chapter discusses these and other findings of the study.

CHAPTER V

DISCUSSION & CONCLUSION

The influence of *top management support* on *perceived security effectiveness* meditated by four variables of managerial practice has been examined from an empirical perspective. This final chapter is divided into three sections that discuss some of the results of the previous chapter before providing the conclusion. First, an evaluation is provided of how the findings in this study are linked to existing IS and organizational behavior theory. Second, a post-results discussion is given on three methodological issues that were proactively addressed in this study: perceived intrusiveness of security research, construct and cultural bias, and common method variance. For each, a discussion of how the rigor used in this study minimized these potential threats. Third, implications for research and practice are made. Throughout the chapter, appropriate research opportunities and study limitations are discussed. Finally, a conclusion to the study is offered.

Links to Existing Theory

In their seminal text on grounded theory, Glaser & Strauss (1967) state that it is desirable to link grounded models to existing theory to enhance internal validity and generalizability (Orlikowski, 1993). Linking also provides a degree of nomological validity of the study by examining the robustness of the constructs as they can be

confirmed within a wider theoretical network of constructs (Smith et al., 1996). In this section, a number of aspects from this study are linked to formal theories published in the IS and management literature to include a discussion of existing models of management support, the 'dilemma of the supervisor' notion, implications regarding task interdependence, and a commentary on socio-technical systems theory and the Theory X–Y dichotomy.

Management support and existing theoretical models. The qualitative data from this study suggested that obtaining top management support is the necessary condition for an effective information security program. As one CISSP stated, "Management buy-in and increasing the security awareness of employees is key. Technology is great, but without…management's backing, all the bits in the world won't help." Appendix F provides numerous statements regarding top management support obtained from the web survey.[20] Additionally, the critically of *top management support* was further demonstrated by the 874 CISSPs who ranked it #1 of 25 issues in February 2004 (Appendix C).

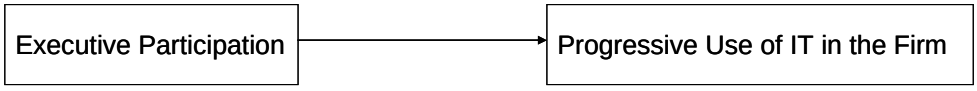
The quantitative results from the web survey are consistent with findings of previous studies that management support is especially important to the success of IT related projects (e.g., Sharma & Yetton, 2003). In the *a priori* model, the hypothesized relationship between *top management support* and each mediator variable was highly significant ($p < .001$) in all of the demographic sub-samples. The direct effect between *top management support* and *perceived security effectiveness* in the *a priori* model was

[20] The 936 CISSPs who completed the Phase I web survey were given the following open-ended question: In general, what do you feel is the most critical factor in determining whether an organization's information security program will be effective or not.

significant in each sub-sample (at least p <. 05) with only three exceptions: the government sector, organizations with less than 500 employees, and for survey respondents with less than 8 years of IT experience. In the alternative model, the relationship between *top management support* and the second-order factor *managerial practice* was highly significant in all demographic sub-samples. Based on the results from this study, the positive association between *top management support* and *perceived security effectiveness* is highly significant in a wide-range of demographic data.

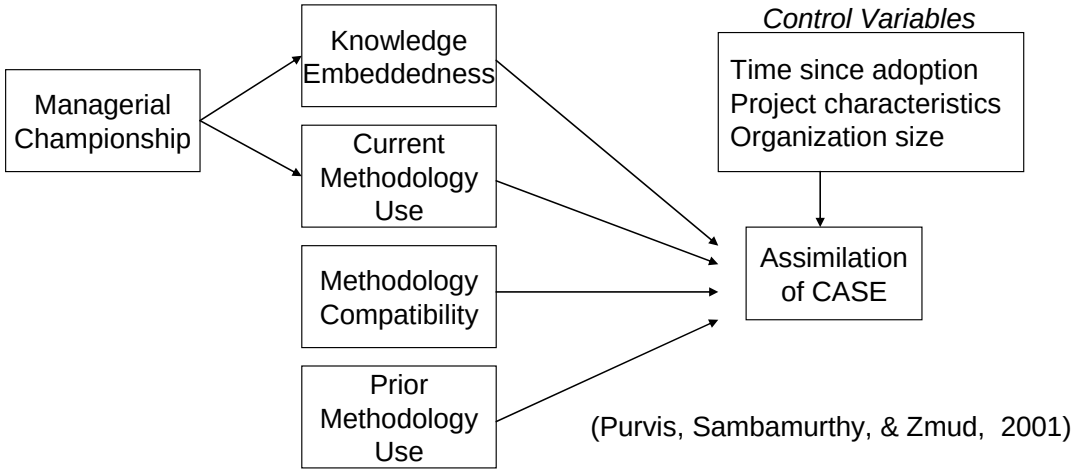
As mentioned in Chapter II, a substantial IS literature stream exists regarding the management support construct. However, with few exceptions, empirical analysis has limited the effect of management support on a dependent 'success' variable to a simple linear function (Sharma & Yetton, 2003). Figure 14 illustrates one example of a simple linear function from the literature (Jarvenpaa & Ives, 1991). Figure 15 illustrates an exception to the simple linear function involving the use of mediator variables (Purvis et al., 2001). The model in Figure 15 represents the closest theoretical structure found in the IS literature to the model of the current study. Consequently, the model in the current study contributes to the IS literature as one of the first models to substantially mediate the relationship between management support and a dependent variable.

Figure 14. *Example of Simple Linear Function*



From Jarvenpaa & Ives, 1991

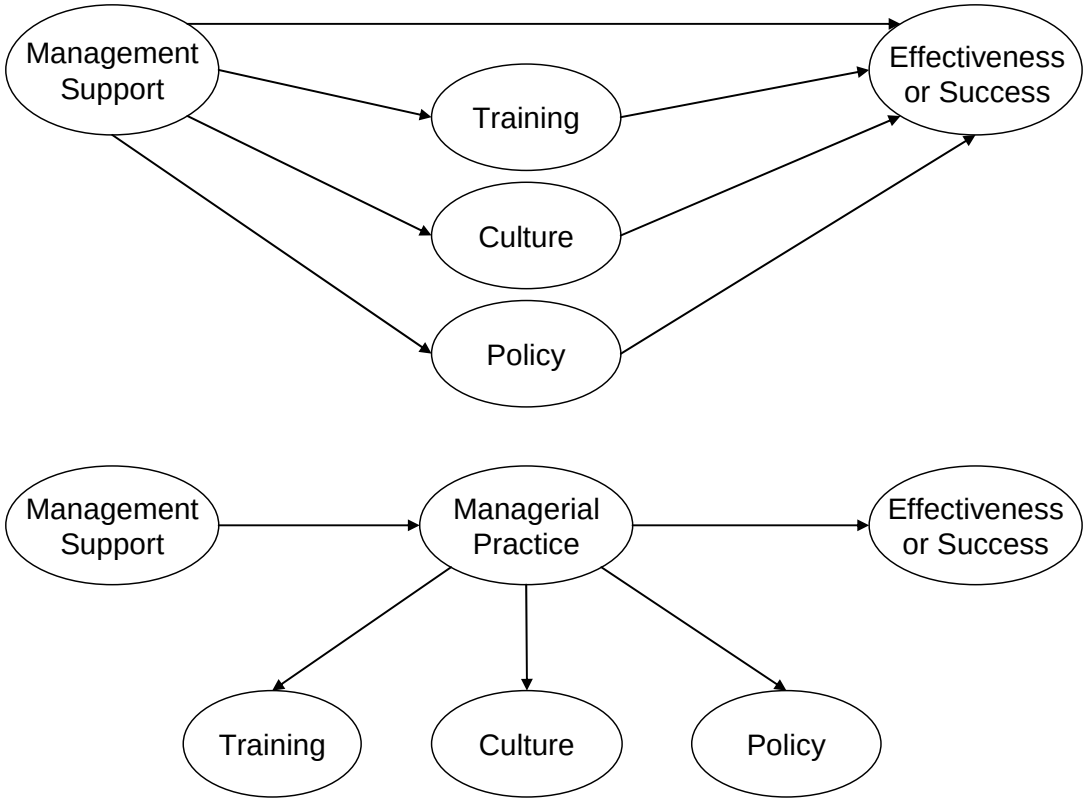
Figure 15. *Closest Theoretical Structure to the Current Study*



Both the *a priori* and alternative models of this study may be structured in a general form. Figure 16 illustrates the *a priori* partial mediation model and the alternative, second-order factor mediation model in general forms. Future research may be able to apply these forms to areas outside the realm of security. Domains where management support is critical to success or environments high in task interdependence may find the general form of the models beneficial. Depending on the study, other mediator variables may be added to the model. For example, an added mediator variable could represent financial resources or support.[21]

[21] Adding a financial resources variable to the present study was avoided because asking financial information risked an undesirable increase in the perceived intrusiveness of the survey instrument.

Figure 16. *General Forms of the Theoretical Models of this Study*



An interesting observation can be made regarding the 'rank order' of the effect size of the variables of the study. Based on the empirical results, the management support construct accounted for 40% of the total effect on the dependent variable, *perceived security effectiveness.* User training followed with 25% and the two policy constructs together accounted for 21% of the total effect. *Security culture* accounted for 15% of the total effect. This 'rank order' listing of effect size on the dependent variable is comparable to the list of the top 25 ranked issues that is provided in Appendix C. This similarity is not surprising since the constructs of this study derived in part from the results of the 2004 survey where 874 CISSPs ranked their top 25 issues. To some extent,

it was supposed that using the top ranked issues as the theoretical variables for this study would ensure the highest percentage of variance explained in the dependent variable. The fact that *top management support* and *user training* had the highest effect on the dependent variable of the present study while also obtaining the highest rankings in the critical issues survey is not a mere coincidence. Thus, combining the findings from these two studies, it seems apparent that gaining senior management support and ensuring a security-trained workforce are arguably the two most critical issues to obtain effectiveness in organizational information security. Table 53 compares the results of the ranking survey to the effect size of each variable from the present study.

Table 53. *Contrasting Ranking Results to Total Effect of Each Construct*

Rank (N=874)	%Who Ranked Issue in Top 3 (N=874)	Critical Issue (N=874)	Corresponding Construct in Present Study (N=740)	% of Total Effect on Dependent Variable (N=740)
1	34%	Top Management Support	Top Management Support	40%
2	25%	User Awareness Training & Education	User Training	25%
6	16%	Policy Related Issues	Policy Relevance + Policy Enforcement	21%
7	14%	Organization Culture	Security Culture	15%

Policy enforcement and the 'dilemma of the supervisor.' The *policy enforcement* construct, while as a stand-along construct demonstrated good reliability ($\alpha = .87$) and excellent overall fit (e.g. insignificant χ^2; GFI = .99; CFI = .99), had the weakest effect on the dependent variable compared to the other variables of the study. This weaker relationship is apparent in three areas. First, although the *a priori* theoretical model had a significant path between *top management support* and *policy enforcement* ($p < .001$), it had lower significance between *policy enforcement* and *perceived security effectiveness* ($p < .05$). Second, analyzing the demographic tables shows that the majority of sub-samples had insignificant *policy enforcement – perceived security effectiveness* paths. In fact, only four sub-samples had significant paths (at least $p < .05$): the finance, banking, and insurance sector, organizations with less than 500 employees, organizations without a senior security officer (e.g. CSO, CISO), and respondents working in managerial positions. Third, of the four mediator variables, *policy enforcement* had the smallest mediated effect (7.5%) on the dependent variable. Overall, it appears that while *policy enforcement* is an important construct in both models, its relationship to *perceived security effectiveness* is often insignificant due to the smaller effect size.

One plausible explanation for the weaker *policy enforcement* relationship with the dependent variable is that policy enforcement is a contingent construct. When organizations have a favorable security climate with higher levels of executive support, training, and culture, the importance of policy enforcement may diminish since employee intrinsic motivation to observe policy increases. Likewise, when organizations have an unfavorable security climate, the importance of enforcement accordingly may increase since intrinsic motivation to observe policy decreases.

A second plausible reason for the weaker relationship may be attributed to the 'dilemma of the supervisor' notion. This dilemma is described by Strickland (1958) as *the situation when the use of surveillance, monitoring, and authority, leads to management's distrust of employees and perception of an increased need for more surveillance and control. Because all behavior is seen by managers as motivated by the controls in place, they develop a jaundiced view of their people* (Ghoshal, 2005, p.85). For employees, the use of control implies they are neither trusted nor trustworthy to comply with security policy. Too much surveillance and monitoring of employee activities to help enforce policy compliance can be perceived as overly controlling and may damage employee self-perception, deteriorate trust, and decrease intrinsic motivation (Ghoshal, 2005).

The *policy enforcement* scale may have captured this dilemma to a degree with items such as, "Employees caught violating important security policies are appropriately corrected" (PE1) and "Repeat security offenders are appropriately disciplined" (PE3). One interpretation is if an organization has excessive monitoring and surveillance, the effect on *perceived security effectiveness* will diminish as employee intrinsic motivation decreases. In other words, the relationship between *policy enforcement* and *perceived security effectiveness* may be non-linear. If organizations want to develop employees that intrinsically behave in a security-minded fashion, then an optimum level of policy enforcement may exist. Either too much enforcement or too little may have negative consequence on effectiveness.

The relationship between monitoring and enforcement needs to be illustrated in order to fully link the policy enforcement construct to the 'dilemma of the supervisor'

concept. In the open-ended question responses, a number of CISSPs mentioned the dependency of enforcement on the monitoring of employees. One stated, "To protect information systems from attacks, you must be…monitoring IT security posture and processes and enforcing security policy where violations exist." Another said, "…so much of policy enforcement [depends on] monitoring and reporting, policies are not effective if employees feel the(y)…are not being monitored." Yet another, "Without the monitoring of logs, transactions, etc. it is impossible to see if any policy breaches are taking place unless a highly visible, public event occurs, such as a virus outbreak." Appendix F provides additional CISSP statements from the Phase I web survey. Thus, based on the above statements and others in the qualitative data, high enforcement will require high levels of employee monitoring and surveillance.

