

THE INSIDER THREAT TO ORGANIZATIONAL INFORMATION
SECURITY: A STRUCTURAL MODEL AND 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.

Todd Michael Dugo

Certificate of Approval:

Thomas E. Marshall
Associate Professor
Management

R. Kelly Rainer, Jr., Chair
George Phillips Privett Professor
Management

F. Nelson Ford
Associate Professor
Management

George T. Flowers
Interim Dean
Graduate School

THE INSIDER THREAT TO ORGANIZATIONAL INFORMATION
SECURITY: A STRUCTURAL MODEL AND EMPIRICAL TEST

Todd Michael Dugo

A Dissertation

Submitted to

the Graduate Faculty of

Auburn University

in Partial Fulfillment of the

Requirements for the

Degree of

Doctor of Philosophy

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

Auburn, Alabama
December 17, 2007

THE INSIDER THREAT TO ORGANIZATIONAL INFORMATION
SECURITY: A STRUCTURAL MODEL AND EMPIRICAL TEST

Todd Michael Dugo

Permission is granted to Auburn University to make copies of this dissertation at its discretion, upon request of individuals or institutions and at their expense. The author reserves all publication rights.

Signature of Author

Date of Graduation

DISSERTATION ABSTRACT
THE INSIDER THREAT TO ORGANIZATIONAL INFORMATION
SECURITY: A STRUCTURAL MODEL AND EMPIRICAL TEST

Todd Michael Dugo

Doctor of Philosophy, December 17, 2007
(M.S., University of Southern California, 1989)
(B.S., University of Maryland, 1996)
(B.S., Pennsylvania State University, 1984)

109 Typed Pages

Directed by R. Kelly Rainer, Jr.

The organizational insider, through his or her intentional violation of organizational security policy, arguably represents one of the greatest threats to organizational information security. Drawing from the Theory of Planned Behavior, General Deterrence Theory, and the organizational behavior concepts of organizational commitment and organizational (security) culture, this study develops a research model to predict an individual's intention to violate an organization's security policy. A test of the model was conducted using data obtained from a convenience sample of government employees. This research found evidence that deterrent factors such as perceived punishment certainty and perceived punishment factors, when placed in the framework of The Theory of Planned Behavior, are useful for predicting an individual's intention to violate his/her organization's information security policy.

Style manual used: Publication Manual of the American Psychological Association, Fifth Edition.

Computer software used: Microsoft Word 2002, Microsoft Excel 2002, SPSS 14.0, PLS-Graph 3.0

TABLE OF CONTENTS

LIST OF TABLES	ix
LIST OF FIGURES	x
INTRODUCTION	1
Purpose of the study and research questions	2
LITERATURE REVIEW	4
Defining Information Security and the Insider Threat.....	4
The Organizational Security Policy	6
Theoretical Framing.....	8
Key Insights from the Existing Literature	10
Research Model Derivation	14
Primary Dependent Variables	16
The Theory of Planned Behavior	17
General Deterrence Theory.....	20
Organizational Commitment.....	22
Organizational Security Culture	28
The Study's Major Assumption.....	33
METHODOLOGY	34

Participants.....	34
Data Collection Procedures	35
Measures	40
Security policy knowledge assessment.....	40
Punishment severity, punishment certainty, attitude, subjective norm, perceived behavioral control and violation intention	41
Security culture	41
Organizational commitment	41
Social desirability	42
Statistical Power	43
RESULTS	47
Demographics and Description of the Sample	47
Research Model Assessment	50
Measurement Model Assessment	51
PLS Factorial Validity	51
Assessment of Discriminant Validity	54
Reliability.....	58
Structural Model Assessment	59
Social Desirability Bias Assessment.....	60
DISCUSSION	63
Findings and Conclusions.....	63
Implications for Managers	70

Implications for Researchers	73
Limitations of the Study	74
REFERENCES	76
APPENDICES	87
Appendix A – Security Policy (Acceptable Use)	88
Appendix B – Security Policy (Acceptable Use) Example	92
Appendix C – Participant Information Letter	97
Appendix D – Measures	98

LIST OF TABLES

Table 1 - Summary of Criminology Theories & Key IS Related Studies	9
Table 2 - Table of Key Definitions & Terms.....	15
Table 3 - Summary of Research Hypotheses	32
Table 4 - Required Sample Size Analysis.....	45
Table 5 - Sample Demographics (N=113).....	49
Table 6 -Descriptive Statistics (N=113)	50
Table 7 - PLS-Graph Outer Model Loadings (using Bootstrap with 200 resamples)	53
Table 8 - Discriminant Analysis Procedure 1 (item loadings and cross-loadings).....	55
Table 9 -Discriminant Analysis Procedure 2 -- AVE Analysis (SQRT AVE on the diagonals).....	57
Table 10 – Results of PLS Confirmatory Factor Analysis	58
Table 11- Tests of hypotheses results	60
Table 12 - ΔR^2 analysis when adding social desirability as a control variable.....	62

LIST OF FIGURES

Figure 1 - Loch & Cogner's Proposed Model of Ethical Decision Making and Computer Use Based on a Modified Version of the Theory of Reasoned Action (Loch & Cogner, 1996, p. 76)	10
Figure 2 - Software Piracy Model (Peace, et al., 2003, p. 162).....	11
Figure 3 - Proposed Holistic Model of Computer Abuse (Lee & Lee, 2002, p. 61)	12
Figure 4 - Security Impact Model (Straub, 1990, p.259).....	13
Figure 5 - Research Model.....	14
Figure 6 - The Theory of Planned Behavior (Ajzen, 1991, p. 182).....	19
Figure 7 - Results of PLS Structural Model Analysis	59

INTRODUCTION

Organizations and their critical operations are becoming more reliant on computer systems and the Internet, which has increased the focus on information security (INFOSEC) to prevent problems which could lead to competitive disadvantage (Kankanhalli, Teo, Tan, & Wei, 2003). In a 2006 nationwide survey of security executives and law enforcement personnel concerning electronic crime (e-crime), out of 434 respondents, 63% reported operational losses, 40% reported financial losses averaging \$740,000, and 40% reported harm to their organization's reputation due to e-crime. (CSO Magazine/U.S. Secret Service/Computer Emergency Response Team [CERT] Coordination Center, Microsoft Corp., 2006). In the same survey, 58% of the security events were committed by outsiders and 27% by insiders. More than 55% of the respondents reported at least one insider event, a 39% increase over the previous year. In another 2004 global INFOSEC survey, the respondents, consisting of chief information officers and chief information security officers, identified "lack of security awareness by users" as the top obstacle to effective information security. However, only 28% of the same respondents listed "raising employee information security training or awareness" as a high priority for 2004 (Ernst & Young, 2004). This fact is disturbing as spending on security products is expected to surpass \$118 billion by 2007 (Messmer, 2003), yet possibly the weakest link in the security chain, and one of the chronic reasons for security system failures, involves people and not the systems themselves (Schneier, 2000).

The implications of poor INFOSEC are becoming more clear. Recent legislation such as the Sarbanes-Oxley Act of 2002, Gramm-Leach-Bliley Act of 1999, and the Health Insurance Portability and Accountability Act (HIPAA) of 1995 each contain provisions for criminal and civil penalties for companies failing to provide the same “due diligence” in securing certain types of information as they do in protecting their other assets (Bisson & Saint-Germain, n.d.). Security was also shown as a factor in consumer attitudes towards e-shopping (Liao & Cheung, 2001), e-banking (Liao & Cheung, 2002), and in the development of customer trust in online companies (Balasubramanian, Konana, & Menon, 2003; Koufaris & Hampton-Sosa, 2004). The potential impact of loss of customer trust due to a company’s security problems and/or failures could spell disaster for many companies in terms of competitive advantage or survival.

This study examines the threat posed by individuals internal to or “inside” the organization, and specifically refers to these “insider” individuals as current or former employees or contractors of an organization. The “insider” represents a major threat to INFOSEC because they are already within the security perimeter of the organization and operate within its protected boundaries (Parker, 1998) and by virtue of their having knowledge of, or access to, employee information systems and assets (U.S. Secret Service & CERT Coordination Center, 2005). Clearly, the potential threat to organizational INFOSEC posed by individuals of the organization is real and represents a major threat to the information security of organizations.

PURPOSE OF THE STUDY AND RESEARCH QUESTIONS

The purpose of this study is to investigate factors relating to the “insider” threat to organizational INFOSEC. The primary research question of this study is as follows:

What are significant predictors of intentional violations of organizational INFOSEC policy committed by organizational insiders (i.e., current employees or contractors of an organization)?

The specific research questions for this study are as follows:

RQ1. Does organizational security culture affect the insider threat to organizational security?

RQ2. Does organizational commitment affect the insider threat to organizational security?

RQ3. Does the perceived severity of punishment affect the insider threat to organizational security?

RQ4. Does the perceived certainty of punishment affect the insider threat to organizational security?

Chapter 2 of this study defines INFOSEC and the insider threat, and reviews several theories and models used in prior insider threat research. Additionally, the chapter reviews the relevant organizational commitment and culture literature and presents the study's research model and hypotheses. Chapter 3 outlines the methodology for conducting the study to include the sample population, instrument development, data collection, and data analysis. Chapter 4 presents the findings of this study. Chapter 5 provides an interpretation of the results and the conclusions drawn from the dissertation. Chapter 5 also discusses the study's limitations, and the theoretical and practical implications for researchers and managers.

LITERATURE REVIEW

This chapter reviews the relevant literature for the development of the study's research model. The research model serves as the foundation for this study.

DEFINING INFORMATION SECURITY AND THE INSIDER THREAT

In order to develop the research model for this study, it is essential to first establish definitions for INFOSEC and the insider threat. The literature has defined INFOSEC in various ways. The Alliance for Telecommunications Industry Solutions Telecom Glossary (an ANSI National Standard and an update to Federal Standard 1037C) defines information security as “the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional” (ATIS telecom glossary, 2000). The U.S. Department of Defense defines INFOSEC as “the system of policies, procedures, and requirements established under the authority of Executive Order 12958 [Classified National Security Information] to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security” (DoD 5200.1-R, 1997, p. 133).

Chief Security Officer Magazine defines information security as:

The process of protecting data from accidental or intentional misuse by persons inside or outside of an organization. Although information security is by no means strictly a technical problem, its technical aspects (firewalls, encryption and the like) are important. Information security is an increasingly high-profile

problem, as hackers take advantage of the fact that more organizations are opening parts of their systems to employees, customers and other businesses via the Internet (CSO Magazine Online Glossary).

In this study, it is also important to delineate the scope of INFOSEC in relation to other similar concepts such as information assurance and defensive information warfare. Like defensive information warfare, both INFOSEC and information assurance address intentional threats. However, unlike information assurance and defensive information warfare, INFOSEC does not address intentional threats related to perception management such as bad publicity, propaganda, or exploitation of public media. Unlike defensive information warfare, INFOSEC and information assurance address unintentional threats such as errors attributed to hardware, software, and humans, as well as accidents and natural disasters (Denning, 1999). Denning also explains how INFOSEC has often been decomposed into the “CIA” model of INFOSEC whose components are confidentiality, integrity, and availability. This study uses the scope of INFOSEC identified by Denning (1999) in that we do not address the threats related to perception management.