The potential problems associated with excessive monitoring has been identified in the IS literature. While monitoring can help enforce important security policies, some employees may regard this as negatively affecting their work habits and privacy. Thus, certain pitfalls exist for excessive monitoring (Ariss, 2002). Managers have a key role to play in designing monitoring and enforcement systems that are effective yet not viewed as too onerous or invasive so that employees not only tolerate the monitoring system, but understand and approve of it (George, 1996). Based on this discussion, future research can study the relationship among security policy enforcement, employee monitoring, culture and security effectiveness.

Task interdependence and information security. As described earlier, task interdependence is the extent to which an individual needs information, materials, and support from other team or organizational members to be able to carry out a job (Van Der

Vegt et al., 2003). Examining the open-ended question responses provide evidence that information security-related tasks are high on task interdependence, cooperation and teamwork. Table 54 provides selected statements from CISSPs regarding this concept. Appendix F provides additional statements from the phase I web survey.

Table 54. *CISSP Statements on Task Cooperation and Interdependence*

• "Devices like a Firewall are often actually managed and configured by Network Engineers, while the rules are designed by Security Engineers….When a single device requires the cooperation of what are all too often, opposing organizations, problems can occur."
• "Official Information Security policy establishment and enforcement requires cooperation and coordination of IT Management, Human Resources, Legal, and Executive Management."
• "It's unrealistic to expect an individual or group to simultaneously champion the delivery of a new application expected to provide benefit to the organization and delay this benefit due to security concerns...to be successful, it must be developed with…interdependent goals for an organization to realize both risk reduction and business benefit."

From the qualitative results of this study, four findings provide evidence that information security work is exceptionally high in task interdependence. First, based on the pilot test results of using the Pearce *task interdependence* scale, information security

received the third highest rating in task interdependence compared to 23 other IT-related tasks in the Sharma & Yetton (2003) meta-analysis. Second, the inclusion of the pilot study results in the Sharma & Yetton meta-analysis strengthen their thesis that higher levels of management support are needed to ensure IS success when task interdependence is high. Third, the 936 CISSPs who completed the Van de Vegt *task interdependence* scale indicated an average of 62% of their daily tasks require the exchange of information or cooperation with others. They also indicated an average of 4 hours per day is spent exchanging information or cooperating with others to do their job well. Fourth, based on a comparison of results in the associated article (Van Der Vegt et al., 2003), information security has nearly twice the measure of task interdependence compared to telecommunication software development work.

The combined qualitative and quantitative results of this study provide persuasive evidence that IS security-related work demands high levels of task interdependence. This finding has ramifications for the IS researcher by identifying new topics for future research. A review of the literature revealed six *task interdependence*-related topics that offer opportunities for future IS security research. First, high levels of task interdependence requires greater instances of information exchange needed to clarify task assignments, project requirements, and progress (Andres & Zmud, 2003). Second, the effects of peer monitoring on work-unit performance had positive effects in high-task interdependency and low supervisory monitoring environments (Loughry, 2002). Third, highly interdependent tasks may especially benefit from control & coordination mechanisms (Sharma & Yetton, 2003). Fourth, education-level may be especially relevant in work high in task interdependence (Van Der Vegt et al., 2003). Fifth,

organizational citizenship behavior (OCB), which helps describe the extent to which employees go above and beyond to contribute to collective success, may be particularly appropriate in tasks high in interdependence (Organ, 1988). Sixth, task interdependence may impact the level of cooperation across cultures and perceptions of the importance of OCB (Bachrach et al., 2004) as well as cooperation levels within groups (Wageman, 1995). In the whole, much of the task interdependence and OCB literature focuses on organizational teamwork (Van Der Vegt et al., 2001). This suggests that it may be particularly useful to view security-related work through the teamwork lens. Additionally, the above topics all represent future research opportunities in IS security.

Socio-technical systems theory and the Theory X - Theory Y dichotomy. The two theoretical models of this study may be understood through the lens of socio-technical systems (STS) theory. STS theory is explicitly grounded in general systems theory (Von Bertanlanffy, 1950) where organizations are seen as consisting of two independent but linked systems: a technical system and a social system. The technical system is concerned with the processes, tasks, and technology needed to gain the desired output where the social system is concerned with the attitudes, skills and values of people, reward systems, and authority structures (Bostrom & Heinen, 1977).

STS is an organizational design technique that has been applied to help solve many types of problems that face IT & MIS departments (Bostrom & Heinen, 1977). Yet, practitioners and researchers often mistakenly take either a technocentric or sociocentric approach rather than giving equal consideration to the technical and social dimension and their interactions (Sarkar & Lee, 2002). A joint optimization of the social

and technical components of the work environment is more desirable than simply optimizing either system at the expense of the other (Manz & Stewart, 1997).

The theoretical constructs of this study take into account critical social aspects of information security. This is in contrast with some viewpoints that information security is primarily a technical issue (Watson, Kelly, Galliers, & Brancheau, 1997). The techno-centric view of information security may have contributed to the general lack of empirical, social science-based studies that explores the managerial and organizational dimensions of the topic (Kotulic & Clark, 2004).

Rather than purely a technical field, information security can be cast as a human-centered domain based on relevant social theoretical constructs (Clarke & Drake, 2003; Dhillon & Backhouse, 2001). Yet, the social theoretical constructs from this study also have critical technical dimensions to them. Consider, for instance, that organizational 'acceptable use' policies require a technical implementation on a network firewall or proxy server. Also, for example, consider the many topics covered in basic user training classes that are IT-intensive such as understanding the dangers posed by spyware or comprehending what a Trojan horse is. The theoretical constructs from the present study are valuable from an STS perspective because they inherently involve both the social and technical dimensions of information security. Taken as a whole, rather than being either techno-centric or socio-centric, IS security may be best understood from the socio-technical perspective.

Another aspect of STS theory regards optimizing motivation work systems through the synchronization of social and technological conditions within organizations (Katzell & Thompson, 1995). Often discussed in an STS framework, Theory X and

Theory Y make different assumptions about the motivational patterns of individuals. For example, Theory X assumes a tightly structured organization emphasizing order to obtain technical efficiently where Theory Y assumes a flexible organization that gives a great deal of self-control in order to obtain organizational effectiveness (Bostrom & Heinen, 1977). The major difference between them is that Theory X places reliance upon external control of human behavior whereas Theory Y relies heavily on self-control and direction (McGregor, 1995).

Applied to the theoretical findings of this study, organizational leadership that emphasizes Theory X qualities would tend to direct people's actions through the approval, monitoring, and enforcement of relevant security policies. Conversely, organizational leadership that emphasizes Theory Y qualities may tend to stress training in order to create a culture where people internalize good security behavior. Figure 17 illustrates this point by segmenting the mediator variables of the *a priori* theoretical model into Theory X and Y groups. Yet, a balanced approach would suggest both groups of mediator variables need the right emphasis depending on an organization's security situation. Likewise, STS theory would suggest that security effectiveness is maximized when both the social and technical aspects of security are addressed together. Like the other topics in this section, future research can explore the socio-technical theory implications of information security.

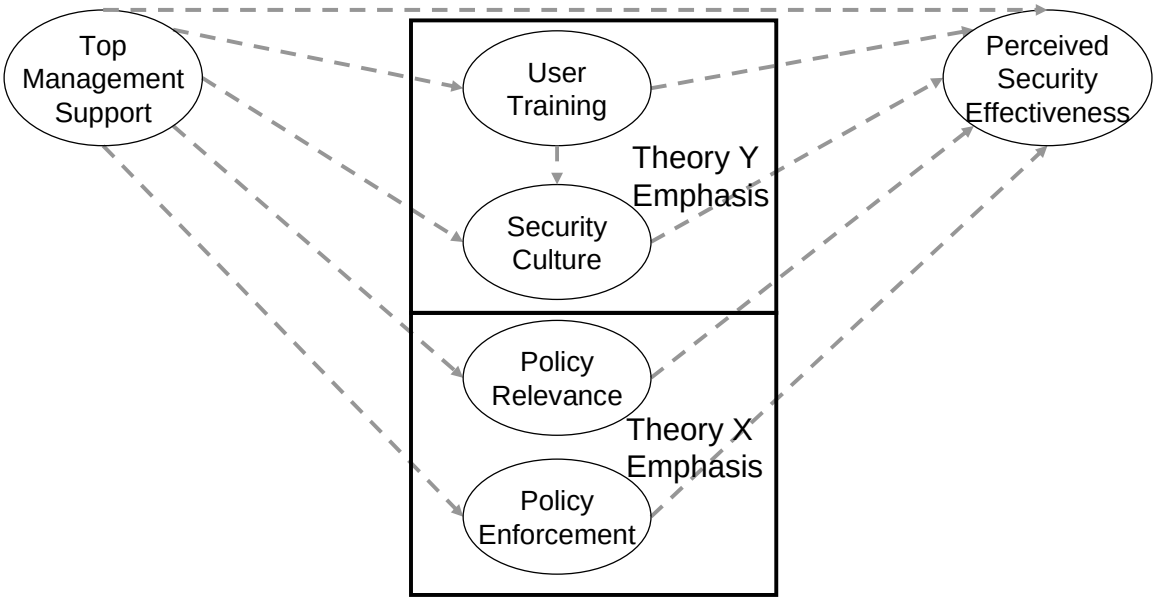


Figure 17. *Theory Y and Theory X Dichotomy*

Methodological Issues

This study proactively addressed a number of potential threats to validity. A post-results discussion on three of these threats are provided starting with perceived intrusiveness, construct bias, and finally, common method variance.

Perceived intrusiveness of the research topic. As noted in Chapter III, some researchers urge caution when engaging in information security research because of the perceived intrusive nature of the topic. Kotulic & Clark (2004) recommend a slow and deliberate approach to minimize potential problems when researching topics that are emerging or of a sensitive nature. The current study has both of these conditions. Thus, the researcher attempted to minimize the problem of perceived intrusiveness. The willingness-to-answer scale was critical in this endeavor. The expert panel rated every candidate item for levels of intrusiveness that helped remove survey questions

respondents might have been uncomfortable or unwilling to answer. Researchers engaged in topics where perceived intrusiveness might represent a problem should consider using this scale to help identify potentially intrusive questionnaire items.

This research employed other treatments aimed at maximizing respondent participation. Treatments included clearly displaying sponsorship of the project by the $(ISC)^2$ organization and mentioning the involvement of the CISSPs expert panel. Together, these remedies along with the others mentioned in Chapter III helped minimize problems relating to the perception of intrusiveness by research participants.

Some individuals dropped out of the survey in between phases of data collection. One sent an email to the researcher stating that he felt uncomfortable with completing the survey because of a company policy not to disclose any information regarding security policy. Even though the survey did not ask questions regarding policy content, which the instructions clearly stated, it is reasonable that a few participants would have misgivings about the survey as they proceed. In the end, a large sample was obtained for the study. While some participants dropped out, the researcher did not receive a single complaint regarding the intrusiveness or sensitivity of the survey instrument.

Construct and cultural issues. The following statement by Ford, Connelly, & Meister reflects the view that the IS literature benefits from studies that place emphasis on cross-cultural differences:

> *There is a need within IS for there to be interpretivist, critical, positivist, quantitative and qualitative research, research at the individual and organizational level, research at the regional and national levels, and research*

on cross-cultural differences between nations and sub-cultures within nations (2003, p.22).

One strength of the research sample of this study is the diversity of the sample pool within the homogeneous CISSP sub-culture. However, using CISSPs exclusively presents some limitations to the study as well. For instance, this constituency supports many workers in government and large business organizations. Concerns from participants in these organizations may have biased the model in favor of those organizations that typically hire certified IS security professionals. For example, only 6% of respondents came from the consumer products sector. Comparatively, the *policy relevance* construct may affect organizations in the healthcare sector more than those in the consumer products sector due to the focus of recent legislation such as the Health Insurance Portability and Accountability Act of 1996 (Volonino, Gessner, & Kermis, 2004). In future uses of the instrument from this study, researchers should be aware that some of the constructs might hold greater significance with certain demographic sub-samples than with others.

Likewise, cross-cultural differences may have biased the results of the study. Research has shown that certain management practices can be compatible and others incompatible depending on the culture of a society (Hofstede, 1993). For instance, highly individualist societies may accomplish policy enforcement differently than more collectivistic societies (Hunter & Beck, 2000). While cultural differences in the sample responses were minimal, the extensive CISSP certification requirements and the global nature of modern Internet security threats may have acted to minimize many cultural differences. Yang (1986, p.67) posited, "Will societal modernization eventually

eliminate cross-cultural psychological differences?" The proliferation of IT certification bodies with rigorous entrance requirements and their role in advancing socio-cultural modernization and minimizing cross-cultural differences is a potential question for future research. Since the theoretical model offers a general framework, specific uses of it should take national culture into account (McCoy, Galletta, & King, 2005).

One form of potential cross-cultural bias is method bias or common method variance. However, this bias can be reduced if careful attention is devoted to sampling and administration of the instrument (Karahanna et al., 2004). In this study, the instrument was administered identically to all participants (e.g. English language, same web site). A necessary goal in cross-cultural studies is sampling equivalence. This equivalence can be achieved if the cross-cultural groups are matched on key demographics, educational, and socioeconomic characteristics (Karahanna et al., 2004). In this study, the rigor of CISSP certification requirements helped to support sampling equivalence since membership requires a level of education, trade knowledge, professional experience, an ethical code, and currency requirements to maintain certification.