The study also uses the CIA model of INFOSEC, and defines INFOSEC as *the organizational processes, policies, procedures, and systems implemented by an organization in an attempt to prevent the unauthorized intentional or unintentional reduction of the confidentiality, integrity, and availability of proprietary or sensitive organizational information (whether in storage, processing, or transit).*

The United States Secret Service and the CERT have defined the term “insider” as “individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm.” (U.S. Secret Service & CERT

Coordination Center, 2005, p.3). According to Theoharidu, Kokolakis, Karyada, and Kiontouzis (2005, p. 473): “the term insider threat refers to threats originating from people who have been given access rights to an IS [information system] and misuse their privileges, thus violating the IS security policy of the organization.” Based on these prior definitions, it is our view that the insider threat refers to intentional violations, but not unintentional violations, of organizational security policy.

This study adopts the definition of the insider threat, as published by Theohardu, et al., (2005), in the preceding paragraph. For the purposes of this study, the definition indicates that the organizational security policy (to include information system security policy and other related security policies) delineates how individuals within the organization use, protect, and control organizational information and the systems used to process it, and any intentional deviation from the policy is considered an INFOSEC violation. Although unintentional violations of the organizational security policy can pose a significant threat to organizational security (Mitnick & Simon, 2002), this study specifically focuses on intentional violations as per the definition of the insider threat.

THE ORGANIZATIONAL SECURITY POLICY

The purpose of an organization’s security policy is to communicate management’s direction and support for INFOSEC and is a document commonly used by management to dictate appropriate behavior of employees and various other related parties (e.g., contractors) (von Solmes & von Solmes, 2004). Security experts consider security policies to be essential for any organization (Mitnick & Simon, 2002; Schneier, 2000; Guel, 2001).

The security policy framework as stated by Guel (2001, p. 2) is as follows:

1. Policies define appropriate behavior.
2. Policies set the stage in terms of what tools and procedures are needed.
3. Policies communicate a consensus.
4. Policies provide a foundation for HR [human relations] action in response to inappropriate behavior.
5. Policies may help prosecute cases.

An organization's security policy often refers to a collection of policies related to the protection of an organization's information and supporting information systems, to include the Acceptable Use Policy, Remote Access Policy, Wireless Communication Policy, and others (SANS, 2006). Specifically, the Acceptable Use Policy "defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information" (SANS, 2006). A document that identifies common prohibited behaviors that are included in an acceptable use policy is located at Appendix A. Managers can use this document as a template for developing their organization's acceptable use policy.

Individuals can violate the security policy either intentionally or unintentionally. To prevent violations of security, organizations often use security awareness training to educate employees about the security policy and other security related matters (Mitnick & Simon, 2002; SANS 2006;). Organizations can also require that individuals acknowledge the existence of the security policy by signing a company document. The employer then retains the signed document in the employee's personnel file for future reference should the employer discover that the employee has committed a policy

violation. Therefore, an employee cannot later say that he/she was never made aware of the security rules. This practice is clearly consistent with the security policy framework previously described. A publicly available document of this type is located in Appendix B.

THEORETICAL FRAMING

Researchers have employed various criminology and behavioral theories in examining the insider threat to organizational information systems to include General Deterrence Theory (GDT), Social Control Theory (SCT), Social Learning Theory, Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB) and Situational Crime Prevention (SCP) (see Theoharidu et al., 2005) and the Theory of Reasoned Action (TRA) (see Loch & Cogner, 1996). The next section addresses several of these theories in the derivation of the research model. For further discussions of GDT, SCT, SLT, TBP, and SCP and their use in prior IS research, we refer the reader to reviews by Lee & Lee (2002) and Theoharidu et al., (2005). Table 1 provides a brief summary of the theories and key IS related studies referred to in subsequent sections of this chapter. According to the review by Theoharidu et al., GDT, SCT, SLT and TBP mainly focus on individuals' motivation, while SCP focuses on the opportunity to perform a particular behavior. Of key note is that many of the concepts contained in these theories have some degree of overlap. This overlap helps explain why researchers have theorized or tested several "hybrid" research models based on concepts drawn from the various theories. In the next section, this study examines the literature that has influenced the development of this study's research model.

Table 1 - Summary of Criminology Theories & Key IS Related Studies

Theory	Key IS Related Studies
<p>General Deterrence Theory (GDT) Humans are rational actors and that punishments serve as “tangible motives” to deter criminal behavior (Becarria, 1995)</p> <p>Incentives can influence human behavior and predicts that increases in the severity of punishment or the certainty of punishment imposition on those detected, will reduce some criminal acts (Blumstein et al., 1978)</p>	<p>Straub, 1990 Straub & Nance, 1990 Straub & Welk, 1998 Kankanhalli, et al., 2003</p>
<p>Social Control Theory (SCT) (a.k.a. Social Bond Theory) Delinquency results when an individual’s bond to society is weak or broken; the elements that bond an individual to society are <i>attachment, commitment, involvement, and belief</i>. (Hirschi, 1969)</p>	<p>Lee, et al., 2004</p>
<p>Social Learning Theory (SLT) Social behavior is learned by conditioning and is shaped from consequences that follow from the behavior, and by imitation of others’ behavior. Variables include: <i>differential association, differential reinforcement and punishment, definitions, and sources of imitation</i>. (Akers, 1985)</p>	<p>Hollinger, 1993 Skinner & Fream, 1997</p>
<p>Theory of Reasoned Action (TRA) Intentions are the antecedent to behavior and are a function of <i>attitude</i> and <i>social norms</i> and that intention mediates an individual’s attitude and social norms towards committing or not committing the referent behavior (Ajzen & Fishbein, 1980)</p>	<p>Loch & Cogner, 1996</p>
<p>Theory of Planned Behavior (TPB) An extension of the TRA. Adds <i>perceived behavioral control</i> as a predictor of intention (Ajzen, 1991)</p>	<p>Siponen, 2000* Lee & Lee, 2002* Peace, et al., 2003</p>

*non-empirical

KEY INSIGHTS FROM THE EXISTING LITERATURE

A synthesis of the relevant literature reveals that past empirical and conceptual studies attempted, with mixed results, to explain both *why* individuals commit certain behaviors that pose a threat to organizational IS, and *how* organizations counter the threats posed by those individuals. In the remainder of this section, this study reviews several key conceptual and empirical studies that influenced the derivation of the research model.

In examining why insiders commit certain behaviors that threaten organizational information, Loch & Cogner (1996) empirically examined ethical decision making and computer use based on a modified TRA model (see Figure 1). Loch & Cogner (1996)

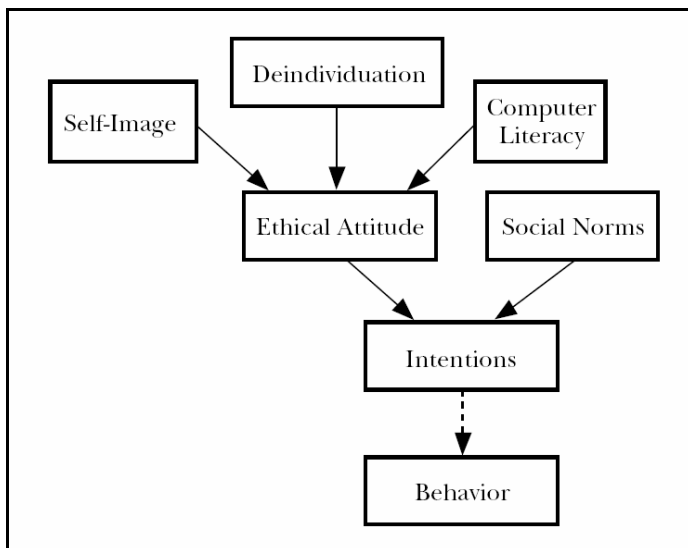


Figure 1 - Loch & Cogner's Proposed Model of Ethical Decision Making and Computer Use Based on a Modified Version of the Theory of Reasoned Action (Loch & Cogner, 1996, p. 76)

found mixed results for predicting the intentions of men and women toward specific types of unethical computer behavior such as stealing technical application documentation, running a program at work for a friend, and reading others' email.

In 1997, Skinner and Fream extended the early work on correlates to computer crime (Hollinger, 1993) and investigated if elements of SLT (i.e., differential association, differential reinforcement and punishment, definitions, and sources of imitation) (Akers, 1985) related to various illegal computer acts committed by college students. Skinner and Fream found general support for these elements and concluded that the SLT was useful in explaining computer crime. However, they noted that their results differed from those of Hollinger in that the certainty of apprehension and the severity of punishment were not useful for deterring software piracy.

In 2003, Peace, Galletta, and Thong used a research model primarily based on the TPB and GDT (punishment severity and punishment certainty) to investigate intention to commit software piracy in the workplace (see Figure 2) and found support for their overall model.

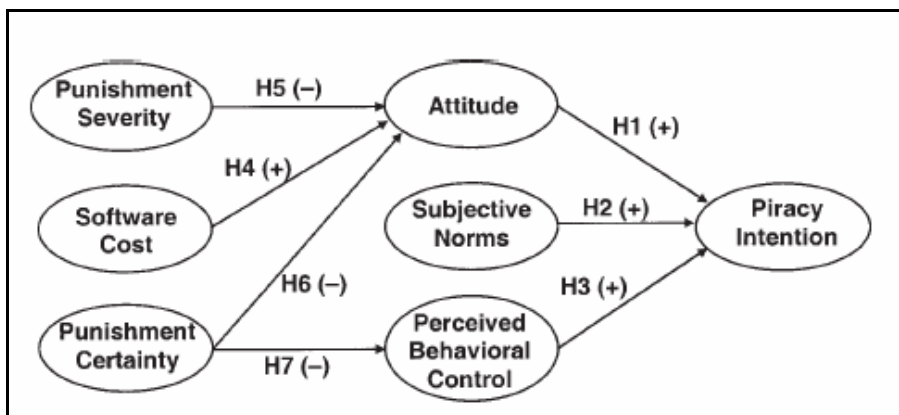


Figure 2 - Software Piracy Model (Peace, et al., 2003, p. 162)

Lee & Lee (2002) used the TPB as a base model and incorporated various individual and organization elements based on the GDT, SCT, and SLC to theorize a holistic model of organizational computer abuse (see Figure 3). Straub & Nance (1990) defined computer abuse as “unauthorized, deliberate, and internally recognizable misuse of assets of the

local organizational information system by individuals” (p. 48). Later, Lee, Lee and Yoo (2004) empirically tested a similar model of integrated computer abuse based on SCT and GDT, but found that hypotheses involving security policy, security awareness, attachment, and commitment toward self defense intention (against abuse by invaders) and induction control intention (abuse by insiders) were not supported.

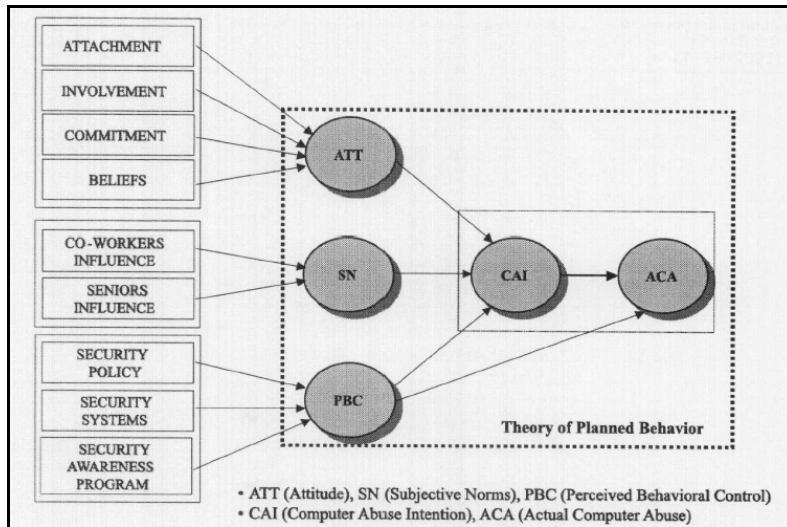


Figure 3 - Proposed Holistic Model of Computer Abuse (Lee & Lee, 2002, p. 61)

To counter the threat posed to information by insiders, organizations have turned to various methods to deter and prevent intentional or accidental insider misuse of information and systems. These methods have been found effective (Straub & Nance, 1990). According to Straub & Nance, deterrent methods include passive or administrative controls such as security awareness training or security policy statements that specify conditions for proper IS usage. Preventive methods are controls such as password protected login screens or physical locks on computer equipment doors or locks on data files (see also Straub & Welk, 1998).