A technique used to detect the presence of bias is factor analysis, which can be used to examine the factor structure of an instrument across cultures and demographics. Based on the analysis in Chapter IV, the alternative, second-order factor model demonstrated a level of general applicability across the demographic sub-samples. The *a priori* model did not demonstrate the same level of general applicability across the demographic sub-samples as the second-order factor model, yet many of the statistical differences in the *a priori* model could be attributed to low statistical power.

When evaluating individual constructs for cultural bias, the results either did not indicate serious cultural bias or were inconclusive. It is difficult to draw reliable conclusions about potential construct bias when some of the sub-samples are very small (e.g. Hong Kong n=20). However, it is not surprising that serious cultural bias was not detected. The instrument developed in this study came from a grounded theory approach of analyzing open-ended question responses given to a sample of CISSPs. The words and phrases in the questionnaire items were extracted from the responses of these certified professionals who are content domain experts. Thus, by following methodological rigor, serious cultural issues may have been minimized or eliminated. Yet, the potential for this type of bias cannot be ruled out. A contribution of the present study is that it proposes two models of information security constructs that demonstrate an extent of cross-cultural applicability. Yet, for future research, the instrument and theoretical model should be applied to populations outside the CISSP membership in a more confirmatory setting.

Common method variance. Studies that rely on self-reported surveys are vulnerable to the inflation of variable correlations by common method variance (Lindell & Whitney, 2001). The seriousness of common method variance has been debated in the management literature (Facteau et al., 1995; Podsakoff et al., 2003) and IS literature (Straub et al., 2004; Whitman & Woszczynski, 2004). Some of the literature tends to generalize any *common variance* in data obtained from self-reported, cross-sectional surveys as common *method* variance or *method* bias. Because the results of this study indicate the existence of common variance, it is worthwhile to discuss this subject at

some length. This sub-section will evaluate some of the aspects of common method variance related to the findings of this study.

The present study employed temporal separation in data collection by inserting at least a three-day time lag between the collection of mediator (phase 1), independent (phase 2) and dependent (phase 3) variables. In addition, a degree of methodological separation was operationalized by having respondents complete phase 2 using a different response format and scale (i.e. seven-point Likert-scale using a spreadsheet attachment delivered through email). Procedural remedies such as these have the potential to minimize, if not eliminate, the effects of common method variance (Podsakoff et al., 2003).

Chapter IV contains the statistical tests to help determine the level of common variance in the data. The findings suggest that the theoretical model benefits from a common variance factor, although the model fit gain is small and that the theoretical models provide a significantly better fit than the single factor (common variance) model to the sampled data. These results suggest that the problem of common method variance did not overly influence the results. Yet, a sizable percentage of the overall variance (38%) was attributed to the common variance factor. However, the percent of common variance varied considerably by theoretical construct, suggesting that that the common variance is not uniformly systematic to the variables of the study.

The results in Chapter IV used the single latent factor technique to identify common variance (Facteau et al., 1995; Podsakoff et al., 2003). However, this method has a disadvantage that the researcher cannot distinguish between common *method* variance and variance due to relationships between the constructs other than the ones

hypothesized (Podsakoff et al., 2003, p.894). For example, this study focused on the managerial and not the technical aspects of IS security practice and its impact on effectiveness. Some of the common variance could originate from the technical dimension of IS security that this study did not measure. Another disadvantage of using the single factor method is that the method factor cannot interact with the variables of the study (Podsakoff et al., 2003) which limits the researchers ability to identify the source of common variance.

Another technique used in this study to analyze method variance involves the use of a marker variable as proposed by Lindell & Whitney (2001). The results of using the *task interdependence* scale (Van Der Vegt et al., 2003) as a marker variable are presented in the results section. While the marker variable technique has limitations (Podsakoff et al., 2003), the test provides a degree of confirmation that the 38% common variance was not systematic across all constructs measured in the survey instrument. If method bias was omnipresent in the survey instrument, one could argue that the percentage of variance in the marker variable would have been consistent with some of the correlations present in other variables of the study. Instead, the *task interdependence* variable demonstrated only one percent shared variance with the common factor. This suggests that the source of the common variance may not be due to the method.

Another technique used to analyze the source of common variance in this study compared the results from the pilot (N=68) to the large-scale survey data (N=740). All the variables collected during the pilot test were collected on the same questionnaire at the same point in time. By comparison, the large-scale survey employed a longitudinal design involving time lags (Sanchez & Viswesvaran, 2002). If the shared variance is

valid and predictable variance that is inherently part of the theoretical model, we should see consistency between the pilot and large-scale survey construct correlations. Since the correlations changed very little between the two data sets, support exists that the shared variance is valid, predictable, and not caused by the data collection method.

The proposition that common variance in survey data is not caused by method bias has been made in studies outside the IS domain. Some have argued that the validity of general condemnations of self-report methods are unwarranted and instead suggest that domain specific investigations are required to determine which areas of research are especially susceptible to artificially high correlations induced by method bias (Crampton & Wagner, 1994). Other studies suggest that common variance is a valid part of a theoretical network and reflect predictable behaviors of the phenomena of interest. Some of these include the medical study of exercise factors with significant cross-situational specificity (Lance et al., 2000), operations management constructs that share common characteristics (Tan & Wisner, 2003), higher order common factors describing shared genetic effects (Jang, McCrae, Angleitner, Riemann, & Livesley, 1998) and expected sources of common variance caused by social desirability or negative affinity (Kline, Sulsky, & Rever-Moriyama, 2000).

In summary, without additional studies involving data collection from other sources and using different methods than those employed in present study, an absolute determination on the source of the common variance cannot be made from the data. However, five indications tend to support the notion that the common variance in this study is an inherent part of the nomological network and not due to method bias. First, procedural remedies were employed to control for method variance. Second, the

constructs of the study are theoretically positively correlated with one another making it probable that common variance should exist. Third, the correlations between the independent variable and the other variables of the study changed very little from the pilot to the large-scale survey data. Fourth, the amount of common variance is not equally shared among the theoretical constructs of the study. This observation includes the marker variable *task interdependence* that had only one percent shared variance with the common factor. Finally, the instrument scales were developed using methodological rigor to include expert panels, pre-tests, and pilot tests to ensure item wordings and survey instructions were clear and less subject to method bias (Kline et al., 2000). Thus, a body of evidence suggests that the common variance in the model (38%) is predominately an artifact of the nomological network and not method bias.

Implications for Research & Practice

This study developed and empirically tested a management theory of organizational IS security. The theoretical model contained managerial constructs that influence the effectiveness of information security in organizations. The two theoretical models proposed in this study (the *a priori* and second-order factor model) represent some of the few theoretical models in the IS literature involving organizational *information security* constructs. Both models achieved statistical significance consistent with the earlier qualitative findings. IS researchers can test the theoretical models from this study using different samples from other certification constituencies, national cultures, specific industries, or in case studies. In addition, the survey instrument may be applied to non-security, organizational employees who are either supervisors or ordinary users instead of security professionals. Four of the constructs, *top management support*,

user training, *security culture*, and *perceived security effectiveness* would be most applicable to the non-security professional. The *policy relevance* and *policy enforcement* constructs, however, might not have the same applicability to non-security employees because the items in the scales may require a higher level of security knowledge to obtain reliable answers. Finally, since this study is more exploratory, it is recommended that future studies use the 35-item instrument that resulted from the pilot test rather than the 29-item instrument.

It is intended that the model developed from this study will promote knowledge exploitation where the research contributions address problems relevant to the IS security practitioner community (Dennis, 2001). The two models of this study emerged from a grounded theory analysis of qualitative data. The grounded models are especially relevant to practitioners since the practitioner community provided the data from which the models emerged. This is important considering that IS researchers continue to struggle to make research relevant to practitioners (Baskerville & Myers, 2004) despite the frequent calls for IS researchers to do so (Benbasat & Zmud, 1999).

Since the constructs of this study embody relevant issues of IS security, managers can improve security effectiveness by applying the theoretical model of this study to their organizations. Specifically, the measurement scales can be utilized to assess the effectiveness of an organization's security program. While the scales and the model do not include every aspect that should be important to managers, the model does focus on the most critical areas that managers can influence to bring about an effective information security program.

Managers who are serious about improving IS security should ensure that professionals such as CISSPs are in their ranks. With proper top management support, such professionals can develop and maintain processes that sustain a trained workforce, robust security policies, and advance a security-minded culture. Considering that security incidents are frequent and costly to businesses, it is especially critical today for organizations to take these practices seriously in order to secure their valuable information.

Conclusion of the Study

No organization or information system can have perfect security. Despite this, there are specific practices that management can do to maximize the protection of their critical information resources. Organizations today face a myriad of internal and external threats to the security of information. Inadequate security is a situation that should not be tolerated because the business risks associated with poor security are high. Because many computer and information security problems today require managerial rather than technical solutions, the theoretical model proposed in this study can help management focus their efforts in the areas where they can make the most difference.

The present study provides evidence that managerial leadership and support of practices promoting employee training, a security-minded culture, policy relevance and enforcement can have significant positive impacts on the overall security effectiveness of an organization. This theoretical and practical assertion is supported by a research project that used a rigorous qualitative-quantitative methodology that produced considerable empirical evidence to support this claim.

REFERENCES

Aggarwal, A. K. (2003). Internalization of End-Users. *Journal of End-User Computing, 15*(1), 54-56.

Allen, B. (1968). Danger Ahead! Safeguard Your Computer. *Harvard Business Review, 46*(6), 97-101.

Andres, H. P., & Zmud, R. W. (2003). A Contingency Approach to Software Project Coordination. *Journal of Management Information Systems, 18*(3), 41-70.

Aquinas, T. (2003). *Saint Thomas Aquinas Meditations, for Every Day* (E. C. McEniry, O.P., Trans.). Fort Collins, Colorado: Roman Catholic Books.

Arbuckle, J. L. (2003). Amos (Output Notes) (Version 5.0.1). Chicago, IL: Small Waters Corp.

Ariss, S. S. (2002). Computer Monitoring: Benefits and Pitfalls Facing Management. *Information & Management, 39*(7), 553-558.

Armstrong, C. P., & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: The Influence of Senior Leadership and IT Infrastructures. *Information Systems Research, 10*(4), 304-327.

Artner, B. (2000, October 9). *Does Your Company Culture Value Corporate Security? (Interview with Gartner Research Vice President)*. Retrieved May, 2004, from http://techrepublic.com.com/5102-6300-1030082.html

Bachrach, D. G., Powell, B. C., & Bendoly, E. (2004). *Organizational Citizenship Behavior and Performance Evaluations: The Impact of Task Interdependence.* Paper presented at the Academy of Management, New Orleans, LA.

Bagchi, K., & Udo, G. (2003). An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the AIS, 12*(46), 684-700.

Barman, S. (2002). *Writing Information Security Policies*. New York: New Riders.

Baron, R. M., & Kenny, D. A. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology, 51*, 1173-1182.

Baskerville, R., & Myers, M. D. (2004). Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice--Forward. *MIS Quarterly, 28*(3), 329-335.

Beachboard, J. C. (2004, August). *Conceptualizing IT Management: Testing a Competing Values Model of Policy Compliance.* Paper presented at the Tenth Americas Conference on Information Systems, New York, NY.

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly, 23*(1), 3-16.

Bento, A., & Bento, R. (2004). Empirical Test of a Hacking Model: An Exploratory Study. *Communications of the AIS, 14*(32), 678-690.

Boncella, R. J. (2001). Internet Privacy - at Home and at Work. *Communications of the AIS, 7*(14), 269-282.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective - Part I: The Causes. *MIS Quarterly, 1*(3), 17-32.

Bostrom, R. P., Olfman, L., & Sein, M. K. (1990). The Importance of Learning Style in End-User Training. *MIS Quarterly, 14*(1), 101-119.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. (1996). Key Issues in Information Systems Management: 1994-95 SIM Results. *MIS Quarterly, 20*(2), 225-242.

Browne, M. W., & Cudeck, R. (1993). Alternative Ways of Assessing Model Fit. In K. A. Bollen (Ed.), *Testing Structural Equation Models* (pp. 136-162). Newbury Park, CA.: Sage.

Buss, M. D. J., & Salerno, L. M. (1984). Common Sense and Computer Security. *Harvard Business Review, 84*(2), 112-121.

Byrne, B. M. (2001). *Structural Equation Modeling with AMOS*. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and Discriminant Validation by the Multi-Trait-Multimethod Matrix. *Psychological Bulletin, 56*(2), 81-105.

Chatterjee, D., & Grewal, R. (2002). Shaping up for E-Commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies. *MIS Quarterly, 26*(2), 65-89.

Clarke, S., & Drake, P. (2003). Social Perspective on Information Security: Theoretically Grounding the Domain. In S. Clarke, E. Coakes, G. M. Hunter & A. Wenn (Eds.), *Socio-Technical and Human Cognition Elements of Information Systems* (pp. 249-265). Hershey, PA: Idea Group Publishing.

Claver, E., Llopis, J., Gonzalez, M. R., & Gasco, J. L. (2003). The Performance of Information Systems through Organizational Culture. *Information Technology & People, 14*(3), 247-260.

Computer Emergency Response Team (CERT). (2004). *CERT Statistics*. Retrieved May, 2004, from http://www.cert.org/stats/cert_stats.html#incidents

Conger, J., A., Kanungo, R. N., & Menon, S. T. (2000). Charismatic Leadership and Follower Effects. *Journal of Organizational Behavior, 21*, 747-767.

Crampton, S. M., & Wagner, J., A. III. (1994). Percept-Percept Inflation in Microorganizational Research: An Investigation of Prevalence and Effect. *Journal of Applied Psychology, 79*(1), 67-76.

Daft, R. L., & Marcic, D. (2001). *Understanding Management* (3rd ed.). New York: Harcourt College Publishers.