Although some of the previous studies investigate some aspects of deterring computer abuse or crimes under GDT (i.e., punishment severity and punishment certainty) with mixed results, additional studies also focused on GDT for deterring computer abuse. In 1990, Straub tested a Security Impact model of computer abuse (see Figure 4) and found that deterrent severity and deterrent certainty were useful for preventing organizational computer abuse. In contrast, a more recent study found that although

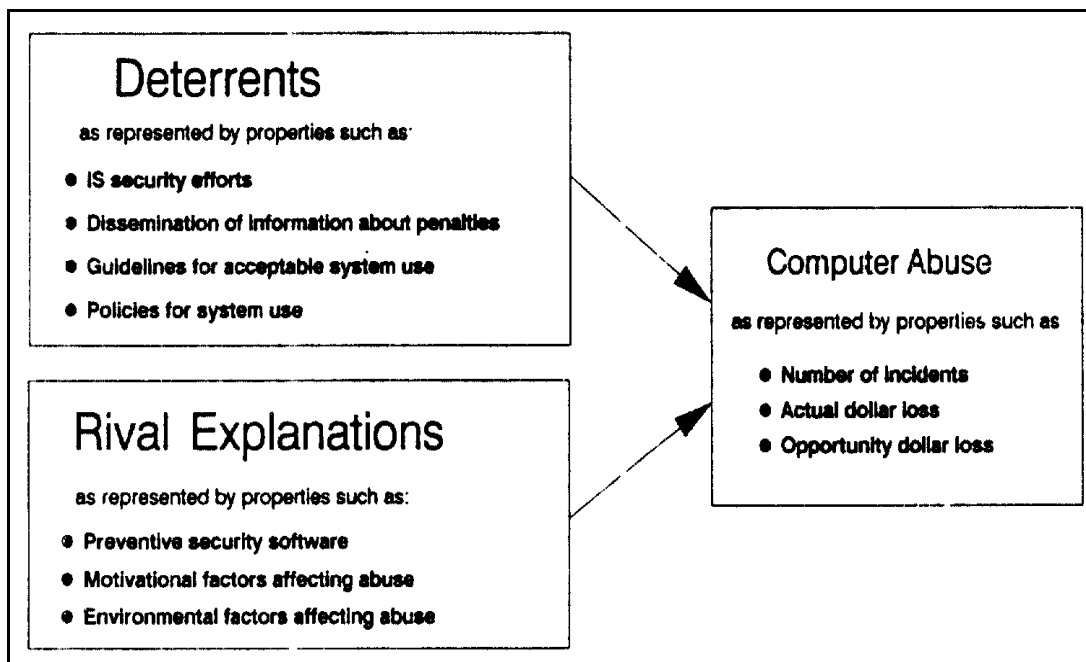


Figure 4 - Security Impact Model (Straub, 1990, p.259)

deterrent and preventive efforts contributed to effective IS security, deterrent severity (the form of punishment imposed on abusers) did not (Kankanhalli, Teo, Tan & Wei, 2003).

In summary, based on the review of the literature, a variety of researchers have examined the insider threat to organizational security by drawing on various elements of criminology and behavioral theories. Unfortunately, the results of these prior studies are mixed and in some instances contradictory. These results warrant further investigation to

gain additional understanding of the various individual and organizational factors contributing to the internal threat faced by today's organizations. The next section more closely reviews several of the theories previously discussed and draws from them and other concepts to derive the research model of the insider threat to organizational INFOSEC.

RESEARCH MODEL DERIVATION

This study's unit of analysis is the individual. We examine various individual and organizational factors that could theoretically influence individual behavior or actions that could in turn affect organizational INFOSEC. We begin by identifying the primary dependent variables in the model and then turn to the theory of planned behavior to serve as a base for the model. We then systematically examine other theories and related concepts to arrive at the overall model (see Figure 5). Table 2 provides a summary of the definitions of the constructs used in our model and other terms used in this study, and Table 3 provides a summary of the research hypotheses.

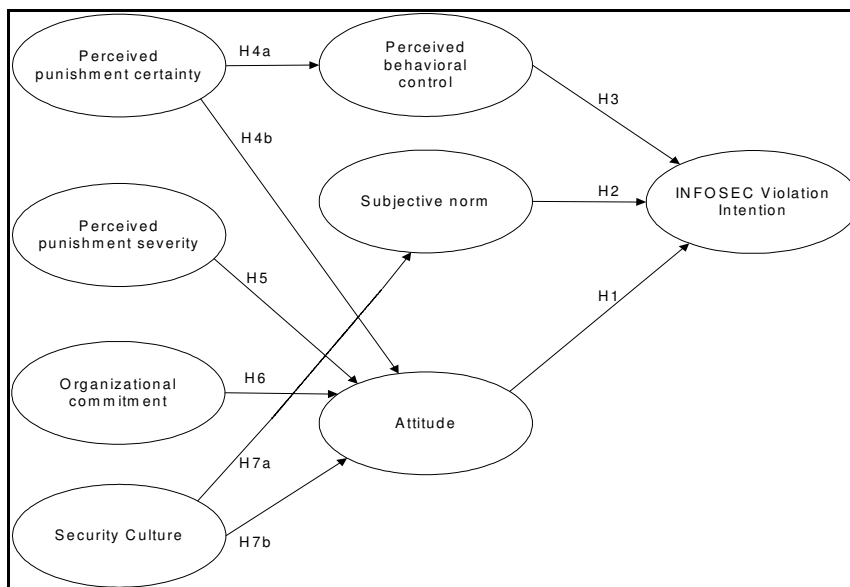


Figure 5 - Research Model

Table 2 - Table of Key Definitions & Terms

Construct/Term	Definition
Attitude	A personal judgment that the behavior is good or bad and is a function of beliefs (see Ajzen & Fishbein, 1980).
INFOSEC	Information security. The organizational processes, policies, procedures, and systems enacted or implemented by an organization in an attempt to protect proprietary or sensitive information (whether in storage, processing, or transit) from unintentional or intentional misuse by persons inside or outside of an organization (definition used in this study).
INFOSEC Violation Intention	An individual's level of intention to violate the organization's INFOSEC or related security policy; the individual is either a current or a previous member of the organization (i.e., the insider) (definition used in this study).
Insider threat	The threat to organizational information posed by individuals who currently have or previously had authorized access to sensitive or proprietary organizational information and have the potential to intentionally violate the INFOSEC policy or rules of the organization (definition used in this study). See also Theoharidu et al., (2005).
Intention	The antecedent of behavior; in the Theory of Planned Behavior is a function of attitude, subjective norm, and perceived behavioral control (see Ajzen and Fishbein 1980; Ajzen, 1991).
Intentional INFOSEC violation	An action taken by an individual who knew that the action was a violation of the organization's INFOSEC policy or rules in advance of actually committing the act (definition used in this study).
Organizational commitment	"The relative strength of an individual's identification with and involvement in an organization" and is characterized by three factors regarding an individual: 1) belief in and the acceptance of the organizations goals and values, 2) willingness to exert considerable effort for the organization, and 3) a strong desire to remain a member of the organization" (Steers, 1977).
Perceived behavioral control	An individual's perception of the ease or difficulty of performing the referent behavior (see Ajzen, 1991).
Perceived punishment certainty	An individual's perception that the organization will detect and punish him/her for violating organizational security policy (definition used in this study).
Perceived punishment severity	An individual's perception of the severity of the punishment for violating organizational security policy. (definition used in this study).
Preventive security controls	Countermeasures such as equipment door locks or system passwords. (See Nance & Straub, 1990; Straub & Welk, 1998)
Security Culture	A set of INFOSEC related beliefs values, understandings, and norms shared by members of an organization. (definition used in this study). See also Knapp (2005).

Subjective norm	A person's perception of social pressures to perform or not perform the behavior. (see Ajzen & Fishbein, 1980)
-----------------	--

PRIMARY DEPENDENT VARIABLES

The primary dependent variable in the model is *INFOSEC violation intention*.

We define this construct as an individual's level of intention to violate the organization's INFOSEC or related security policy. The individual is either a current or a previous member of the organization (i.e., the insider). An intentional INFOSEC violation is an action that an individual knows is a violation of the organization's INFOSEC policy or rules in advance of actually committing the act. In other words, the individual must form the intention to knowingly violate organizational policy prior to actually committing the act, which causes the violation. An example of an intentional violation might be the unauthorized installation of a modem to an office computer by an individual to circumvent network firewall or proxy server restrictions. In this case, the individual knows that such an installation violates the security policy but, for whatever reason, goes ahead and installs the equipment anyway.

In contrast, an unintentional violation is any action taken by an individual, which in turn unintentionally causes a security violation. In this instance, there is no formation of intention on the part of the individual to cause a security violation, thus the violation is unintentional. An example of an unintentional violation might be an individual forgetting to backup or encrypt a critical or sensitive data file. An unintentional violation could also stem from an individual unintentionally facilitating an attack initiated by an outsider (an individual outside of the organization) against the organization. An example of this situation would be an outsider's use of social engineering techniques (Parker, 1998;

Denning, 1999; Schneier, 2000; Mitnick & Simon, 2002) to elicit a user name or password from an individual inside the organization. In this particular example, the individual internal to the organization did not intend to actually cause a security violation, but was instead duped by an outsider into unintentionally facilitating an attack on an organization's information asset(s). Again, the research model focuses only on intentional violations of organizational security policy.

THE THEORY OF PLANNED BEHAVIOR

To assist in examining the phenomenon of intentional violations perpetrated by individuals internal to the organization, this study first turns to the Theory of Planned Behavior (TPB) (Ajzen, 1991) which researchers have successfully used to predict deviant behaviors such as cheating, lying, shoplifting (Beck & Ajzen, 1991), and software piracy in the workplace (Peace, et al., 2002). The TPB is an extension to the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980). The TRA posits that intentions are the antecedent to behavior and are a function of *attitude* and *subjective norm* and that intention mediates an individual's attitude and subjective norms toward committing or not committing the referent behavior (Ajzen & Fishbein, 1980). In expounding on the importance of intentions and their relation to behavior, Ajzen & Fishbein argued that most actions of social relevance are under volitional control and "people consider the implications of their actions before they decide to engage or not engage in a given behavior" (Ajzen & Fishbein, 1980, p. 5). *Intention* reflects motivational factors towards performing or not performing a particular behavior (Ajzen, 1991).