Davis, S. A., & Bostrom, R. P. (1993). Training End Users: An Experimental Investigation of the Roles of the Computer Interface and Training Methods. *MIS Quarterly, 17*(1), 61-85.

DeLone, W. H. (1988). Determinants of Success for Computer Usage in Small Business. *MIS Quarterly, 12*(1), 51-61.

Dennis, A. R. (2001). Relevance in Information Systems Research. *Communications of the Association for Information Systems, 6*(Article 10), 7p.

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A Framework for Linking Culture and Improvement in Organizations. *Academy of Management Review, 25*(4), 850-863.

DeVellis, R. F. (2003). *Scale Development. Theory and Applications* (2nd ed. Vol. 26). Thousand Oaks, CA: Sage Publications.

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal, 11*(2), 127-153.

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review, 45*(1), 67-87.

Facteau, J. D., Dobbins, G. H., Russell, J. E. A., Ladd, R. T., & Kudisch, J. D. (1995). The Influence of General Perceptions of Training Environment on Pretraining Motivation and Perceived Training Transfer. *Journal of Management, 21*(1), 1-25.

Ford, D. P., Connelly, C., E., & Meister, D. B. (2003). Information Systems Research and Hofstede's Culture's Consequences: An Uneasy and Incomplete Partnership. *IEEE Transactions on Engineering Management, 50*(1), 8-26.

Frazier, P. A., Barron, K. E., & Tix, A., P. (2004). Testing Moderator and Mediator Effects in Counseling Psychology. *Journal of Counseling Psychology, 51*(1), 115-134.

Garg, A., Curtis, J., & Halper, H. (2003). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Systems Security, 12*(1), 22-34.

Gasson, S. (2004). Rigor in Grounded Theory Research: An Interpretive Perspective on Generating Theory from Qualitative Field Studies. In M. E. Whitman & A. B. Woszczynski (Eds.), *The Handbook of Information Systems Research*. Hershey, PA: Idea Group Publishing.

Gefen, D. (2003). Assessing Unidimensionality through LISREL: An Explanation and Example. *Communications of the AIS, 12*, 23-46.

George, J. F. (1996). Computer-Based Monitoring: Common Perceptions and Empirical Results. *MIS Quarterly, 20*(4), 459-480.

Ghoshal, S. (2005). Bad Management Theories Are Destroying Good Management Practices. *Academy of Management Learning & Education, 4*(1), 75-91.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New York: Aldine Publishing Company.

Gopal, R. D., & Sanders, G. L. (1997). Preventive and Deterrent Controls for Software Piracy. *Journal of Management Information Systems, 13*(4), 29-47.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). *9th Annual CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

Green, G., & Farber, R. C. (1975). *Introduction to Security*. Los Angeles, CA: Security World Publishing, Co. Inc.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Analysis* (5th ed.). Delhi, India: Pearson Education.

Hansche, S. D. (2002). Making Security Awareness Happen. In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (4th ed., Vol. 3, pp. 337-351). New York: Auerbach Publications.

Hare, C. (2002). Policy Development. In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (4th ed., Vol. 3, pp. 353-383). New York: Auerbach Publications.

Harrington, S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly, 20*(3), 257-278.

Harter, D. E., & Slaughter, S. A. (2003). Quality Improvement and Infrastructure Activity Costs in Software Development: A Longitudinal Analysis. *Organization Science, 49*(6), 784-800.

Hinkin, T. R. (1995). A Review of Scale Development Practices in the Study of Organizations. *Journal of Management, 21*(5), 967-988.

Hinkin, T. R. (1998). A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires. *Organizational Research Methods, 1*(1), 104-121.

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review*(Summer), 35-43.

Hofstede, G. (1993). Cultural Constraints in Management Theories. *Academy of Management Journal, 7*(1), 81-94.

Hone, K., & Eloff, J. H. P. (2002). Information Security Policy--What Do International Standards Say? *Computers & Security, 21*(5), 402-409.

Howard, P. D. (2003). The Security Policy Life Cycle: Functions and Responsibilities. In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (4th ed., Vol. 4, pp. 999). Boca Raton: CRC Press, LLC.

Hoyle, R. H. (1995). The Structural Equation Modeling Approach. In R. H. Hoyle (Ed.), *Structual Equation Modeling. Concepts, Issues, and Applications*. Thousand Oaks, CA: Sage Publications, Inc.

Hu, L.-T., & Bentler, P. M. (1995). Evaluating Model Fit. In R. H. Hoyle (Ed.), *Structural Equation Modeling. Concepts, Issues, and Applications* (pp. 76-99). Thousand Oaks, CA: Sage Publications, Inc.

Hunter, G. M., & Beck, J. E. (2000). Using Repertory Grids to Conduct Cross-Cultural Information Systems Research. *Information Systems Research, 11*(1), 93-101.

Im, K. S., & Grover, V. (2004). The Use of Structural Equation Modeling in IS Research: Review and Recommendations. In M. E. Whitman & A. B. Woszczynski (Eds.), *The Handbook of Information Systems Research*. Hershey, PA: Idea Group Publishing.

ISO/IEC. (2000). *Information Technology - Code of Practice for Information Security Management* (No. ISO/IEC 17799:2000(E)): The International Standards Organization/The International Electrotechnical Commission.

James, P. N. (1992). Education and Training. *Information Systems Management, 9*(2), 15-21.

Jang, K. L., McCrae, R. R., Angleitner, A., Riemann, R., & Livesley, W. J. (1998). Heritability of Facet-Level Traits in a Cross-Cultural Twin Sample: Support for a Hierarchical Model of Personality. *Journal of Personality and Social Psychology, 74*(6), 1556-1565.

Jarvenpaa, S. L., & Ives, B. (1991). Executive Involvement and Participation in the Management of Information Technology. *MIS Quarterly, 15*(2), 205-221.

Jasperson, J. S., Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J. P., & Zheng, W. (2002). Power and Information Technology Research: A Metatriangulation Review. *MIS Quarterly, 26*(4), 397-459.

Jöreskog, K. G. (1970). A General Method for Analysis of Covariance Structures. *Biometrika, 57*, 239-251.

Jöreskog, K. G., & Sörbom, D. (1984). LISREL Vi: Analysis of Linear Structural Relationships by Maximum Likelihood, Instrumental Variables and Least Squares Methods. Mooresville, IN: Scientific Software.

Kankanhalli, A., Hock-Hai, T., Bernard, C. Y. T., & Kwok-Kee, W. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly, 12*(4), 571-587.

Karahanna, E., Evaristo, R., & Srite, M. (2004). Methodological Issues in MIS Cross-Cultural Research. In M. E. Whitman & A. B. Woszczynski (Eds.), *The Handbook of Information Systems Research* (pp. 166-177). Hershey, PA: Idea Group Publishing.

Katzell, R. A., & Thompson, D. E. (1995). Work Motivation: Theory and Practice. In D. A. Kolb, J. S. Osland & I. M. Rubin (Eds.), *The Organizational Behavior Reader* (6th ed., pp. 110-124). Englewood Cliffs, New Jersey: Prentice Hall.

Kidder, L. H., & Judd, C. M. (1986). *Research Methods in Social Relations* (5th ed.). New York: CBS College Publishing.

King, W., R., & Zmud, R. W. (1981). *Managing Information Systems: Policy Planning, Strategic Planning, and Operational Planning.* Paper presented at the Proceedings from the 2nd International Conference on Information Systems, Boston, MA.

Klein, A. S., Masi, R. J., & Weidner, C. K. (1995). Organization Culture, Distribution, and Amount of Control and Perceptions of Quality. *Group & Organization Management, 20*(2), 122-148.

Kline, R. B. (1998). *Structural Equation Modeling*. New York: Guilford Press.

Kline, T. J. B., Sulsky, L. M., & Rever-Moriyama, S. (2000). Common Method Variance and Specification Errors: A Practical Approach to Detection. *The Journal of Psychology, 34*(4), 401-421.

Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Morrow, D. W. (2004). *Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)^2 Survey Results*. Alabama: Auburn University.

Kock, N. (2004). The Three Threats of Action Research: A Discussion of Methodological Antidotes in the Context of an Information Systems Study. *Decision Support Systems, 37*, 265-286.

Koh, C., Ang, S., & Straub, D. W. (2004). IT Outsourcing Success: A Psychological Contract Perspective. *Information Systems Research, 15*(4), 356-373.

Kotulic, A. G., & Clark, J. G. (2004). Why There Aren't More Information Security Research Studies. *Information & Management, 41*(5), 597-607.

Lance, C. E., Newbolt, W. H., Gatewood, R. D., Foster, M. R., French, N. R., & Smith, D. E. (2000). Assessment Center Exercise Factors Represent Cross-Situational Specificity, Not Method Bias. *Human Performance, 13*(4), 323-353.

Larsson, G., Larsson, B. W., & Munch, I. M. E. (1998). Refinement of the Questionnaire 'Quality of Care from the Patient's Perspective' Using Structural Equation Modeling. *Scandinavian Journal of Caring Science, 12*, 111-118.

Lee, S. M., Kim, Y. R., & Lee, J. (1995). An Empirical Study of the Relationship among End-User Information Systems Acceptance, Training, and Effectiveness. *Journal of Management Information Systems, 12*(2), 189-202.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories. *Information & Management, 41*(6), 707-718.

Leonard, L. N. K., & Cronan, T. (2000). Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences. *Journal of the Association for Information Systems, 1*(12), 1-31.

Lindell, M., K., & Whitney, D., J. (2001). Accounting for Common Method Variance in Cross-Sectional Research Designs. *Journal of Applied Psychology, 86*(1), 114-121.

Loughry, M. L. (2002). *Coworkers Are Watching: Performance Implications of Peer Monitoring.* Paper presented at the Academy of Management Conference, Hammersmith, London.

Lowery, C. L. (2002). *Developing Effective Security Policies: Powersolutions*. Retrieved May, 2004, from http://www.dell.com/powersoulutions

Luftman, J., & McLean, E. R. (2004). Key Issues for IT Executives. *MIS Quarterly Executive, 3*(2), 89-104.

MacKinnon, D. P., Krull, J. L., & Lockwood, C. (2000). Mediation, Confounding, and Suppression: Different Names for the Same Effect. *Prevention Science, 2*, 15-27.

Manz, C. C., & Stewart, G. L. (1997). Attaining Flexible Stability by Integrating Total Quality Management and Socio-Technical Systems Theory. *Organization Science, 8*(1), 59-70.

Markus, M. L. (1981). Implementation Politics: Top Management Support and User Involvement. *Systems, Objectives, and Solutions*, 203-215.

Marshall, T. E., & Byrd, T. A. (1998). Perceived Task Complexity as a Criterion for Information Support. *Information & Management, 34*, 251-263.

McCoy, S., Galletta, D. F., & King, W. R. (2005). Integrating National Culture into IS Reseach: The Need for Current Individual-Level Measures. *Communications of the Association for Information Systems, 15*, 211-224.

McGregor, D. M. (1995). The Human Side of Management. In D. A. Kolb, J. S. Osland & I. M. Rubin (Eds.), *The Organizational Behavior Reader* (6th ed., pp. 56-64). Englewood Cliffs, New Jersey: Prentice Hall.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis*. Thousand Oaks, California: Sage Publications.

Mitnick, K. (2003). Are You the Weak Link? *Harvard Business Review, 81*(4), 18-20.

Nahm, A. Y. (2003). The Impact of Organizational Culture on Time-Based Manufacturing and Performance. *Decision Sciences, 35*(4), 579-208.

Nelson, R. R., & Cheney, P. H. (1987). Training End Users: An Exploratory Study. *MIS Quarterly, 11*(4), 547-559.

Nunnally, J. (1978). *Psychometric Theory*. New York: McGraw-Hill.

Organ, D. W. (1988). *Organizational Citizenship Behavior: The Good Soldier Syndrome*. Lexington MA: Lexington Books.

Orlikowski, W. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science, 3*(3), 398-427.

Orlikowski, W. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly, 17*(3), 309-340.

Orne, M. T. (1979). On the Social Psychology of the Psychological Experiment. In R. T. Mowday & R. M. Steers (Eds.), *Research in Organizations: Issues and Controversies*. Santa Monica, CA: Goodyear Publishing Company, Inc.

Parker, D. B. (1981). *Computer Security Management*. Reston, Virginia: Reston Publishing Company.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2002). Software Pirarcy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems, 20*(1), 153-177.

Pearce, J. L., Sommer, S. M., Morris, A., & Frideger, M. (1992). *A Configurational Approach to Interpersonal Relations: Profiles of Workplace Social Relations and Task Interdependence* (Working Paper GSM #OB92015): University of California, Irvine.

Peltier, T. R. (2002). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* (1st ed.): CRC Press.

Piccoli, G., Ahman, R., & Ives, B. (1995). Web-Based Virtual Learning Environments: A Research Framework and a Preliminary Assessment of Effectiveness in Basic IT Skills Training. *MIS Quarterly, 25*(4), 401-426.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common Method Bias in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management, 12*(4), 531-544.

Post, G., & Kagan, A. (2000). Management Tradeoffs in Anti-Virus Strategies. *Information & Management, 37*(1), 13-24.

President. (2003, February). *National Strategy to Secure Cyberspace*. Retrieved May, 2004, from http://www.whitehouse.gov/pcipb

Purvis, R. L., Sambamurthy, V., & Zmud, R. W. (2001). The Assimilation of Knowledge Platforms in Organizations: An Empirical Investigation. *Organization Science, 12*(2), 117-135.

Ragins, B. R. (2000). Marginal Mentoring: The Effects of Type of Mentor, Quality of Relationship, and Program Design on Work and Career Attitudes. *Academy of Management Review, 43*(6), 1177-1194.