Attitude formation, as generally viewed by social psychologists, is a cognitive or information processing function, and reflects an individual's personal beliefs concerning the referent behavior (Ajzen, 1991). In accordance with the expectancy-value model of attitudes (Fishbein and Ajzen, 1975), the attitudes toward a particular object form from the beliefs people hold about the object. These beliefs form from associating the object with certain attributes such as other objects, characteristics, or events. With regard to behavior (i.e., the object in this case), each belief links the behavior to a certain outcome or cost of performing the behavior. Thus, people learn to form favorable attitudes toward behaviors associated with favorable outcomes, and likewise form unfavorable attitudes toward behaviors associated with negative or unfavorable outcomes (Ajzen, 1991).

Subjective norm reflects an individual's belief that other individuals or groups think he or she should or should not perform the same referent behavior. In the TRA model, one can assign relative weights to attitude and subjective norm to reflect their relative importance to an individual in determining whether to perform a particular behavior (Ajzen & Fishbein, 1980).

According to Ajzen (1991) the TPB (see Figure 6) as an extension to the TRA, addresses the TRA's limitation in dealing with behaviors where people have incomplete volitional control. In the TPB, the constructs *attitude*, *subjective norm*, and *intention* are the same as in the TRA, but the TPB adds *perceived behavioral control* (PBC) as an additional predictor of behavioral intention. PBC reflects an individual's perceived ease or difficulty in performing the referent behavior. According to the theory, PBC can also directly affect behavior holding the other variables in the model constant.

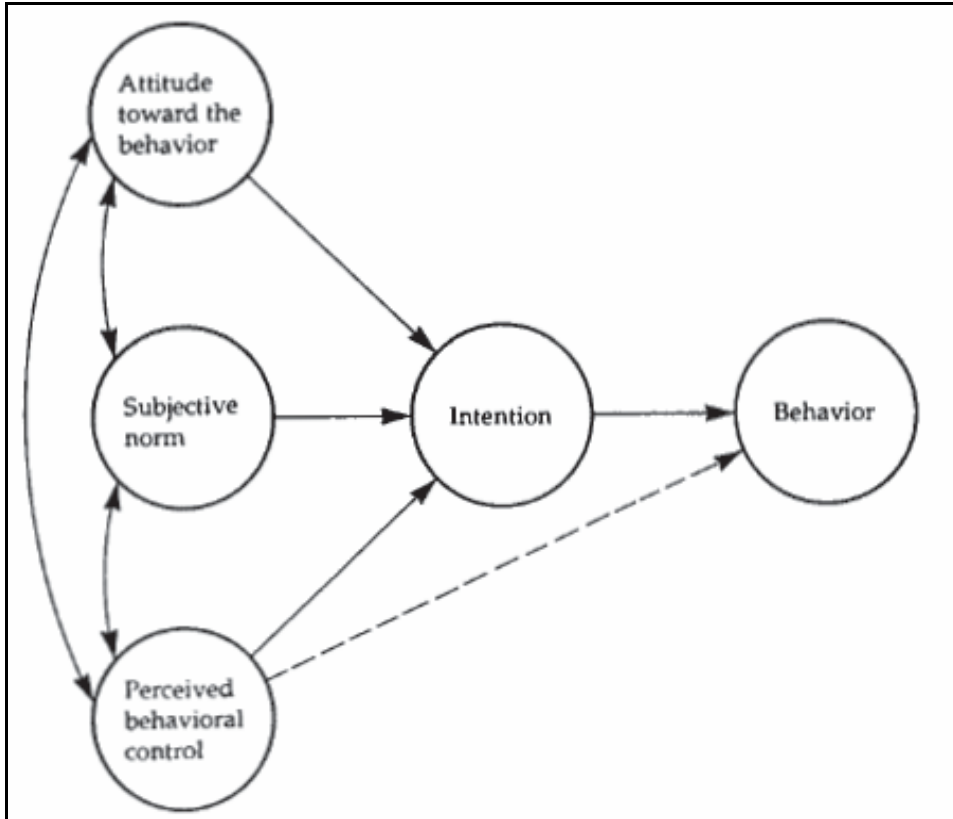


Figure 6 - The Theory of Planned Behavior (Ajzen, 1991, p. 182)

Using the TPB framework in the context of intentional INFOSEC violations, the actual behavior of an insider to knowingly or intentionally violate an organization's INFOSEC policy or rules depends on the individual's *intention* to commit the violation, which in turn is a function of 1) the individual's *attitude* towards committing the violation, 2) how the individual feels that other individuals or groups would approve or disapprove of the violation (i.e., *subjective norm*), and 3) the extent to which the individual thinks he or she is capable of committing the violation (i.e., *PBC*). This discussion leads to the following research hypotheses:

Hypothesis 1: The more favorable an individual's attitude toward committing an INFOSEC violation, the greater the individual's intention to commit the INFOSEC violation.

Hypothesis 2: The greater an individual's subjective norm for committing an INFOSEC violation, the greater the individual's intention to commit the INFOSEC violation.

Hypothesis 3: The greater an individual's perceived behavioral control for committing an INFOSEC violation, the greater the individual's intention to commit the INFOSEC violation.

In accordance with the TPB, behavioral intention is an antecedent of the actual behavior. However, similar to the study by Peace, et.al., (2005), due to the sensitive nature of security and the potential risks and reliability involved with self-reported actual intentional violations of security policy, this study does not directly examine actual intentional violations of policy. To collect data at a later point in time using a code list to test if intention precedes actual behavior would violate participant anonymity and potentially risk harm to study participants. Therefore, this study stops short of testing for the relationship between behavioral intention and actual behavior and accepts that intention is the best predictor of future behavior as per the TPB. This study utilizes the above framework as the basis for the remaining derivation of the research model.

GENERAL DETERRENCE THEORY

General Deterrence Theory (GDT), has its roots in criminology theory and posits that humans are rational actors and that punishments serve as “tangible motives” to deter criminal behavior. The sovereign (e.g., monarch, legislative making body, etc.), for the

basic good of society, has the right to enact laws to punish offenders. The punishment should be proportional to the crime, and society and its laws bind every individual lest anarchy begin (Beccaria, 1995). The basic hypothesis of GDT is that incentives can influence human behavior. The theory predicts that increases in the severity of punishment or the certainty of punishment imposition on those detected, will reduce some criminal acts (Blumstein, et al., 1978).

From an organizational INFOSEC perspective, organizations have effectively used the threat of disciplinary action as a deterrent against IS abuse (Straub, 1990; Straub & Welk, 1998) and researchers have found punishment certainty effective in deterring software piracy in the workplace (Peace, et al., 2003). Straub found that security countermeasures that include deterrent administrative procedures and preventive security software reduced computer abuse. For offenders, severity of punishment for violating INFOSEC rules can range from verbal or written counseling or reprimand, loss of system privileges or, in the case of the federal government, imprisonment or even the death penalty for certain deliberate offenses such as treason (18 USC 794). Computer crime committed by an employee is theorized as a rational act (Dhillon & Moores, 2001), and it is therefore reasonable to assume that people usually commit other INFOSEC related acts based on some sort of rational decision process. Therefore, we argue that the more potential attackers perceive the organization will detect and punish them for violating organizational security policy, the less they believe they are capable of successfully violating INFOSEC policy. In the context of the TPB, this discussion suggests that if an individual perceives that punishment certainty for intentionally violating security is high, then an individual's PBC for intentionally violating security policy would be low. In

accordance with Fishbein & Ajzen's (1975) expectancy-value model of attitudes, it is also reasonable to expect that if a person perceives that management will surely impose punishment for violating INFOSEC policy, then the individual's attitude towards intentionally violating INFOSEC will also be less favorable. This discussion leads to the following research hypotheses:

Hypothesis 4a: The greater the perceived punishment certainty for intentionally violating INFOSEC policy, the lower the perceived behavioral control toward intentionally violating INFOSEC policy.

Hypothesis 4b: The greater the perceived punishment certainty for intentionally violating INFOSEC policy, the less favorable the attitude toward intentionally violating INFOSEC policy.

Under the same line of reasoning using GDT and the expectancy-value model of attitudes (Fishbein & Ajzen, 1975), this study also argues that the perceived severity of punishment meted out by management for violating INFOSEC policy influences an individual's attitude towards violating that policy. This leads to the following research hypothesis:

Hypothesis 5: The greater the perceived punishment certainty for intentionally violating INFOSEC policy, the less favorable the attitude towards intentionally violating INFOSEC policy.

ORGANIZATIONAL COMMITMENT

Organizational commitment (OC) is a psychological construct that represents an important employee attitude (Organ & Bateman, 1986). Many studies examine this

construct in the management literature (see Mathieu & Zajac, 1990). One of the earliest OC definitions is by Steers (1977):

The relative strength of an individual's identification with and involvement in an organization and is characterized by three factors regarding an individual: 1) belief in the acceptance of the organizations goals and values, 2) willingness to exert considerable effort for the organization, and 3) a strong desire to remain a member of the organization (Steers, 1977, p. 46).

According to the above definition which we use in this study, OC has a distinct three-dimensional nature. There does however, appear to be some disagreement in the literature regarding OC's conceptualization and measurement.

Mathieu & Zajac (1990) found that researchers have defined and measured OC in several ways. A common theme they found in the definitions was that "...OC is considered to be a bond or linking of the individual to the organization" (p. 171) and that the definitions seem to differ in the way the bond develops. *Attitudinal* OC, the most common type studied, was defined almost identically to Steers' (1977) definition, and was often measured using the corresponding OCQ scale (Mathieu & Zajac, 1990). Researchers have criticized the OCQ scale for purportedly claiming to be homogenous when the above OC definition implies a three-dimensional nature to the construct which could lead to problems with measuring OC (Benkoff, 1996) and testing relationships between OC and employee turnover (Bozeman & Perrewé, 2001).

According to Mathieu & Zajac, (1990), *calculated* commitment, the second most studied type of OC, was often measured using a scale developed by Hrebiniak and Alutto (1972). As cited by Mathieu & Zajac, calculated commitment was defined by them as "a

structural phenomenon which occurs as a result of individual-organizational transactions and alterations in side-bets or investments over time." Mathieu & Zajac clearly note that attitudinal and calculative OC are not entirely distinguishable concepts in that they somewhat overlap.

Other OC types such as *normative* commitment, which describes a process in which organizational actions and individual predispositions lead to a development of OC, and *organizational identification* have emerged in the literature but have either been subsumed into the attitudinal or calculative definitions or treated separately from OC and treated as correlates (Mathieu & Zajac, 1990).

Mathieu & Zajac's (1990) meta-analysis studied 26 antecedents, 14 correlates, and 8 outcomes for the OC construct and found personal characteristics such as marital status, position tenure, ability, and salary were statistically significant¹ antecedents of OC. In addition, they also found that overall motivation and both intrinsic and extrinsic job satisfaction were significant positive correlates to OC. Finally, they found that job performance (output measure), attendance, and lateness were significant consequences of OC. Lateness was in the negative direction and output measure and attendance were in the positive direction. Mathieu & Zajac did not find many large² correlations with OC and employees' actual behaviors. However, they did find relatively large correlations between OC and behavioral intentions such as *intention to search* and *intention to leave*. Mathieu & Zajac concluded that the results of the meta-analysis suggest that behavioral intentions mediate the influence of OC on the actual behavior. More recent studies found

¹ Indicated by a non-significant chi-square test for the variance remaining unaccounted for across the studies.

² Based on conventions suggested by Cohen (1969) (as cited by the authors) using mean weighted correlation corrected for attenuation.

support for an inverse relationship between OC and employee turnover intention (Allen, Shore, & Griffith, 2003; Thatcher, Stepina, & Boyle, 2002). These findings appear consistent with the TPB in that behavioral intention mediates the actual behavior.

A review of the OC literature by Meyer & Allen (1991) also revealed three general themes in the various definitions encountered: (a) affective attachment to the organization, (b) perceived costs with departing the organization, and (c) obligation to stay with the organization. Meyer & Allen (1991) respectively referred to these themes as *affective*, *continuance*, and *normative* commitment, and adopted them as the components comprising their inductively derived framework for conceptualizing organizational commitment. This process led to the development of separate scales to measure the three OC components (Meyer & Allen, 1991; Benkoff, 1996), and researchers have found evidence to support the construct validity of the three separate measures (Allen & Meyer, 1996). A recent longitudinal study that examined the influence of mentoring on protégé affective commitment and continuance commitment found that only affective commitment partially mediated the negative relationship between mentoring and protégé turnover 10 years later (Payne & Huffman, 2005).

IS and security researchers have theorized or investigated the link between OC and other IS or security-related phenomena. In the IS literature, Igarria & Greenhaus (1992) found significant positive links between a management information systems employee's OC and his/her age, organizational tenure, salary, promotability, and job satisfaction. They also found significant negative relationships between an employee's OC and his/her role conflict and career opportunities. Igarria & Greenhaus (1992) also found that OC had a direct negative effect on turnover intentions, which is similar to

findings by Igarria & Guimaraes (1993), and Thatcher, et al., (2002). Alder, Noel, & Ambrose (2006) found that employee trust in the organization after employer implementation of employee Internet usage monitoring (*post-implementation trust*) was positively related to OC. OC was considered an employee attitude.

In the security literature, Siponen (2001) described the organizational dimension of INFOSEC as a prescriptive dimension of INFOSEC awareness in that the organization requires users to have commitment to the security of the organization. Spurling (1995) also described the importance of achieving a high level of commitment to security in organizations and how leaders in the organization can promote this commitment. Stanton, Stam, Guzman, and Caldera (2003) studied the relationship between organizational commitment and INFOSEC and found inverse relationships between an individual's organizational commitment and certain low-skill security-related computer system behaviors such as personal web surfing, personal gaming, personal email, and abiding by acceptable use policy in general. However, the finding that higher levels of commitment related to lower levels of abiding by acceptable use policy was counterintuitive.

In a Control Theory of Delinquency (Hirschi, 1969), also referred to as Social Control Theory or Social Bond Theory (see Lee & Lee, 2002), a primary assumption is that delinquency results when "... an individual's bond to society is weak or broken" (Hirschi, p. 16). The elements that bond an individual to society are attachment, commitment, involvement, and belief. Attachment refers to an individual's sensitivity to the opinions of others. Commitment refers to an individual's commitment to conventional action, that is: "one is committed to conformity by not only what one has

but also by what one hopes to attain” (Hirschi, p. 21). Involvement refers to the involvement of an individual in conventional activities. The rationale here is that individuals that are too busy doing conventional things have less time to devote to deviant behaviors. Belief refers to the assumption that individuals vary in their belief in the moral validity of social rules, and “...the less a person believes he [or she] should obey the rules, the more likely he [or she] is to violate them. (Hirschi, p. 26).

Placed in the context of TPB for explaining intentional violations of INFOSEC rules, Hirschi’s (1969), concept of attachment is almost identical to the definition of the *subjective norm* construct. The *attitude* construct, in the context of organizational security, reflects the salient beliefs the individual has concerning the INFOSEC rules of the organization. Commitment and involvement as described by Hirschi are also similar to Steers’ (1977) concept of organizational commitment.

This study has expounded on why security plays an important role in organizations today and that individuals should be committed to organizational security. This study argues that if one desires to remain a member of an organization, one must obey the established rules of the organization. Therefore, it is logical to propose that an individual’s organizational commitment inversely relates to an individual’s attitude towards intentional violations of INFOSEC policy. This discussion leads to the following research hypothesis:

Hypothesis 6: The greater the level of organizational commitment, the less favorable the attitude towards intentional violations of INFOSEC.

ORGANIZATIONAL SECURITY CULTURE

This section examines a construct called *security culture*, which is based on the well-known concept of organizational culture. First, this study examines the concept of organizational culture and its related construct, organizational climate. The study then describes the concept of security culture and develops the related research hypotheses.

Many definitions of organizational culture are found in the literature (Park, et al., 2004; Schein, 2004). Although one could use a number of these definitions to define organizational culture, this study, as did Schein (2004), adopts the following definition of the culture of a group:

A pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems (Schein, 2004, p. 17).

Schein's concept of organizational culture (i.e., culture of a group) was first proposed in 1981 and remains one of the few conceptual models of organizational culture ever offered (Hatch, 1993). In Schein's model, organizational culture is composed of three levels. *Artifacts* comprise the first level of organizational culture. These are the visible aspects of organizational culture (e.g., processes and structures) and are difficult for those outside of the organization to decipher. *Espoused values and beliefs* comprise the second level of organizational culture. These values and beliefs (e.g., strategies and

philosophies) can predict or explain much of the behavior observed at the artifact level. They are called espoused, because people may say they will do one thing, yet may actually do something different. *Underlying assumptions* make up the third level of organizational culture. This level consists of ideas and values that are so closely held, that they are rarely questioned or debated by individuals of the organization and are difficult to change. One can think of these assumptions as the paradigm in which the company operates (Schein, 2004).

Other concepts of organizational culture exist. Gagliardi (1986) builds on the concept of assumptions and basic values and links them to organizational strategy and modes of implementation. Hatch (1993) combines Schein's three-level model of organizational culture into a new model called "cultural dynamics" that includes various "processes" drawn from symbolic-interpretive perspectives. As Schein's model is more simplistic, remains influential, and serves as a foundation for competing models, this study uses it.

Others have debated the difference between the concepts of organizational culture and organizational climate, and some have suggested that quantitative-based studies relate more to an organization's climate, and qualitative studies relate more to its culture (as summarized by Bock et al., 2004). Schwartz and Davis (1981) state that climate is not culture (p. 33). Climate measures employees' expectations of what they think working at a particular company should be like. This measure can be used in identifying causes of employee dissatisfaction, which when corrected, can lead to improvements in employee motivation and, in turn, employee performance. Schwartz and Davis argue that culture has more to do with the basic nature of the expectations (e.g., patterns of beliefs)

rather than the measure of whether employee expectations are being met. Schwartz and Davis also regard culture as a more of a long-term or strategic phenomenon that is harder to change because it is deeply embedded in the organization. Climate is more short-term or tactical in nature and is more readily managed than culture. Schwartz and Davis's (1981) view of culture appears consistent with that of Schein's (2004) view in that as one moves from the upper layer of the organizational culture, (the artifacts layer) down through the values and beliefs layer and to the underlying assumptions layer, those lower-level aspects of organizational culture are more deeply embedded in the organization and thus are more difficult to change (Schein, 2004).

Similarly, Moran and Volkwein (1992) examined the differences between organizational culture and organizational climate, and concluded that they are distinct yet closely related constructs with climate being more dynamic than culture, and climate subject to short-term variations in the external and internal environments of the organization. Thus, organizational climate is influenced by organizational culture, but it climate is easier to change than culture. However, in order to be successful, desired changes in climate must take into account the more established aspects of the organization's culture (Moran and Volkwein, 1992).

Given the long-standing debate between organizational culture and organizational climate and the closely related nature of the two constructs, this study's research framework examines a construct similar to organizational culture but focuses on the specific aspects that reflect the INFOSEC or security related artifacts, attitudes, beliefs, and assumptions of the organization. This study refers to this construct as *security*

culture and is identical to the security culture construct described and operationalized by Knapp (2005).

Although studies of both organizational culture and climate and their relationship to other organizational phenomena are found in the general management literature (e.g., Klien, Masi, & Weidner, 1995; Verbeke, Volgering, & Hessels, 1998; Detert, Schroeder & Mauriel, 2000) and in the IS literature (e.g., Tolsby, 1998; Robey & Boudreau 1999; Nahm, Vonderembse, & Koufteros, 2003; Bock, Zmud, Kim, & Lee, 2005), there is an apparent paucity of studies specifically examining the relationship between an organization's security culture and INFOSEC. Of the few studies that exist on this subject, von Solms & von Solms (2004) theorized on the importance of the alignment of a company's security policy to the organization's culture and the role of management in effecting this alignment. In Knapp's (2005) model of managerial effectiveness in INFOSEC, an organization's security culture was found to partially mediate the relationship between top management support (the extent senior leadership is involved in INFOSEC) and perceived security effectiveness as assessed by a survey of 740 information security professionals. For the purposes of this study, security culture is defined as "a set of INFOSEC related beliefs values, understandings, and norms shared by members of an organization."

Placed in the context of the TPB for explaining intentional violations of INFOSEC rules, and using the concept of security culture, it is reasonable to expect that a strong security culture, with its shared values and beliefs of INFOSEC, should engender a strong collective subjective norm against violating security policy. In turn, it is reasonable to expect that a strong collective subjective norm against violations of security

policy will also influence an individual’s subjective norm as it pertains to intentional violations of security policy. In addition, a strong security culture that espouses strong positive values and beliefs about INFOSEC within the organization should also serve to strengthen an individual’s belief in the validity of the INFOSEC policy or rules.

Therefore, we posit that an inverse relationship exists between security culture and an individual’s attitude and subjective norm towards intentional violations of organizational INFOSEC policy. This discussion leads to the following research hypotheses:

Hypothesis 7a: The stronger the security culture, the weaker an individual’s subjective norm towards intentional violations of INFOSEC.

Hypothesis 7b: The stronger the security culture, the less favorable an individual’s attitude towards intentional violations of INFOSEC.

Table 3 provides a summary of the study’s research hypotheses.

Table 3 - Summary of Research Hypotheses

H1	The more favorable an individual’s attitude towards committing an INFOSEC violation, the greater the individual’s intention to commit the INFOSEC violation.
H2	The greater an individual’s subjective norm for committing an INFOSEC violation, the greater the individual’s intention to commit the INFOSEC violation.
H3	The greater an individual’s perceived behavioral control for committing an INFOSEC violation, the greater the individual’s intention to commit the INFOSEC violation.
H4a	The greater the perceived punishment certainty for intentionally violating INFOSEC policy, the lower the perceived behavioral control towards intentionally violating INFOSEC policy.
H4b	The greater the perceived punishment certainty for intentionally violating INFOSEC policy, the less favorable the attitude towards intentionally violating INFOSEC policy.
H5	The greater the perceived punishment severity for intentionally violating INFOSEC policy, the less favorable the attitude towards intentionally violating INFOSEC policy.
H6	The greater the level of organizational commitment, the less favorable the attitude towards intentional violations of INFOSEC.

H7a	The stronger the security culture, the weaker an individual's subjective norm towards intentional violations of INFOSEC.
H7b	The stronger the security culture, the less favorable an individual's attitude towards intentional violations of INFOSEC.

THE STUDY'S MAJOR ASSUMPTION

As discussed earlier, in accordance the TPB, the formation of intention regarding individual behavior is a rational process. Therefore, a major assumption of this study is that predicting intention to violate security policy relies on individuals behaving in a rational manner. We address the possible implications of this assumption in Chapter 5.