Ragu-Nathan, B. S., Apigian, C. H., Ragu-Nathan, T. S., & Tu, Q. (2004). A Path Analytic Study of the Effect of Top Management Support for Information Systems Performance. *Omega, 32*, 459-471.

Rainer, R. K., Jr., & Watson, H. J. (1995). What Does It Take for Successful Executive Information Systems? *Decision Support Systems, 14*, 147-156.

Richardson, R. (2003). *8th Annual Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

Rigdon, E. E. (1996). CFI Versus RMSEA: A Comparison of Two Fit Indices for Structural Equation Modeling. *Structural Equation Modeling, 3*(4), 369-379.

Robey, D., & Boudreau, M.-C. (1999). Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications. *Information Systems Research, 10*(2), 167-185.

Rossman, G. B., & Wilson, B. L. (1984). Numbers and Words: Combining Quantitative and Qualitative Methods in a Single Large-Scale Evaluation Study. *Evaluation Review, 9*(5), 627-643.

Sanchez, J., I., & Viswesvaran, C. (2002). The Effects of Temporal Separation on the Relations between Self-Reported Work Stressors and Stains. *Organizational Research Methods, 5*(2), 173-183.

Sarkar, S., & Lee, A. S. (2002). Using a Positivist Case Research Methodology to Test Three Competing Theories-in-Use of Business Process Redesign. *Journal of the AIS, 2*(2), 1-72.

Schein, E. H. (1995). Coming to a New Awareness of Organizational Culture. In D. A. Kolb, J. S. Osland & I. M. Rubin (Eds.), *The Organizational Behavior Reader* (Sixth ed.). Englewood Cliffs, New Jersey: Prentice Hall.

Schein, E. H. (1996). Defining Organizational Culture. In J. M. Shafritz & J. S. Ott (Eds.), *Classics of Organizational Theory* (4th ed.). New York: Harcourt Brace College Publishers.

Schou, C. D., & Trimmer, K. J. (2004). Information Assurance and Security. *Journal of Organizational and End User Computing, 16*(3), i-vii.

Segars, A. H., & Grover, V. (1998). Strategic Information Systems Planning Success: An Investigation of the Construct and Its Measurement. *MIS Quarterly, 22*(2), 139-163.

Sein, M. K., Bostrom, R. P., & Olfman, L. (1999). Rethinking End-User Training Strategy: Applying a Hierarchical Knowledge-Level Model. *Journal of End-User Computing, 11*(1), 32-39.

Sharma, R., & Yetton, P. (2003). The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation. *MIS Quarterly, 27*(4), 533-555.

Shaw, N. C., DeLone, W. H., & Niederman, F. (2002). Sources of Dissatisfaction in End-User Support: An Empirical Study. *The DATABASE for Advances in Information Systems, 33*(2), 41-57.

Simon, H. A. (1957). *Administrative Behavior* (2nd ed.). New York: The Free Press.

Smircich, L. (1992). Organizations as Shared Meanings. In J. M. Shafritz & J. S. Ott (Eds.), *Classics of Organization Theory* (3rd ed.). Pacific Grove, CA: Brooks, Cole Publishing Company.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly, 20*(2), 167-196.

Spector, P. E. (1992). A Consideration of the Validity and Meaning of Self-Report Measures of Job Conditions. In C. L. Cooper & I. T. Robertson (Eds.), *International Review of Industrial and Organizational Psychology*. West Sussex, England: John Wiley.

Spector, P. E. (1994). Using Self-Report Questionnaires in OB Research: A Comment on the Use of a Controversial Method. *Journal of Organizational Behavior, 15*, 385-392.

Srinivasan, A. (1985). Alternative Measures of System Effectiveness: Associations and Implications. *MIS Quarterly, 9*(3), 243-253.

Stanne, M. B., Johnson, D. W., & Johnson, R. T. (1999). Does Competition Enhance or Inhibit Motor Performance: A Meta-Analysis. *Psychological Bulletin, 125*, 133-154.

Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly, 13*(2), 146-169.

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

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validating Guidelines for IS Positivist Research. *Communications of the AIS, 13*(24), 380-427.

Straub, D. W., & Goodhue, D. L. (1991). Security Concerns of System Users. A Study of Perceptions of the Adequacy of Security. *Information & Management, 20*(1), 13-27.

Straub, D. W., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring System Usage: Implications for IS Theory Testing. *MIS Quarterly, 41*(8), 1328-1342.

Straub, D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly, 14*(1), 45-60.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469.

Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research. Techniques and Procedures for Developing Grounded Theory* (2nd ed.). Thousand Oaks, CA: Sage.

Strickland, L. H. (1958). Surveillance and Trust. *Journal of Personality, 26*, 200-215.

Swanson, M., & Guttman, B. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Washington D. C.: U.S. Department of Commerce, National Institute of Standards and Technology (NIST).

Tan, K.-C., & Wisner, J. D. (2003). A Study of Operations Management Constructs and Their Relationships. *International Journal of Operations & Production Management, 23*(11), 1300-1325.

Thong, J. Y. L., Yap, C. S., & Raman, K. S. (1996). Top Management Support, External Expertise, and Information Systems Implementation in Small Business. *Information Systems Research, 7*(2), 248-267.

Thong, J. Y. L., Yap, C. S., & Raman, K. S. (1997). Environments of Information Systems Implementation in Small Businesses. *Journal of Organizational Computing and Electronic Commerce, 7*(4), 253-278.

Tolsby, J. (1998). Effects of Organizational Culture on a Large Scale IT Introduction Effort: A Case Study of the Norwegian Army's EDBLF Project. *European Journal of Information Systems, 7*(2), 108-114.

Tompkins, W. (2002). Maintaining Management's Commitment. In H. F. Tipton & M. Krause (Eds.), *Information Systems Management Handbook* (Vol. 3). New York: Auerbach Publications.

Turkel, M. C., & Ray, M. A. (2001). Rational Complexity: From Grounded Theory to Instrument Development and Theoretical Testing. *Nursing Science Quarterly, 14*(4), 281-287.

van de Vijver, F., & Poortinga, Y. H. (1997). Towards an Integrated Analysis of Bias in Cross-Cultural Assessment. *European Journal of Psychological Assessment, 13*, 21-29.

Van Der Vegt, G. S., Eman, B. J. M., & Van De Vliert, E. (2001). Patterns of Interdependence in Work Teams: A Two-Level Investigation of the Relations with Job and Team Satisfaction. *Personnel Psychology, 54*, 51-69.

Van Der Vegt, G. S., Van De Vliert, E., & Oosterhof, A. (2003). Informational Dissimilarity and Organizational Citizenship Behavior: The Role of Intrateam Interdependence and Team Identification. *Academy of Management Journal, 46*(6), 715-727.

Van Tassel. (1972). *Computer Security Management*. Englewood Cliffs, New Jersey: Prentice-Hall.

Venkatraman, N., & Ramanujam, V. (1987). Measurement of Business Economic Performance: An Examination of Method Convergency. *Journal of Management, 13*(1), 109-122.

Volonino, L., Gessner, G. H., & Kermis, G. F. (2004). Holistic Compliance with Sarbanes-Oxley. *Communications of the Association for Information Systems, 14*, 219-233.

Von Bertanlanffy, L. (1950). The Theory of Open Systems in Physics and Biology. *Science, 3*, 23-29.

von Solms, R., & von Solms, B. (2004). From Policies to Culture. *Computers & Security, 23*, 275-279.

Wageman, R. (1995). Interdependence and Group Effectiveness. *Administrative Science Quarterly, 40*(1), 145-181.

Wasserman, J. J. (1969). Plugging the Leaks in Computer Security. *Harvard Business Review, 47*(5), 119-129.

Watson, R. T., Kelly, G. G., Galliers, R. D., & Brancheau, J. C. (1997). Key Issues in Information Systems Management: An International Perspective. *Journal of Management Information Systems, 13*(4), 92-115.

Whitman, M. E., & Mattord, H. J. (2004). *Management of Information Security*. Cambridge, MA: Course Technology - Thompson Learning.

Whitman, M. E., & Woszczynski, A. B. (2004). The Problem of Common Method Variance in IS Research. In M. E. Whitman & A. B. Woszczynski (Eds.), *The Handbook of Information Systems Research*. Hershey, PA: Idea Group Publishing.

Williams, L. J., Cote, J. A., & Buckley, M. R. (1989). Lack of Method Variance in Self-Reported Affect and Perceptions at Work: Reality or Artifact? *Journal of Applied Psychology, 74*, 462-468.

Wood, C. C. (2003). *Information Security Policies Made Easy* (9th ed.): Net IQ Corporation.

Yang, K. S. (1986). Will Societal Modernization Eventually Eliminate Cross-Cultural Psychological Differences. In M. H. Bond (Ed.), *The Cross-Cultural Challenge to Social Psychology*. Newbury Park, CA: Sage.

Zviran, M., & Haga, W. J. (1999). Password Security: An Empirical Study. *Journal of Management Information Systems, 15*(4), 161-185.

APPENDIX A

List of Categories after Open Coding

Fifty-seven categories after open-coding listed in alphabetical order

1 3rd Party Connectivity Issues
2 Applications & Systems Development & LC Support
3 Auditing Of Systems
4 BC & DP
5 Biometrics
6 Change Management/Rapid Change
7 Computer Crime
8 Configuration Management
9 Embedded, Small, Mobile Devices
10 Encryption
11 External Threats
12 Firewall & IDS Configurations
13 Funding And Budgets
14 Governance
15 Grid Computing
16 Hacker Threat
17 High Cost Of Security
18 Home Computer Security
19 Inappropriate Use Of Resources
20 Incident Response
21 Industrial Espionage
22 Information Warfare Concerns
23 Institutes Of Higher Learning
24 Integrated Security Management
25 Intellectual Property
26 Internal Threats
27 Justifying Expenditures (ROI)
28 Lack Of Skilled Security Staff
29 Legacy Systems
30 Logging & Monitoring/Event Correlation
31 Malware (Virus, Trojan, Worms…)
32 Misinformation In The Media

33 Network Security Architecture
34 Organizational Culture
35 OS Insecurity
36 Outsourced Personnel
37 Over Reliance On Technology & Tools
38 Patch Management
39 Personnel Security
40 Physical Security Issues
41 Policy Development, Enforcement
42 Privacy
43 Remote Access/Telecommunicating Issues
44 Single IT Platform Dominance
45 Single Sign On/Password Mgt/Access Control
46 Small/Medium Sized Business Security
47 Social Engineering
48 Software And Systems Inherent Insecurity
49 Spam
50 Standards, Lack Of Universal
51 Strategy, Lack Of Vision
52 Top Management Support
53 Training Of Security & IT Personnel
54 User Awareness Training And Education
55 Vulnerability & Risk Management
56 Web Services/Port 80 Threats
57 Wireless Vulnerabilities

APPENDIX B

List of Categories after Axial Coding

Twenty-five categories after axial coding reviewed and prioritized by 115 CISSPs and listed in ranked order.

1 User Awareness Training and Education
2 Top Management Support
3 Patch Management
4 Policy Related Issues (i.e. Enforcement)
5 Malware (i.e. Virus, Trojans, Worms)
6 Legal and Regulatory Issues
7 Low Funding and Inadequate Budgets
8 Inherent Insecurity of IS and Networks
9 Wireless Vulnerabilities
10 Internal Threats
11 Access Control and Identity Management
12 Governance
13 Vulnerability & Risk Management
14 Systems Dev & Life Cycle Support
15 Lack of a Skilled Security Workforce
16 Protection of Personnel Info (Privacy)
17 Business Continuity & Disaster Planning
18 Justifying Security Expenditures
19 Fighting Spam
20 Lack of Standards
21 Firewall & IDS Configurations
22 Organizational Culture
23 Security Training for IT Staff
24 Network Security Architecture
25 External Connectivity to Org Networks

APPENDIX C

Results of Critical Issues in Information Security Survey

(From Knapp et al., 2004)

Executive Summary

Information security is one of the most critical domains challenging the modern organization. As organizations face an increasing variety of security threats, the number and type of issues have become progressively more complex. Improved knowledge of the full-range of critical information security issues will help practitioners and researchers focus on solving the leading problems.

The purpose of this study is to promote a better understanding of the most critical information security issues. This purpose has two primary motivations. The first is to provide organization executives and information technology (IT) managers a methodically derived list of the top 25 information security issues. Second, to offer information system (IS) academics a list of topics that can provide direction to future research and theory development.

Project Background

The 25 information security issues in this survey surfaced using an established methodology aimed at providing reliable and valid results. This project involved four phases.

In Phase 1, 220 Certified Information System Security Professionals (CISSP) responded to an open-ended question asking for the top five information security issues facing organizations today. Researchers then created 57 issue categories based on a content analysis of the key words and themes of the responses.

In Phase 2, the 1,100 issues (220 participants x five issues each) were placed into one of the 57 categories for which it was best suited. Using the content from the responses, researchers developed definitions for the top 25 of the 57 categories.

In Phase 3, 115 of the 220 participants reviewed the preliminary list of 25 issues. In doing so, participants ranked the issues while providing comments about the proposed categories and definitions. Based on the feedback, researchers made changes to some of the definitions.

In Phase 4, 874 $(ISC)^2$ certified professionals ranked their top 10 of the 25 finalized issues. This process took place on a web-based survey between January and March 2004. Table 1 lists the top ten issues. Table 2 details the complete top 25 results. Appendix A contains the issue definitions.

This report presents only aggregated results of the survey without identification of survey participants or organizations.

Table 55. *The Top Ten Ranked Issues*

Rank	Issue Category
1	Top Management Support
2	User Awareness Training & Education
3	Malware
4	Patch Management
5	Vulnerability & Risk Management
6	Policy Related Issues
7	Organization Culture
8	Access Control & Identity Management
9	Internal Threats
10	Business Continuity/Disaster Preparation

Summary of Key Findings

- A high level of agreement concerning the top five issues exists across most of the demographics. A consensus of the top information security issues seems to exist.