In summary, this chapter reviewed the relevant literature to gain insight to factors that have the potential to affect intentional violations of organizational security policy by organizational insiders. By definition, these intentional violations of security policy by members of the organization constitute the insider threat to organizational INFOSEC. Using the theory of planned behavior as a base theory, the study also drew from general deterrence theory (perceived punishment certainty and severity) and organizational behavior concepts (organizational commitment and security culture) to propose a research model. The next chapter details the methodology used to empirically test the research model presented in this chapter.

METHODOLOGY

This chapter describes the research methodology for conducting this study. The participants in this study are individuals of an organization that has an established information security policy. We collected the data using a paper survey instrument.

Survey research is a frequently used and accepted method for conducting research in the field of management information systems. Surveys used for research purposes have three characteristics: (a) Their purpose is to produce quantitative descriptions of some aspects of a studied population, which may include the study of relationships between variables, (b) the collection of information from the participants is accomplished by asking people structured or predefined questions, and (c) the information is usually collected from a sample or fraction of the population in a manner that allows the generalization of the results from the sample to the population (Pinsonneault & Kraemer, 1993). The sample survey methodology also leads to greater generalizability of the results when compared to other research methods (McGrath, 1981).

PARTICIPANTS

As previously discussed in Chapter 2, the unit of analysis in this study's research model is the individual. According to Malhotra & Grover (1998), the unit of analysis is an important survey attribute and should address the following three questions: (a) Is the unit of analysis clearly defined? (b) Does the instrument consistently reflect the unit of analysis? (c) Is the participant(s) chosen appropriate for the research question? For this study, the unit of analysis is the individual who is a member of an organization that has

an established INFOSEC or similarly related security policy (see Chapter 2) that addresses the member's behavior or actions regarding organizational INFOSEC matters. For reasons of anonymity, this study refers to this organization using a pseudonym called Alpha Group. Alpha Group is represented by a convenience sample consisting of mid-level management government employees or contractors currently located at one location. In addition, all members of Alpha group must complete mandatory annual information assurance training understand information assurance policies and procedures.

To address Malhotra & Grover's (1998) attribute questions regarding the unit of analysis, this study clearly defines the individual, who is a member of an organization that has an established security policy, as the unit of analysis. The measures for this study detailed in Appendix C consistently reflect that unit. The participants, who are obligated to adhere to the requirements communicated in an INFOSEC policy, are appropriate for this study's research questions.

DATA COLLECTION PROCEDURES

This study utilizes a paper survey to collect data from the participants. Although the rapid growth in the ubiquity of the Internet has currently made Web-based surveys popular among researchers, these types of surveys usually involve a computerized, self-administered questionnaire (Simsek & Veiga, 2001). However, this study could not guarantee participant anonymity using this venue since computers and their systems may be subject to employer monitoring. Participants returned the survey to the researcher using a pre-paid business reply envelope provided by the researcher.

Despite the ability that surveys have for collecting data from a large number of participants over dispersed geographical areas, Pinsonneault & Kraemer's (1993)

assessment revealed that past MIS surveys suffered from the following shortcomings: (a) single-method designs, (b) unsystematic and inadequate sampling procedures, (c) low response rates, (d) weak relationships between the unit of analysis and the participants, and (e) over reliance on cross-sectional instead of longitudinal surveys.

Given Pinsonneault & Kraemer's (1993) critique of the past shortcomings of MIS survey research, the intrusiveness of INFOSEC research warrants special consideration when selecting study participants (Kotulic & Clark, 2004). An INFOSEC related study by Kotulic & Clark (2004), which included mass mailings of surveys to over 1,500 potential respondents selected from a database of 5,001 US businesses yielded a response rate of approximately 5.1%. This low response rate resulted in the cancellation of the study. Kotulic & Clark investigated the reasons for the low response rate and offered the following lessons learned:

1. INFOSEC research is one of the most intrusive types of organizational research, and the mistrust of "outsiders" makes it virtually impossible to obtain information of this type by mail without a major supporter within the organizations surveyed.
2. Researchers should not use mass mailings of surveys to attempt to collect data of a sensitive nature.
3. Researchers should focus on only a few select firms with whom they have developed an excellent rapport and trust.

Although the unit of analysis for Kotulic & Clark (2004) was at the organization level, this study involves obtaining permission from an organization, Alpha Group, to survey its members about security related matters and behaviors. We have established a

high level of trust and a rapport with the Alpha Group and obtained a major supporter associated with the study sample. This supporter sent out an email to the potential participants prior to the distribution of the survey. The purpose of the supporter's email is to generate interest and encourage individuals to participate in the survey. The supporter also sent two follow-up emails, approximately one week apart, to the participants as an appeal and reminder to complete the survey.

Although a survey of randomly selected individuals from a random sample of organizations would be better at addressing some of the concerns raised by Pinsonneault & Kraemer (1993), the nature of this research requires adoption of the recommendations of Kotulic & Clark (2004), which lends support to the selection of the study participants.

This study also collected demographic data from the participants and compared the demographic data to personnel records in order to calculate the overall response rate and to test for other response biases as required. Traditional sampling frames such as company staff records or employee databases offer the greatest potential for inviting potential respondents. Researchers can then calculate the response rate to assess the generalizability of the survey data (Simsek & Vega, 2001).

A potential shortcoming of this study is its single research method design. This is because the single research method design is susceptible to common method variance, which refers to the variance attributable to the measurement method rather than to the construct of interest (Podsakoff, P., MacKenzie, Lee, and Podsakoff, N., 2003). Another potential shortcoming is the *consistency motif*, a potential method bias where participants attempt to maintain consistency between cognitions and attitudes and therefore make

their responses appear consistent and rational based on responses to similar questions (Podsakoff, et al., 2003).

Another possible source of method bias is *social desirability* (Podsakoff, et al., 2003). Social desirability is a tendency for individuals to admit to socially desirable traits and deny socially undesirable traits (Fernandes & Randall, 1992) and has been suspected as a problem in self-administered surveys such as those involving ethics-based research (Fernandes & Randall, 1992) and personality testing (Dalen, Stanton, & Roberts, 2001). Because this study involves a self-administered questionnaire and deals with undesirable or ethical individual behavior (i.e., violations of security policy), social desirability could present a problem and needs to be addressed and adequately controlled. Reliable scales exist for measuring social desirability and the *measures* section discusses the scale used for this study.

Podsakoff, et al., (2003) describe seven different research situations and provide recommended procedures for controlling common method variance in each setting. To arrive at the research situation that best describes this study, we utilized the flow diagram provided by Podsakoff, et al., (p. 898) as follows: (a) The predictor and criterion variables cannot be obtained from different sources, (b) the predictor and criterion variables cannot be measured in different contexts, (c) the source of the method can be identified (e.g., social desirability), and the method bias can be measured. This results in the selection of research situation #5 to best describe this study. For research situation #5, Podsakoff, et al., (p. 898) recommended the following procedures for controlling common method variance:

1. Use procedural remedies related to questionnaire design such as counterbalancing the order of the items for the independent and dependent variables, or the use of varying response formats.
2. Separate measurement of predictor and criterion variables psychologically and guarantee response anonymity. An example of psychological separation would be through the use of a cover story to make it appear that the independent variables are unconnected to the dependent variables.
3. Utilize the single-specific-method-factor-approach to estimate and control for method bias.

This study implemented the questionnaire design guidelines suggested by Podsakoff, et al., (2003) by counterbalancing the items for the independent and dependent variables and varying the response format of the questions where possible. Furthermore, the study attempted to psychologically separate the independent variables from the independent variables by creating a cover story. The cover story, which is communicated in an information sheet included in the survey package (see Appendix B) informs the potential participant that the purpose of the study concerns factors contributing to *information technology usage* instead of INFOSEC violation intention. Additionally, the study also guarantees response anonymity. The study offers participants and the organization a synopsis of the study findings in a manner and format so that individual responses are not traceable to any single participant. Finally, the study utilizes the statistical methods recommended by Podsakoff, et al., (2003) to estimate and control for social desirability bias.

MEASURES

This section describes the instruments used to measure each of the constructs identified in the research model. A listing of the measures and their associated items is located in Appendix D.

SECURITY POLICY KNOWLEDGE ASSESSMENT

At the beginning of the survey, the instructions first ask participants to refer to a one-page document included in the survey package that identifies common (but not all-inclusive) specific behaviors that are prohibited by the organization's INFOSEC or similar related security policy. To preserve organizational anonymity, that document is not included in this study, but the prohibited behaviors are similar to prohibited behaviors found in the examples provided in Appendix A and Appendix B.

The first item on the survey asks the following question on a 5-item response scale: *I would recognize a security policy violation if I saw one.* Only participants who respond with a value of 4 (*agree*) or 5 (*strongly agree*) are included in the study. The rationale for the review of the specific prohibited behaviors and subsequent assessment screening is that this study is only concerned about intentional violations of security policy. By having participants review their organization's security policy and performing the initial screening, we should have a reasonable level of confidence that a participant is able to recognize a security policy violation, which is fundamental to many of the measures described in the remainder of this section.

PUNISHMENT SEVERITY, PUNISHMENT CERTAINTY, ATTITUDE,
SUBJECTIVE NORM, PERCEIVED BEHAVIORAL CONTROL AND VIOLATION
INTENTION

Measures for these constructs were adapted from the study by Peace et al., (2003). These measures utilize responses on a 5-point scale that is similar to the *semantic differential* technique described by Ajzen & Fishbein (1980, p.20). The composite reliabilities reported by Peace et al., for these constructs were all $\geq .87$, which is well above the .7 cutoff suggested by Nunnally (1978). This study adapted the measures by changing the referent behavior in each original item from *committing software piracy* to *intentionally violating security policy*. Adaptation of measures to reflect the behavior of interest is consistent with previous studies (see Peace et al., 2003; Beck & Ajzen, 1991).

SECURITY CULTURE

We utilized the final 5-item measure of security culture obtained from the study by Knapp (2005). The alpha level of .90 reported by Knapp for this measure is well above the .7 cutoff suggested by Nunnally (1978).

ORGANIZATIONAL COMMITMENT

Although researchers have argued over the past couple of decades about the homogeneous versus the heterogeneous conceptualization and measurement of OC (Porter, Steers, Mowday, & Boulian, 1974; Mowday, Porter, & Steers, 1982; Allen & Meyer, 1990, 1996; Benkhoff 1996; Bozeman & Perrewé, 2001), one of the most widely used measures of OC is the 15-item organizational commitment questionnaire (OCQ) developed by Mowday, Steers Porter (1979). The 15-item OCQ used for this study was obtained from page 221 of Mowday, Porter, & Steers, (1982) and reflects the three-

dimensional definition of OC (Igarria, Greenhaus; & Parasuraman, 1991). Coefficient alpha reported for this measure ranged from .82 to .93 (Mowday, Steers Porter, 1979; Mowday, Porter, & Steers, 1982); and .92 (Igarria, et al., 1991), which is well above the .7 cutoff suggested by Nunnally (1978). Although a shorter 9-item version of the OCQ is available and has been validated by previous IT research (Igarria & Greenhaus, 1992; Igarria, Parasuraman, & Badawy, 1994; Thatcher, et al., 2003), this shortened scale omits items that are highly correlated to employee turnover intention (Igarria & Greenhaus, 1992; Thatcher, et al., 2003). Since this study adopts the three-dimensional definition of OC and does not specifically hypothesize a relationship between OC and employee turnover, we opted to use the 15-item OCQ instead of the shortened version.

SOCIAL DESIRABILITY

The Marlowe-Crowne Social Desirability Scale (M-C SDS) is the most commonly used social desirability bias assessment (Leite & Beretvas, 2005) and several shortened versions of the scale have also been developed and used in past research (Strahan & Gerbasi, 1972; Mandell, n.d.). To minimize the length of the total survey instrument in an attempt to lessen respondent fatigue, we chose to utilize a 20-item version of the original 33-item M-C SDS scale, called the M-C (20) developed by Strahan & Gerbasi (1972). The reliabilities reported for the M-C (20) in four studies conducted by Strahan & Gerbasi (1972) were .78, .83, .73, and .77. The reliabilities reported for the 20-item short form compare favorably to the respective reliabilities of .83, .87, .73, and .78 reported for the original 33-item M-C SDS in the same studies, and are all above the .70 cutoff suggested by Nunnally (1978).

STATISTICAL POWER

Statistical power is defined as “the probability of correctly rejecting the null hypothesis when it is false” (Hair, Black, Babin, Anderson & Tatham, 2006), and is a function of the following: (a) the significance criterion (α) set by the researcher, (b) the sample size used in the study, (c) and the effect size (Hair, et.al, 2006). Researchers can conduct a power analysis when designing a study to ensure they have a reasonable chance of detecting a significant finding (Baroudi & Orlikowski, 1989). A commonly accepted prescription to guard against false positive claims in research studies is to strive for a power of at least .80 (Baroudi & Orlikowski, 1989). Of the three determinants of statistical power, probably the most important determinant is the effect size (Baroudi & Orlikowski, 1989).

Effect size represents an estimate of the magnitude to which the phenomenon under investigation exists within the population (Hair, et. al, 2006). A widely used convention for expressing the magnitude of an effect size is *small*, *medium*, and *large* (Cohen, 1988; Baroudi & Orlikowski, 1989). The accepted values, or convention, associated with these magnitudes vary depending on the specific statistical test employed, and in the case of regression analysis, the values for *small*, *medium*, and *large* are .02, .15, and .35 respectively (Cohen, 1988, p. 412-414). Past MIS research studies are likely to display only small to medium effect sizes, and when past studies do not explicitly report the effect size an alternative approach is to express the effect size in terms of the proportion of the explained variance (R^2) (Baroudi & Orlikowski, 1989). Given that this study utilizes validated measures from previous studies, we can develop an *a priori* estimation of the effect size from previous results. For the measures we plan to utilize for

this study, Peace et al., (2003) reported R^2 values of .24, .46, and .65, which would range from medium to large effect sizes. Knapp (2005) reported an R^2 of .64, and Igbaria & Guimaraes (1993) reported an R^2 of .40, which are both large effect sizes according to Cohen. Although the effect sizes in previous studies ranged from medium to large, several of the measures (e.g., perceived punishment certainty, perceived punishment severity, and security culture) have only been used in a single previous study. Therefore, they do not constitute an established cumulative finding. Thus, researchers should approach these reported effect sizes with caution. As a result, it would be appropriate in this case to employ conventional or proxy effect size levels established by Cohen (1977), which represent small, medium and large effect-size levels of a phenomenon, when calculating the required sample size to achieve a desired power of .80 (Baroudi & Orlikowski, 1989). Additionally, an assumption underlying statistical power is that we randomly select the sample from the population, and that the use of a convenience sample, which is the case here, will result in an overestimation of the statistical power of the tests (Baroudi & Orlikowski, 1989). Thus, we will utilize the more conservative medium effect size instead of the large effect size to determine the required sample size for this study to achieve a statistical power level of .80.

According to Cohen (1988), the calculation of the required sample size requires one to know the desired alpha level, number of predictors, effect size, and the desired statistical power level. For multiple regression, Cohen defines a medium effect size as 0.15 (Cohen, 1988, p. 413). For this study, the value for the number of predictors is based on the use of the Partial Least Squares (PLS) method for analyzing the data. PLS is a method for statistical modeling that has gained acceptance in the MIS literature.

Either simple or multiple regressions are performed during the PLS estimation procedure and, due to the partial nature of the estimation which involves only a portion (i.e., block) of the model at a time, only the portion that constitutes the largest multiple regression is important (Chin & Newsted, 1999; Chin, 2000). The largest multiple regression refers to the specific block of the model containing the endogenous variable that has the greatest number of predictor variables. In the research model for this study, the endogenous variable that has the greatest number of predictors is *Attitude*, which has four predictor variables. Therefore, this block of the model constitutes the largest multiple regression in the PLS analysis (Chin & Newsted, 1999; Chin, 2000). We then calculated the required sample sizes sufficient for obtaining a statistical power of .80 utilizing a medium (.15) effect size, with alpha levels of .01 and .05. Table 4 displays the results of the required sample size analysis. In sum, using a medium anticipated effect size, a sample size between 84 (for $p < .05$) and 118 (for $p < .01$) is required for this study to achieve a statistical power level of .80.

Table 4 - Required Sample Size Analysis

Alpha level	Number of predictors	Anticipated Effect size	Desired Statistical Power Level	Required Sample Size*
.01	4	.15	.80	118
.05	4	.15	.80	84
*calculated using the <i>A-priori Sample Size Calculator (multiple regression)</i> available at http://www.danielsoper.com/statcalc/calc01.aspx (last accessed on November 2, 2006). According to the author of the software, the calculations are based on the approach described in Chapter 9 of Cohen (1988).				

Although increasing the sample size is the most apparent method to increase the statistical power of a study, researchers can use other techniques to increase the statistical power of their studies (Baroudi & Orlikowski, 1989). Among the techniques to improve

statistical power include (a) employing appropriate statistical tests, (b) selecting the independent variables with care, (c) increasing the homogeneity of the sample, and (d) reducing measurement error (Baroudi & Orlikowski, 1989). This study will use PLS which is an accepted MIS data analysis technique, and the researchers carefully selected the independent variables for this study using accepted theory and previous empirical and conceptual studies. By limiting this study to a convenience sample consisting of mid-level government managers at one location who indicate they would recognize a security policy violation if they saw one, this sample should display a relatively high degree of homogeneity. Additionally, in an effort to minimize measurement error, this study employs the use of previously validated measures with past reported reliabilities generally well above the .70 cutoff suggested by Nunnally (1978).

In summary, the methodology employed for this study consists of an anonymous paper-based survey distributed to a convenience sample of government employees. We will test the proposed research model using the collected data and the Partial Least Squares analysis technique.

RESULTS

This chapter describes the methods used to analyze the data collected for this study and the results obtained from the analysis. We collected all data anonymously using a paper-based survey and pre-tested the survey using a group of doctoral students. We made minor formatting modifications to the survey based on the feedback from the students prior to its distribution to the potential participants of Alpha Group (the organization). The participants representing Alpha Group returned the surveys to the researcher using the U.S. Postal Service and the pre-paid Business Reply Mail envelope provided in each of the survey packages. We received the majority of the surveys in the mail approximately one week after the survey distribution; a small number of surveys (6) arrived in the mail approximately four weeks after the survey distribution date. The postmark date printed on each return envelope was the date used as the “received” date. For some unknown reason, 19 of the return envelopes had missing or unreadable postmark dates. We manually transferred the data from the paper surveys to a Microsoft Excel spreadsheet for further analysis and export to SPSS and PLS-Graph software.

DEMOGRAPHICS AND DESCRIPTION OF THE SAMPLE

The sample representing Alpha Group consisted of individuals at a professional government school with students comprising the majority of members. The students are mid-level professionals within the government and generally attend the school at approximately the mid-point of their careers as members of the organization. After attending the school for approximately 10 months, the students move on to other

positions within the government at various locations. The remaining individuals at the school consisted of faculty, management, and administrative support staff whose tenure at the school varies.

Out of 555 survey packages distributed, we received 119 completed surveys for an overall response rate of 21.44%. We excluded five of the responses from the analysis because they failed to meet screening variable criteria (≥ 4); one additional response was excluded from the analysis due to several missing values for social desirability items.

This left a total of 113 usable responses for the analysis. The overwhelming majority of the participant responses (96.46%) were from the students. Unfortunately, we could not ascertain if the lack of responses from the non-students at the school was due to either a lack of interest in the study, the survey packages not reaching them as we intended, or some other non-response factor. The relatively small number of female participants who were all students (8 or 7.3% of the student participants) is consistent with overall female population of the targeted student population at the school (43 females out of 529 total students or 8.1%). Given the relatively short window in which we received the bulk (95%) of the completed surveys, and that 16% of the return envelopes had missing postmarks, we did not find it essential to perform a late versus early responder analysis.

Table 5 summarizes the demographics for the sample.

We calculated descriptive statistics for the variables by first summing the individual indicators for each latent variable to create a composite score. We performed this to gauge the overall score level for each construct. Table 6 provides a summary of the descriptive statistics.

Table 5 - Sample Demographics (N=113)

Gender	Total	Percent
Male	105	92.92
Female	8	7.08
Current position with the organization		
Student	109	96.46
Faculty	0	0
Management	4	3.54
Administrative or Support Staff	0	0
Other	0	0
Total length of time in organization		
Less than 1 year	49 ³	43.36
1 year to less than 5 years	4	3.54
5 years to less than 10 years	1	0.88
10 years to less than 15 years	47	41.59
15 years to less than 20 years	9	7.96
More than 20 years	3	2.65

³ All of these participants also identified themselves as students as their current position within the organization. Students at this school have a least 10 years total time in the greater organization (i.e. government). Therefore, it is reasonable to assume that these individuals mistakenly responded for this question using the length of time in their current position (student) at the school instead of their total length of time in the greater organization.

Table 6 -Descriptive Statistics (N=113)

Variable	Total possible points	Range	Min.	Max.	Mean		Std. Deviation	Variance
		Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Attitude (ATT)	20	8.00	4.00	12.00	5.0391	.17490	1.85925	3.457
Organizational Commitment (OC)	105	65.00	40.00	105.00	81.9527	1.33391	14.17961	201.061
Perceived Behavioral Control (PBC)	10	8.00	2.00	10.00	6.4087	.23443	2.49198	6.210
Perceived Punishment Certainty (CERT)	10	8.00	2.00	10.00	6.5310	.17240	1.83260	3.358
Perceived Punishment Severity (SEV)	10	8.00	2.00	10.00	7.8938	.17883	1.90095	3.614
Screening Variable	5	1.00	4.00	5.00	4.2301	.03977	.42276	.179
Security Culture (CULT)	25	17.00	8.00	25.00	20.3186	.29111	3.09454	9.576
Social Desirability (SD)	20	19.00	1.00	20.00	11.5487	.40520	4.30737	18.553
Subjective Norm (NORM)	15	11.00	3.00	14.00	4.9458	.21627	2.29894	5.285
Violation Intention (VINT)	15	8.00	3.00	11.00	4.7434	.21473	2.28262	5.210

RESEARCH MODEL ASSESSMENT

We utilized the Partial Least Squares (PLS) analysis technique to assess the research model and its proposed hypotheses. Compared to covariance-based SEM techniques such as LISREL, AMOS, and RAMONA, PLS places minimal demands on measurement scales, sample size, and residual distributions, and has as its overall goal to obtain determinate values of the latent variables for the purpose of prediction. PLS also avoids inadmissible solutions and factor indeterminacy issues that can be problems with covariance-based SEM procedures. In addition, in PLS analysis, identification does not pose a problem for recursive models, both reflective and formative measures can be used, and there is no assumption for the presumed distributional form of the data (Chin, 1988).