- Managerial rather than technical issues dominate the list of top issues.

- An impressive 34% of total respondents ranked *Top Management Support* as one of their first three issues.

- Internationally, a number of particular issues demonstrated a high degree of variability in their rankings, particularly *Low Funding & Inadequate Budgets, Lack of Skilled Security Workforce*, and *Governance*.

- Of the demographic categories in the study, the rankings by respondents who identified themselves as consultants correlated the highest with the full survey results (all 874 respondents).

- Of the demographic categories in the study, the rankings by respondents in the education sector had the lowest correlation with the full results.

- Rankings among respondents at different organizational positions (e.g. top versus lower management) demonstrated a high level of overall agreement.

- During survey development, the scope and definition of the issues revealed how participants perceive many security problems. For instance, participants described some issues broadly, such as *Internal Threats*, and others narrowly, such as *Fighting SPAM*.

- During survey development, participants identified 33 additional issue categories. While these issues did not make the top 25 list, many considered them very important.

Table 56. *Top 25 Ranking Survey Results (874 respondents)*

Rank	Issue	Total Score[22]	Ave Rank	Times in Top 10	Times Ranked #1
1	Top Management Support	3678	7.14	515	165
2	User Awareness Training & Education	3451	5.95	580	78
3	Malware	3336	6.42	520	91
4	Patch Management	3148	5.85	538	57
5	Vulnerability & Risk Management	2712	5.53	490	47
6	Policy Related Issues	2432	5.43	448	26
7	Organization Culture	2216	5.44	407	33
8	Access Control & Identity Management	2203	5.22	422	30
9	Internal Threats	2142	5.33	402	36
10	Business Continuity/Disaster Prep	2030	5.02	404	23
11	Low Funding & Inadequate Budgets	1811	5.75	315	32
12	Protection of Privileged Information	1790	5.61	319	35
13	Network Security Architecture	1636	5.00	327	17
14	Security Training for IT Staff	1604	4.98	322	11
15	Justifying Security Expenditures	1506	5.21	289	18
16	Inherent Insecurity of Networks & Info Systems	1502	5.44	276	39
17	Governance	1457	5.90	247	36
18	Legal & Regulatory Issues	1448	5.25	276	23
19	External Connectivity to Org. Networks	1439	5.29	272	15
20	Lack of Skilled Security Workforce	1370	5.02	273	13
21	Systems Development & Life Cycle Support	1132	4.68	242	9
22	Fighting SPAM	1106	4.67	237	13
23	Firewall & IDS Configurations	1100	5.12	215	13
24	Wireless Vulnerabilities	1047	4.65	225	7
25	Standards Issues	774	4.32	179	7

[22] Total Score is the sum of all respondent's top ten rankings on a reverse scale.

APPENDIX D

Text Of Email Blast from $(ISC)^2$ to Constituency

From: ISC2_Users-owner@mail.isc2.org [mailto:ISC2_Users-owner@mail.isc2.org] On Behalf Of (ISC)2 Management
Sent: Friday, January 14, 2005 9:54 PM
To: isc2_users@isc2.org
Subject: OFFICIAL: (ISC)²® and Auburn University Invite your Participation in the Online Critical Issues in Information Security Survey

In connection with 2005 - The Year of the Information Security Professional, (ISC)² is sponsoring research projects to increase understanding and raise awareness of the vital role information security professionals play in today's global information society.

Researchers at Auburn University, who are among supporters of the Year initiative, are conducting a survey investigating associations between many of the top issues constituents currently face. The team at Auburn will feature the survey results in articles to be published in academic and practitioner journals.

How to Participate

Your contributions are needed to make this survey an informative and valuable service. We invite CISSPs and SSCPs worldwide to take the online Critical Issues in Information Security Survey. This survey uses 100% SSL encryption, and all information obtained will remain fully confidential. Click here to participate. The survey will remain open until 5 p.m. EST, on Friday, Feb. 4, 2005.

Constituent Briefing (via Webinar) on Jan. 17

James Duffy, president and CEO of (ISC)², …snip…

To register for the Webinar, click here.

To validate the source of this email, please login to the members' side of the (ISC)² Website and visit the eBlast Archives

APPENDIX E

Phase One, Two, & Three Survey Instruments

Survey on Critical Dimensions of Information Security

Thank you for expressing interest in this survey. Through your participation as a CISSP or SSCP, we hope to learn more about important aspects of information security. This survey asks for your opinion about the security-related practices of the organization (i.e. company or enterprise) you currently work for or support.

Two prerequisites for taking this survey:
1) You are a CISSP or SSCP.
2) You have sufficient experience at the current organization (company/enterprise) that you work for to have an opinion about its security-related practices.

Consultants or outsourced employees: If you divide your time supporting more than one client, answer the questions in relation to the organization where you spend most of your time.

Three Phases: This survey takes about 25 minutes to complete over three phases. This is the first phase and takes about 15-20 minutes. You will be contacted by email for Phase 2 and 3 over the next week. These phases will take about 5 minutes each.

****

Privacy & Survey Information:

A 12-member panel of CISSPs evaluated *each* question. Only questions evaluated as non-intrusive (i.e. non-sensitive) are asked in this survey. Thus, the following topics are NOT asked: system architecture, configurations, vulnerabilities, incidents, or policy content.

Kenneth Knapp, an Auburn University doctoral student, is conducting this study. He is supervised by Thomas Marshall, PhD. Address questions to Kenneth Knapp. Information collected in this study will be part of a dissertation and published in professional journals. Only aggregated results will be published.

Information obtained in this study identified to you will remain fully confidential. Other than an email address, only general demographic questions are asked. Your email address will not be shared with anyone. Click for the Web Surveyor privacy policy. Please participate only once.

All participants will receive a report of the results by email. After delivery, we will delete your email address from our files.

Your decision whether or not to participate will not jeopardize relations with Auburn University or (ISC)2. If you withdraw from this study, we will delete all provided information.

For information about your rights as a participant, contact Auburn University's Office of Human Subjects Research. Contact E.N. Burson, (334) 844-5966, bursoen@auburn.edu.

If you agree to participate, please click the NEXT PAGE below.
Otherwise, close this window

Demographic Questions: All questions pertain to the entire organization (i.e. company or enterprise) that you work for or support.

Answering these questions is very important for correct interpretation of the survey results. Please select the best answer.

Please enter your email address (* required):

Please select your certification:

- ☐ CISSP
- ☐ SSCP

How many employees work in the organization?

- ○ less than 500
- ○ between 500-2,499
- ○ between 2,500-7,499
- ○ between 7,500-15,000
- ○ more than 15,000

Select the country where you work. To protect anonymity, only countries with at least seven CISSP/SSCPs are listed. Please select OTHER if not listed.

Select One

Are you an outsourced (consultant) worker?

- ○ NO, I'm a regular/permanent employee.
- ○ YES, I'm an outsourced worker.

From the list below, please select the primary industry(s) that best describes the organization you work for or are supporting. If you are a consultant, please select consultant along with the industry(s) you are currently supporting.

- ☐ Consultant
- ☐ Government - federal, local, military, police, etc.

- [ ] Medical/Healthcare - public or private
- [ ] Finance, Banking & Insurance
- [ ] Professional Services - Legal, Marketing, etc.
- [ ] Consumer Products/Retail/Wholesale
- [ ] Education/Training
- [ ] Energy
- [ ] Info Tech-Security-Telecomm
- [ ] Entertainment
- [ ] Industrial Tech
- [ ] Manufacturing
- [ ] Non-Profit
- [ ] Publishing
- [ ] Travel/Hospitality
- [ ] Transportation/Warehousing
- [ ] Utilities
- [ ] Real Estate, Rental & Leasing
- [ ] Other (please specify)

If you selected other, please specify:

Which of the following most closely describes your current job function? (Please check only one)

- [ ] Owner/Partner
- [ ] Senior manager/Executive (e.g. CEO, CIO)
- [ ] Department manager/supervisor/director
- [ ] MIS/IS/IT/technical management
- [ ] Other managerial
- [ ] Other IT/technical/scientific/professional

How many total years of experience do you have in both information technology and security?

- less than 8
- between 8 and 15
- more than 15

Is information security a primary or secondary responsibility in the normal course of your job?

- primary
- secondary

How many years of experience do you have with the current organization?

- 1 year or less
- 2-4 years
- 5 years or more

Select the best answer.

Does the organization have a dedicated office responsible for addressing information security issues?

- Yes
- No
- Not Sure

Does the organization have a top security position such as Chief Security Officer, CISO, Director of Information Security or an equivalent?

- Yes
- No
- Not Sure

At what organizational level are information security policies officially approved?

- Executive or Upper Management
- Middle Management
- Other management
- The organization has policies, but management does not approve them
- The organization does not have approved policies

Directions: Choose the answer that best reflects your opinion about the entire organization (company) that you work for or provide support in regards to information security.

For each statement in the survey, the following scale is provided:

SD =	Strongly Disagree or the statement is definitely false.
D =	Disagree or the statement is mostly false.
N =	Neutral, no opinion or the statement is equally true and false.
A =	Agree or the statement is mostly true.
SA =	Strongly Agree or the statement is definitely true.

Please do not skip questions--*this is important in order to fully apply your input.*

The following statements begin with the phrase: In the organization[23],

	SD	D	N	A	SA
Practicing good security is part of the shared beliefs of employees.					
Information security policy is properly enforced.					
Information security is a key norm shared by organizational members.					
Information security policies reflect the objectives of the organization.					
Security has traditionally been considered an important organizational value.					
The overall environment fosters security-minded thinking.					
Information security policies are aligned with business goals.					

The following statements begin with the phrase: In the organization,

Policy is updated when legal & regulatory changes require it.					
A culture exists that promotes good security practices.					
Repeat security offenders are appropriately disciplined.					
Employees value the importance of security.					
Top management is properly informed of vital information security developments.					
Employee computer practices are properly monitored for policy violations.					
Information security policies often conflict and contradict each other.					
Information security policies are written with the proper understanding of legal requirements.					
Policies are consistently enforced across the organization.					

[23] Note: items were randomized in blocks of around 10 questions each by the survey software.

The following statements begin with the phrase: In the organization,

There is intensity among employees to achieve security goals.
Practicing good security is the accepted way of doing business.
The need to protect information is a basic assumption of employees.
An established information security policy review and update process exists.
Security policy is properly updated on a regular basis.
Employees often complain about security rules.
Employees caught violating important security policies are appropriately corrected.
There is intensity among employees to achieve security goals.
Practicing good security is the accepted way of doing business.
The need to protect information is a basic assumption of employees.
An established information security policy review and update process exists.
Security policy is properly updated on a regular basis.
Employees often complain about security rules.
Employees caught violating important security policies are appropriately corrected.

The following statements begin with the phrase: In the organization,

Employees have a favorable attitude about security.
The information security staff keeps top management informed on vital issues.
Information security rules are enforced by sanctioning the employees who break them.
Termination is a consideration for employees who repeatedly break security rules.
Information security policy is consistently updated on a periodic basis.
Information security policy is updated when technology changes require it.
Risk assessments are conducted prior to writing new security policies.

The following questions refer to typical information security tasks that you perform in the organization. Colleagues refers to other people that you work with in the organization. Select the best choice.

I have to work closely with my colleagues to do my work properly.
I depend on my colleagues for the completion of my work.
In order to complete their work, my colleagues have to obtain information and advice from me.
In order to complete our work, my colleagues and I have to exchange information and advice.
I have a one-person job; I rarely have to check or work with others.

Indicate the percentage of your tasks for which you have to exchange information or cooperate with others in your organization.

per cent

Indicate the total number of hours per day you have to exchange information or cooperate with others to do your job well.

hours per day

****

In general, what do you feel is the most critical factor in determining whether an organization's information security program will be effective or not. (Answer with a short phrase.)

Why is this the most critical factor? (Please explain.)

The following statements begin with the phrase: In the organization,

Users receive adequate security training prior to getting a network account.
Necessary efforts are made to educate employees about new security policies.
Top management is comfortable discussing information technology (IT) issues.
The IT staff has been sufficiently trained regarding information security policies.
Important security policies are unknown to many employees.
The information security program is successful.
Information security awareness is communicated well.
A continuous, ongoing security awareness program exists.

The following statements begin with the phrase: In the organization,

Social engineering threats are properly addressed during employee security training.
Top management is often involved in deciding critical technology issues.
Users receive adequate security refresher training appropriate for their job function.
The security staff does a good job of getting top management involved in important issues.
A variety of business communications (notices, posters, newsletters, etc.) are used to promote security awareness.
An effective security awareness program exists.
Employees clearly understand the ramifications of violating security policies.

If you have comments to leave the researcher, please feel free to type them here.

Thank you for participating.

We will send you the PHASE 2 questions by email in about three days. PHASE 3 will follow about three days after completion of PHASE 2. Both of these phases are much shorter and will take about 5 minutes each.

Once SUBMIT SURVEY is selected, you will not be able to return to any previous page.

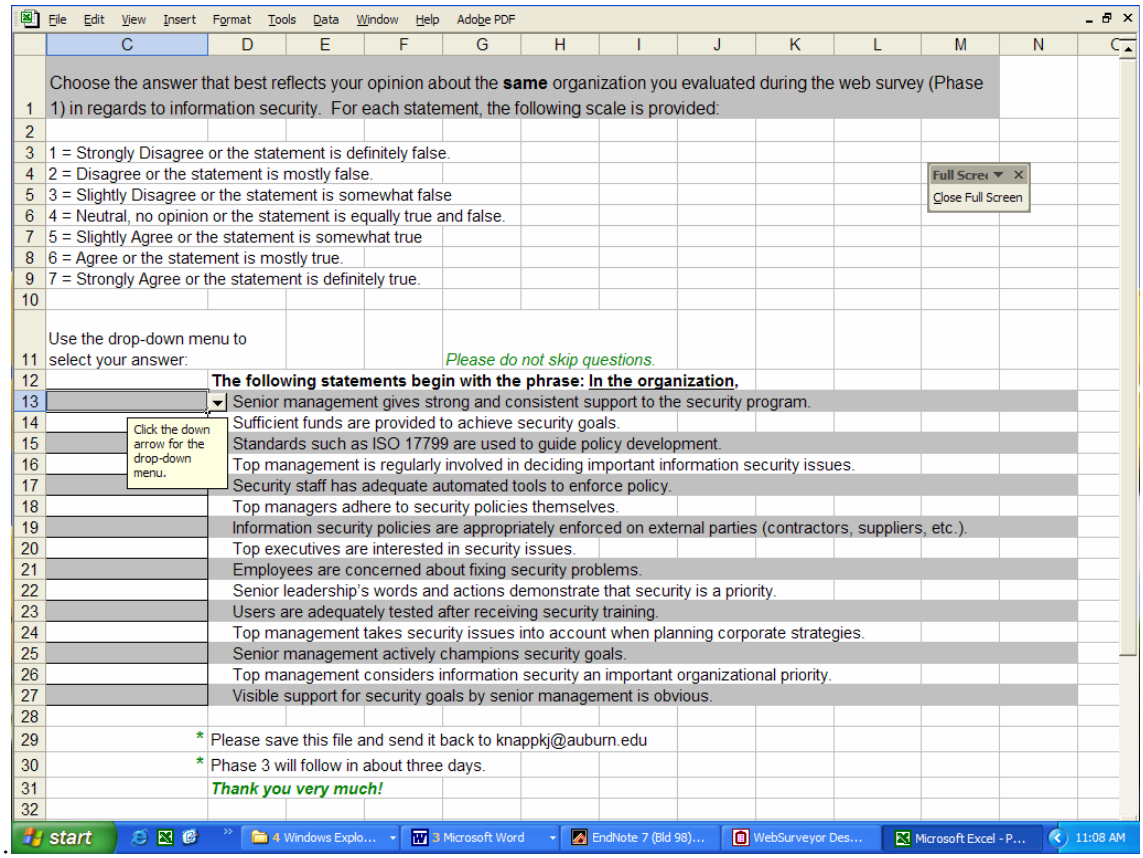


Figure 18. *Phase Two Questionnaire in Excel.*

.

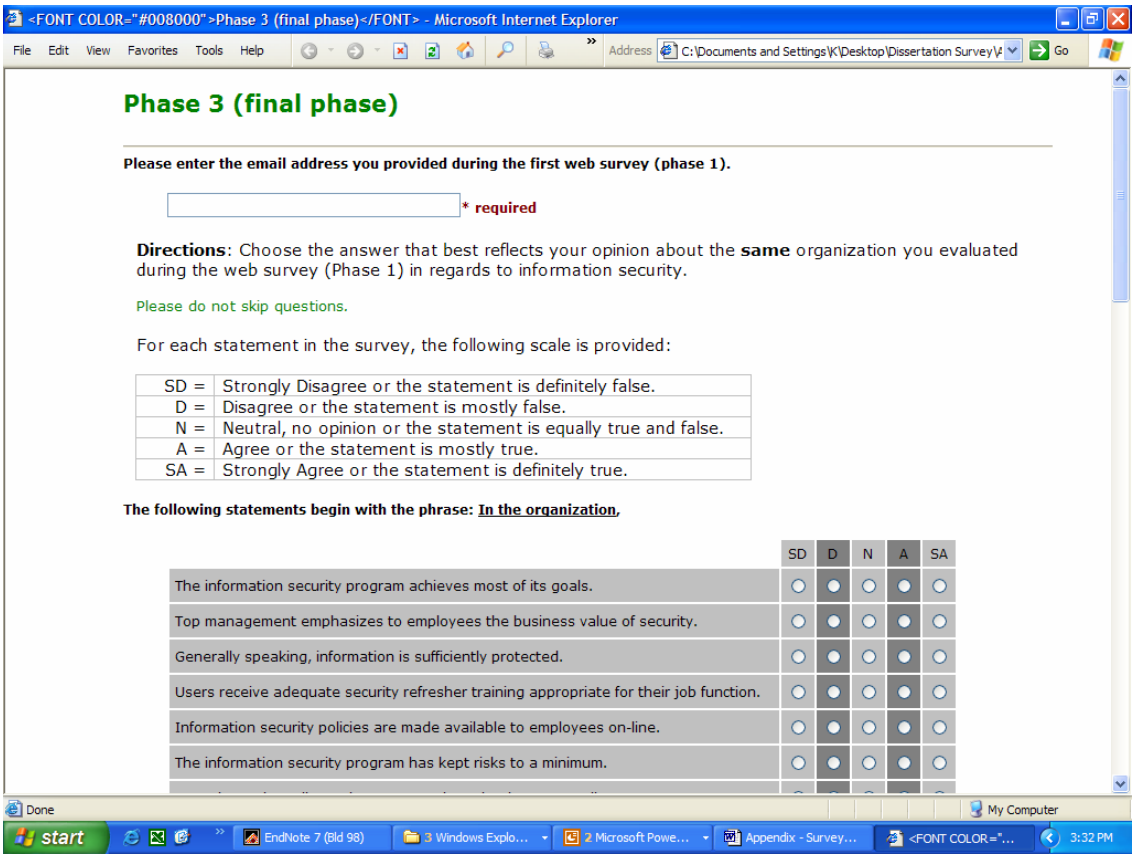


Figure 19. *Phase Three Web Survey in Microsoft Explorer*

Phase 3 (final phase)

Please enter the email address you provided during the first web survey (phase 1).

*** required**

Directions: Choose the answer that best reflects your opinion about the **same** organization you evaluated during the web survey (Phase 1) in regards to information security.

Please do not skip questions.

For each statement in the survey, the following scale is provided:

SD =	Strongly Disagree or the statement is definitely false.
D =	Disagree or the statement is mostly false.
N =	Neutral, no opinion or the statement is equally true and false.
A =	Agree or the statement is mostly true.
SA =	Strongly Agree or the statement is definitely true.

The following statements begin with the phrase: In the organization,
The information security program achieves most of its goals.
Top management emphasizes to employees the business value of security.
Generally speaking, information is sufficiently protected.
Users receive adequate security refresher training appropriate for their job function.
Information security policies are made available to employees on-line.
The information security program has kept risks to a minimum.
Formal security policy reviews are conducted at least annually.
Information security policies are written in a manner that is clear and understandable.
Employees value the importance of security.
Overall, the information security program is effective.
Employees are properly trained about the dangers of the Internet.
Adequate in-house security knowledge among security staff exists.
The information security program accomplishes its most important objectives.

PHASE 2. If you haven't sent in the Phase 2 responses yet, we can resend the email to you. (e.g. Perhaps the email didn't arrive.) If so, please check the box.

☐ Send the Phase 2 email to me.

Thank you. This completes Phase 3. If you have any questions, feel free to send me an email: knappkj@auburn.edu. We plan to issue a final report in May. When complete, please hit **Submit Survey** below.

APPENDIX F

CISSP Statements from the Phase One Web Survey

The CISSP/SSCPs who completed Phase 1 of this study were given the following open-ended question: *In general, what do you feel is the most critical factor in determining whether an organization's information security program will be effective or not.*

Multiple verbatim statements are provided categorized by the constructs of this study. Many statements overlap categories. Reviewing these statements helps to provide a richer meaning and interpretation of the quantitative results of this study.

Statements on Top Management Support

- Without management support resources will be allocated, lower level staff will not believe security is important and policies will not be enforced.
- Without top management support the information security program will become merely a suggestion. Because information security can often be considered as a nuisance, the suggestions will not be followed.
- Without executive management support security doesn't receive proper attention, coordination across the business, coordination with business process, appropriate authority for enforcement, or appropriate funding.
- Without top management support, the information security program and policies are just a "paper" and not being enforced.
- With senior management support policies will receive the proper levels of communication and enforcement. Otherwise adoption of the policies will not be consistent throughout the organization and there would be too much variation from established security.
- Without top mgt buy-in, your security program will never get off the ground.
- Without leadership at the top, the effort is doomed to a dismal failure.
- Without the complete support of management, a security program is little more than a stick used to beat the more egregious violators of policy. Minor policy violations get ignored, leading to an overall attitude that security is not a concern of each employee
- Demonstrated support from top management creates a security-conscious culture and shows everyone security is important.
- If (management) don't support, encourage, and provide resources for a security program, the program won't have the ability to be effective nor well accepted by staff and other employees

Statements on User Training

- Mgmt can write and enforce policies but if mgmt doesn't communicate and train employees it is all for naught
- People need to be aware of today's environment and understand the consequences of their actions. Initial training and at least once a year compliance training is essential.
- Training and end user awareness allows for dissemination of information through training about best practices, and methodologies for doing things, as well as raising awareness among the end user population about potential threats.
- People are always the weakest link in Security. Most WANT to do a good job. If they understand WHY something is vulnerable they are more willing to mitigate those vulnerabilities.
- Because unless employees are involved and support the policies, policy enforcement can not be done effectively. This requires proper training and management support.
- Once people are aware of the issues, they willingly participate. It isn't lack of interest, but lack of knowledge that leads to apathy towards security.

Statements on Security Culture

- The executive drives the company culture and the resources allocated. This is the primary factor, followed by technical expertise of the people implementing security technologies
- Without a corporate culture solidly based on security, all the policies and procedures on the planet will not be effective at maintaining it.
- Security requires a holistic approach. Just like it's a process, not a product, an organization much make security and risk assessment part of the way that they do business, their operational culture, if they want to achieve any amount of success.
- Management direction will set the expectations of employees and form a security-aware organization culture
- Educate and communicate with the employee on the company's support of Information security…(w)ill build a company culture, support and awareness towards IT security.
- Without top down support for security the enterprise culture cannot reflect a security conscious business practice and security cannot gain a significant foothold in a business.
- The influence and guidance of management fosters a positive attitude of security.

Statements on Policy Relevance

- Buy-in must be secured both from upper management and the employees to ensure that policies are relevant, enforced and properly updated with an eye on the needs of the organization as a whole.
- Ignoring organizational goals, culture, and/or environment will result in policies that are costly, not followed, and seen as irrelevant.
- the most critical factor is management approval of the policy and regular update.
- Management must not only communicate the "contents" of the policy, but also the need for it. Management should reinforce the need and importance with consistent

enforcement as well as a clearly-defined process for updates and reviews.

- Collection of various metrics and then monitoring based on the data will help identifying the effective implementation of the policy. Also, the frequent review of the policy.
- We can develop the most detailed and strict security policy, mandate employees to follow them strictly but without audits and reviews, we may never know whether the policies and standards are being followed or effective.
- Because technology changes everyday, an outdated policy is ineffective
- Is the policy realistic and current? All actions depend on policy - when policy is inadequate all actions will fall short of the needed level of rigor.
- If it is not current it cannot be effective. Security must (be) reviewed periodically.

Statements on Policy Enforcement

- A policy or procedure is not valid, therefore not effective if not monitored for compliance and appropriate actions when not in compliance.
- Absent appropriate monitoring of policies and enforcement of sanctions, policies are little more than paper statements of intent.
- Without the enforcement you can not achieve any security in your organization. My organization has many good security policies and many good people but no one feel he has to apply any of them since no real care by our management.
- Without proper enforcement, employees may choose to regard information security as a 'nice to have'.
- Without support and enforcement by management, any policy, no matter how simple is doomed to fail.
- I have seen many good "paper" security plans but it is rare to see them enforced. Enforcement or acceptance among the employees is key to a successful security strategy.
- Without enforcement, any program will be useless document wasting rack/disk space.
- Security Awareness will eliminate assumptions and will reduce dramatically the number of security issues…Effective Security Monitoring will enforce the Security Control Policies.

Statements on Security Effectiveness

- The absence of a culture where security is consistently applied and where management lives by example, security will not be effective.
- Without upper management backing and support a security program will not be successful.
- Ultimately, the success of security lies in the individual. Technology can facilitate security. Only individuals can ensure security.
- The success of an infosec program is determined by the employees; they need to hear and learn what the infosec policies are so they can conform to them.
- Success flows down through the organization. Management can promote security programs with organizational support and budget.

- Without support and understanding of both management and employee and effective security program is impossible.
- Senior mgmt support & action is need for an effective security program and that will be driven by a clear & accurate understanding of the threats, risks & safeguards.

Statements on Interdependence and Cooperation

- Security is dependent upon cooperation of people. If people are not sold on the need, they will sabotage all good intentions.
- In order for our INFOSEC policy to be effective, it is necessary for all our units to cooperate, implement, and enforce the policy.
- We have developed very rigorous written security policies and procedures. We have also developed security awareness training program. Without active participation of all operating and supporting organizations these efforts will not be as effective as it (should).
- Everyone must cooperate, only one not trying is enough to reduce the program to non functional
- Without cooperation, Infosec policy and regulation are toothless.
- Continuous awareness is the root to better understanding and participation/cooperation.
- unable to enforce policies without…executive management's involvement,...understanding and cooperation

APPENDIX G

Standardized Residual Covariance Matrix from Alternate Model

From second-order factor mediation model:[24]

	EF1	EF2	EF3	EF4	EF5	TM6	TM5	TM4	TM3	TM2	TM1	PR5	PR4	PR2	PR1	SC6	SC5	SC4	SC3	SC1	UT6	UT5	UT4	UT2	UT1	PE4	PE3	PE2	PE1
EF1	0.00																												
EF2	0.54	0.00																											
EF3	0.14	-0.31	0.00																										
EF4	-0.35	-0.05	0.02	0.00																									
EF5	0.10	0.09	0.24	-0.07	0.00																								
TM6	1.35	1.81	1.13	1.88	1.45	0.00																							
TM5	-0.02	-0.03	-0.83	0.52	-0.55	0.02	0.00																						
TM4	0.10	-0.33	-0.56	0.49	0.18	0.28	0.16	0.00																					
TM3	0.00	-0.09	-0.45	0.38	-1.08	-0.68	-0.19	-0.39	0.00																				
TM2	0.34	0.05	-0.27	0.66	-1.86	-0.88	-0.32	0.38	0.90	0.00																			
TM1	-0.68	-0.66	-0.49	0.59	-1.27	-0.24	0.16	-0.45	0.67	0.68	0.00																		
PR5	0.21	0.48	-0.34	0.08	1.20	-0.17	-0.95	-0.57	-1.02	-2.04	-2.03	0.00																	
PR4	0.94	1.74	0.79	1.14	1.81	0.25	-0.60	-0.37	-0.69	-1.68	-0.64	-0.01	0.00																
PR2	1.70	2.88	2.15	2.64	1.87	1.24	1.24	1.31	0.44	0.75	0.13	-0.02	-0.45	0.00															

[24] In the symmetric matrix displayed here, each residual covariance has been divided by an estimate of its standard error (Gefen, 2003; Jöreskog & Sörbom, 1984). Covariance values greater than 2.58 are darkened. All three related to item PR2.

	EF1	EF2	EF3	EF4	EF5	TM6	TM5	TM4	TM3	TM2	TM1	PR5	PR4	PR2	PR1	SC6	SC5	SC4	SC3	SC1	UT6	UT5	UT4	UT2	UT1	PE4	PE3	PE2	PE1
PR1	0.70	0.17	-0.08	0.23	0.72	0.03	-0.90	-0.95	-0.84	-2.68	-1.79	0.09	0.07	-0.16	0.00														
SC6	-0.87	-0.90	0.43	0.44	-0.12	1.57	0.71	0.49	1.13	-0.05	0.98	-0.98	0.02	0.80	-0.60	0.00													
SC5	-0.77	-0.96	0.38	0.20	-0.36	1.57	0.55	1.04	0.80	0.58	-0.17	-1.62	-1.25	0.60	-1.72	0.05	0.00												
SC4	-0.44	-0.94	0.70	0.41	-0.29	0.82	0.20	0.62	0.57	0.01	0.91	-0.27	-0.66	1.07	-0.92	-0.37	0.01	0.00											
SC3	-1.69	-1.66	-0.70	-0.66	-1.77	1.08	0.08	0.41	1.53	0.10	1.51	-2.90	-1.97	-0.72	-2.29	0.50	0.31	-0.29	0.00										
SC1	-0.44	-0.78	-0.09	0.30	-0.41	1.36	0.11	0.50	0.59	0.21	0.56	-2.31	-1.95	0.38	-1.43	-0.36	-0.47	0.50	0.41	0.00									
UT6	0.08	-0.20	0.92	1.25	0.69	0.87	0.25	-0.45	0.09	-1.55	-0.84	0.53	1.45	1.94	0.75	0.86	1.11	1.12	0.14	1.84	0.00								
UT5	-0.16	-1.33	-1.29	0.18	-0.68	-0.26	-0.56	-0.88	-1.20	-1.97	-2.06	1.12	2.35	2.12	0.85	-0.39	-0.23	-0.60	-1.15	-0.70	-0.52	0.00							
UT4	-0.10	-0.89	-0.40	0.61	-0.66	0.40	-0.06	-0.32	-0.58	-1.80	-1.44	1.26	1.70	1.50	0.90	-0.16	0.39	0.76	-0.91	0.03	-0.06	0.50	0.00						
UT2	0.25	-0.38	0.56	0.83	-0.03	0.79	-0.25	-0.50	-0.69	-1.45	-1.70	0.96	1.42	1.75	0.32	0.11	0.32	0.50	-0.42	0.96	0.15	-0.02	-0.22	0.00					
UT1	0.36	-0.24	0.40	1.40	0.58	-0.23	-0.56	-1.20	-0.63	-1.87	-2.14	1.31	1.70	3.38	1.44	0.06	-0.13	0.84	-1.18	0.22	-0.18	-0.21	-0.14	0.42	0.00				
PE4	-0.53	-0.61	-1.02	-0.50	-0.85	0.70	-1.06	-0.77	-1.12	-1.10	-1.00	0.05	0.69	1.96	0.73	0.31	-0.51	-0.67	-1.55	0.02	0.28	-0.56	-0.20	-0.88	0.28	0.00			
PE3	-0.07	-0.02	-0.11	0.30	-0.26	1.42	0.00	-0.11	0.30	-0.20	0.59	0.00	1.11	1.64	0.37	0.13	-0.84	-0.09	-0.30	0.71	0.69	-1.48	-1.02	-0.70	0.77	0.06	0.00		
PE2	0.37	-0.79	-0.62	0.24	-0.24	1.91	0.21	0.04	1.03	-0.13	0.23	-0.07	1.14	1.98	1.00	0.45	0.40	0.12	0.17	0.91	1.73	0.41	0.57	0.03	0.66	0.47	-0.30	0.00	
PE1	-0.33	0.03	-0.25	0.37	-0.29	1.10	-0.49	-0.57	0.37	-0.88	-0.08	0.04	0.74	2.20	0.73	0.19	-0.24	0.04	-0.81	1.04	1.16	-0.90	-0.38	-0.27	0.47	-0.14	0.19	-0.15	0.00

APPENDIX H

Covariance Matrix of Second Order Factor Model - Part 1

	EF1	EF2	EF3	EF4	EF5	TM6	TM5	TM4	TM3	TM2	TM1	PR5	PR4	PR2	PR1	SC6	SC5	SC4	SC3	SC1	UT6	UT5	UT4	UT2	UT1	PE4	PE3	PE2	PE1
EF1	0.79																												
EF2	0.57	0.82																											
EF3	0.52	0.53	0.85																										
EF4	0.59	0.60	0.54	0.78																									
EF5	0.57	0.57	0.52	0.59	0.94																								
TM6	0.46	0.46	0.42	0.48	0.46	1.08																							
TM5	0.51	0.52	0.47	0.53	0.51	0.82	1.16																						
TM4	0.51	0.51	0.46	0.53	0.50	0.81	0.90	1.15																					
TM3	0.46	0.46	0.42	0.48	0.46	0.73	0.81	0.80	1.18																				
TM2	0.43	0.44	0.40	0.45	0.43	0.69	0.77	0.76	0.69	1.04																			
TM1	0.46	0.46	0.42	0.48	0.46	0.74	0.82	0.81	0.73	0.70	1.03																		
PR5	0.38	0.38	0.34	0.39	0.37	0.43	0.48	0.47	0.43	0.40	0.43	0.99																	
PR4	0.35	0.35	0.32	0.36	0.35	0.40	0.44	0.44	0.40	0.38	0.40	0.74	1.07																
PR2	0.27	0.27	0.25	0.28	0.27	0.31	0.35	0.34	0.31	0.29	0.31	0.58	0.54	0.79															
PR1	0.37	0.38	0.34	0.39	0.37	0.43	0.48	0.47	0.43	0.40	0.43	0.79	0.74	0.58	0.97														
SC6	0.51	0.52	0.47	0.53	0.51	0.58	0.65	0.64	0.58	0.55	0.59	0.48	0.44	0.35	0.48	1.15													
SC5	0.54	0.54	0.50	0.56	0.54	0.62	0.69	0.68	0.61	0.58	0.62	0.50	0.47	0.37	0.50	0.86	1.26												

	EF1	EF2	EF3	EF4	EF5	TM6	TM5	TM4	TM3	TM2	TM1	PR5	PR4	PR2	PR1	SC6	SC5	SC4	SC3	SC1	UT6	UT5	UT4	UT2	UT1	PE4	PE3	PE2	PE1
SC4	0.46	0.46	0.42	0.48	0.46	0.52	0.58	0.57	0.52	0.49	0.52	0.43	0.40	0.31	0.43	0.73	0.76	0.94											
SC3	0.52	0.53	0.48	0.54	0.52	0.59	0.66	0.66	0.59	0.56	0.60	0.49	0.45	0.35	0.49	0.83	0.87	0.74	1.44										
SC1	0.42	0.42	0.38	0.44	0.42	0.48	0.53	0.52	0.47	0.45	0.48	0.39	0.36	0.28	0.39	0.66	0.70	0.59	0.68	0.95									
UT6	0.46	0.47	0.43	0.48	0.46	0.53	0.59	0.58	0.53	0.50	0.53	0.43	0.40	0.31	0.43	0.59	0.62	0.53	0.60	0.48	1.11								
UT5	0.53	0.53	0.48	0.55	0.52	0.60	0.67	0.66	0.60	0.57	0.60	0.49	0.45	0.36	0.49	0.67	0.71	0.60	0.68	0.54	0.83	1.30							
UT4	0.55	0.55	0.51	0.57	0.55	0.63	0.70	0.69	0.63	0.59	0.63	0.51	0.48	0.37	0.51	0.70	0.74	0.63	0.72	0.57	0.87	0.98	1.21						
UT2	0.50	0.51	0.46	0.52	0.50	0.57	0.64	0.63	0.57	0.54	0.58	0.47	0.43	0.34	0.47	0.64	0.67	0.57	0.65	0.52	0.79	0.90	0.94	1.11					
UT1	0.47	0.47	0.43	0.49	0.47	0.54	0.60	0.59	0.53	0.51	0.54	0.44	0.41	0.32	0.44	0.60	0.63	0.53	0.61	0.49	0.74	0.84	0.88	0.80	1.13				
PE4	0.35	0.36	0.32	0.37	0.35	0.40	0.45	0.44	0.40	0.38	0.41	0.33	0.31	0.24	0.33	0.45	0.47	0.40	0.46	0.37	0.41	0.46	0.48	0.44	0.41	1.17			
PE3	0.39	0.40	0.36	0.41	0.39	0.45	0.50	0.49	0.45	0.42	0.45	0.37	0.34	0.27	0.37	0.50	0.53	0.45	0.51	0.41	0.45	0.51	0.54	0.49	0.46	0.67	1.08		
PE2	0.33	0.33	0.30	0.34	0.33	0.37	0.42	0.41	0.37	0.35	0.38	0.31	0.28	0.22	0.31	0.42	0.44	0.37	0.43	0.34	0.38	0.43	0.45	0.41	0.38	0.56	0.62	0.85	
PE1	0.37	0.37	0.34	0.38	0.37	0.42	0.47	0.46	0.42	0.40	0.42	0.34	0.32	0.25	0.34	0.47	0.50	0.42	0.48	0.38	0.43	0.48	0.51	0.46	0.43	0.63	0.70	0.58	0.91

Covariance Matrix of Second Order Factor Model - Part 2

	TM[25]	MP	EF	PR	SC	UT	PE
TMS	0.74						
MP	0.43	0.35					
EF	0.46	0.38	0.58				
PR	0.43	0.35	0.38	0.79			
SC	0.59	0.48	0.52	0.48	0.82		
UT	0.63	0.51	0.55	0.51	0.70	1.03	
PE	0.42	0.34	0.37	0.34	0.47	0.51	0.66
EF1	0.46	0.38	0.57	0.38	0.51	0.55	0.37
EF2	0.46	0.38	0.58	0.38	0.52	0.55	0.37
EF3	0.42	0.34	0.53	0.34	0.47	0.51	0.34
EF4	0.48	0.39	0.60	0.39	0.53	0.57	0.38
EF5	0.46	0.37	0.57	0.37	0.51	0.55	0.37
TM6	0.74	0.43	0.46	0.43	0.58	0.63	0.42
TM5	0.82	0.48	0.52	0.48	0.65	0.70	0.47
TM4	0.81	0.47	0.51	0.47	0.64	0.69	0.46
TM3	0.73	0.43	0.46	0.43	0.58	0.63	0.42
TM2	0.70	0.40	0.44	0.40	0.55	0.59	0.40
TM1	0.74	0.43	0.46	0.43	0.59	0.63	0.42
PR5	0.43	0.35	0.38	0.79	0.48	0.51	0.34
PR4	0.40	0.32	0.35	0.74	0.44	0.48	0.32
PR2	0.31	0.25	0.27	0.58	0.35	0.37	0.25
PR1	0.43	0.35	0.38	0.79	0.48	0.51	0.34
SC6	0.59	0.48	0.52	0.48	0.82	0.70	0.47
SC5	0.62	0.50	0.54	0.50	0.86	0.74	0.50
SC4	0.52	0.43	0.46	0.43	0.73	0.63	0.42
SC3	0.60	0.49	0.53	0.49	0.83	0.72	0.48
SC1	0.48	0.39	0.42	0.39	0.66	0.57	0.38
UT6	0.53	0.43	0.47	0.43	0.59	0.87	0.43
UT5	0.60	0.49	0.53	0.49	0.67	0.98	0.48
UT4	0.63	0.51	0.55	0.51	0.70	1.03	0.51
UT2	0.58	0.47	0.51	0.47	0.64	0.94	0.46
UT1	0.54	0.44	0.47	0.44	0.60	0.88	0.43
PE4	0.41	0.33	0.36	0.33	0.45	0.48	0.63
PE3	0.45	0.37	0.40	0.37	0.50	0.54	0.70
PE2	0.38	0.31	0.33	0.31	0.42	0.45	0.58
PE1	0.42	0.34	0.37	0.34	0.47	0.51	0.66

[25] TM: top management support, MP: managerial practice; EF: perceived effectiveness; PR: policy relevance; SC: security culture; UT: user training; PE: policy enforcement