Like other SEM analysis techniques, the overall assessment of the research model takes place in two distinct steps as suggested by Anderson & Gerbing (1988). The first step, measurement model assessment, establishes the validity and reliability of the measures used in the study. The second step, structural model assessment, tests the strength of the hypothesized relationships between the latent variables in the model Anderson & Gerbing (1988).

MEASUREMENT MODEL ASSESSMENT

Prior to testing the hypothesized relationships between the constructs, one is required to demonstrate that the measurement model meets acceptable levels of validity and reliability (Fornell & Larcker, 1981). Convergent validity and discriminant validity are two elements of factorial validity that represent how well the measurement items used in the survey relate to the latent variables in the research model (Gefen & Straub, 2005). We assessed the items used to measure *social desirability* separately using Cronbach's alpha and performed a correlation with the other constructs to test for the influence of social desirability on the other latent variables. We present this analysis after the assessment of the original research model.

PLS FACTORIAL VALIDITY

To demonstrate factorial validity for reflective measurement items, one needs to show that a measurement item satisfactorily correlates with its intended construct (i.e., convergent validity) and correlates weakly (i.e., discriminant validity) with the other constructs in the research model. PLS performs a confirmatory factor analysis (CFA) to assess factorial validity (Gefen & Straub, 2005). All measurement items used in this study are reflective.

Convergent validity is demonstrated when the Outer Model Loadings for the items have a t-statistic of >1.96 (Gefen & Straub, 2005). We obtained the values from the Outer Model Loadings section of the PLS boot.out file using the Generate Bootstrap procedure with 200 resamples in PLS-Graph (see Table 7). Upon inspection of the t-statistics for each item, four items (OC4, OC7, OC12, and OC13) had t-statistics less than 1.96. Therefore, we dropped those four items from all further analyses and re-executed the Generate Bootstrap procedure in PLS-Graph. All t-statistics in the subsequent Bootstrap procedure were >1.96 , therefore there is evidence to support a claim of convergent validity.

Table 7 - PLS-Graph Outer Model Loadings (using Bootstrap with 200 resamples)

Item	t-statistic
CERT1	13.1009
CERT2	25.3589
SEV1	89.5249
SEV2	64.5856
OC1	2.3561
OC2	2.8277
OC3	2.3759
OC4	1.6544*
OC5	2.5538
OC6	2.8327
OC7	0.3597*
OC8	2.8694
OC9	2.5680
OC10	2.7483
OC11	2.8905
OC12	0.1691*
OC13	1.2645*
OC14	2.1935
OC15	2.0893
CULT1	3.8538
CULT2	3.7830
CULT3	4.8435
CULT4	3.3281
CULT5	3.5906
PBC1	21.3947
PBC2	26.8825
NORM1	43.7208
NORM2	33.2542
NORM3	5.3430
ATT1	27.2311
ATT2	8.0764
ATT3	31.4652
ATT4	18.8299
VINT1	28.7915
VINT2	7.7109
VINT3	16.7290

* These items dropped from further analyses since they did not display a t-statistic of >1.96 (see Gefen & Straub, 2005).

ASSESSMENT OF DISCRIMINANT VALIDITY

Gefen and Straub (2005, p. 97) detail two procedures for assessing discriminant validity using PLS-Graph:

1. Examine item loadings to construct correlations.
2. Examine the ratio of the square root of the AVE of each construct to the correlations of this construct to all the other constructs.

Discriminant validity using PLS-Graph is demonstrated when:

1. The correlation of the latent variable scores with the measurement items needs to show an appropriate pattern of loadings, one in which the measurement items load highly on their theoretically assigned factor and not highly on other factors.
2. Establishing discriminant validity in PLS also requires an appropriate AVE (Average Variance Extracted) analysis. In an AVE analysis, we test to see if the square root of every AVE (there is one for each latent construct) is much larger than any correlation among any pair of latent constructs. (Gefen & Straub, 2005, p. 93-94)

Using the process detailed by Gefen & Straub (2005) for Procedure 1, we first generated item loadings based on latent factor scores for each of the constructs in the model using PLS-Graph. Then, using SPSS, we performed a bivariate correlation analysis (Spearman's rho) between those latent variable scores and the original item values. Spearman's rho is nonparametric and should be used if the data could violate distributional assumptions (Gefen & Straub, 2005). Because we made no distributional

assumptions concerning the data, we chose to utilize Spearman's rho correlations versus Pearson correlations. Results of the correlation analysis are located at Table 8. The bolded items in the table emphasize the loading of the items on the constructs assigned in the confirmatory factor analysis.

Table 8 - Discriminant Analysis Procedure 1 (item loadings and cross-loadings)

	SEV	CERT	ATT	NORM	PBC	VINT	CULT	OC
SEV1	0.965	0.275	-0.396	-0.427	-0.011	-0.327	0.177	-0.041
SEV2	0.941	0.284	-0.380	-0.506	-0.109	-0.410	0.149	-0.097
CERT1	0.234	0.707	-0.162	-0.273	-0.271	-0.243	0.148	-0.106
CERT2	0.288	0.957	-0.158	-0.203	-0.350	-0.261	0.231	0.068
ATT1	-0.465	-0.084	0.695	0.465	-0.013	0.411	-0.104	0.088
ATT2	-0.284	-0.059	0.893	0.325	0.142	0.346	-0.199	0.031
ATT3	-0.458	-0.256	0.741	0.461	0.090	0.448	0.035	0.152
ATT4	-0.393	-0.135	0.755	0.525	0.092	0.446	-0.091	0.118
NORM1	-0.467	-0.201	0.510	0.830	0.092	0.600	-0.117	0.087
NORM2	-0.444	-0.161	0.444	0.875	0.051	0.592	-0.098	0.054
NORM3	-0.307	-0.234	0.292	0.803	0.115	0.467	-0.104	0.120
PBC1	0.021	-0.287	0.145	0.082	0.878	0.205	-0.117	-0.051
PBC2	-0.089	-0.336	0.120	0.135	0.912	0.163	-0.079	0.041
VINT1	-0.365	-0.243	0.444	0.611	0.179	0.924	-0.044	-0.062
VINT2	-0.328	-0.230	0.392	0.417	0.103	0.649	-0.109	-0.015
VINT3	-0.339	-0.316	0.455	0.568	0.217	0.911	-0.001	0.102
CULT1	0.116	0.129	-0.092	-0.171	-0.164	-0.039	0.769	0.343
CULT2	0.104	0.109	-0.115	-0.123	-0.034	-0.039	0.706	0.331
CULT3	0.196	0.251	-0.177	-0.208	-0.126	-0.088	0.865	0.264
CULT4	0.108	0.241	-0.115	-0.056	-0.029	0.085	0.741	0.298
CULT5	0.060	0.235	0.003	-0.098	-0.064	0.038	0.771	0.249
OC1	-0.057	-0.001	-0.057	0.053	-0.038	-0.035	0.048	0.515
OC2	-0.031	-0.063	-0.002	0.083	0.135	0.046	0.212	0.761
OC3	-0.050	0.015	0.005	0.067	-0.100	-0.047	0.127	0.697
OC5	0.016	0.060	-0.011	-0.089	0.146	-0.059	0.422	0.627
OC6	0.088	0.085	0.062	-0.010	0.090	-0.003	0.283	0.763
OC8	0.019	0.136	0.030	0.046	-0.002	-0.047	0.317	0.784
OC9	-0.027	0.106	0.043	0.018	0.009	-0.115	0.332	0.679
OC10	-0.069	-0.056	0.034	-0.028	0.030	0.000	0.270	0.772
OC11	-0.116	0.084	0.070	0.013	-0.134	0.039	0.325	0.752
OC14	0.030	0.076	-0.063	-0.006	-0.095	-0.062	0.336	0.682
OC15	0.036	-0.042	0.015	-0.045	0.093	-0.012	0.276	0.594

When examining the table of item loadings and cross-loadings (Table 8), we utilized the following heuristic stated by Gefen & Straub, 2005:

Established thresholds do not yet exist for loadings to establish convergent and discriminant validity. In fact, comparing a CFA in PLS with a [Exploratory Factor Analysis] EFA with the same data and model, Gefen et al., (2000) showed that loadings in PLS could be as high as .50 when the same loadings in an EFA are below the .40 threshold. Nonetheless, in our opinion, all the loadings of the measurement items on their assigned latent variables should be an order of magnitude larger than any other loading. For example, if one of the measurement items loads with a .70 coefficient on its latent construct, then the loadings of all the measurement items on any latent construct but their own should be below .60 (p. 93-94).

Applying the above heuristic, no items appeared problematic. In addition, in factor analysis, researchers recommend that items load on their theorized constructs with values of at least 0.5 to 0.7 as evidence of validity (Chin, 1998). All items in the sample loaded on their theorized constructs with acceptable loading values. Therefore, we retained all the remaining items for further analyses.

Using the second process detailed by Gefen & Straub (2005) for assessing discriminant validity, we re-executed the Bootstrap procedure (sans items OC4, OC7, OC12, and OC13) to obtain the updated AVE values calculated for the latent constructs from the Boot.out file. We then obtained the correlations of the latent variables obtained from the .LST file and compared the correlations to the square root of the AVE reported for each latent variable (see Table 9). Applying Gefen and Straubs' (2005) above

heuristic for Procedure 2, no items appear problematic and therefore we conclude that there is adequate support for discriminant validity. However, one should note that for this heuristic, Gefen and Straub state: “The square root of the AVE of each construct needs to be much larger, although there are no guidelines about how much larger, than any correlation between this construct and any other construct.” (Gefen & Straub, 2005, p. 105)

Table 9 -Discriminant Analysis Procedure 2 -- AVE Analysis (SQRT AVE on the diagonals)

	CERT	SEV	OC	CULT	PBC	NORM	ATT	VINT
CERT	0.874							
SEV	0.316	0.958						
OC	0.006	-0.098	0.705					
CULT	0.267	0.156	0.33	0.791				
PBC	-0.372	-0.062	-0.02	-0.137	0.895			
NORM	-0.254	-0.551	0.098	-0.15	0.102	0.809		
ATT	-0.157	-0.474	0.107	-0.04	0.092	0.593	0.858	
VINT	-0.342	-0.446	0.045	-0.08	0.215	0.606	0.494	0.814

One can also use the AVE as an additional assessment of discriminant validity because it represents the amount of variance captured by the construct in relation to the amount of variance due to measurement error, and the AVE should be at least .50 (Fornell & Larcker, 1981). Table 10 provides the AVE calculated by PLS-Graph for each latent variable using the Bootstrap process. The AVE for OC is at the minimum acceptable threshold (when rounding to two decimal places) and we therefore retained the variable in the model. All other reported AVEs were also satisfactory.

Table 10 – Results of PLS Confirmatory Factor Analysis

Variable	Items	Average Variance Extracted	Composite Reliability
Perceived punishment certainty (CERT)	2	0.764	0.866
Perceived punishment severity (SEV)	2	0.917	0.957
Organizational commitment (OC)	11	0.497	0.914
Security Culture (CULT)	5	0.625	0.892
Perceived behavioral control (PBC)	2	0.801	0.890
Subjective norm (NORM)	3	0.654	0.846
Attitude (ATT)	4	0.736	0.917
Violation intention (VINT)	3	0.663	0.854

In summary, the statistical evidence supports the factorial validity (both convergent and discriminant) of the retained measurement items. The final item to address with respects to assessment of the measurement model concerns the statistical concept of reliability.

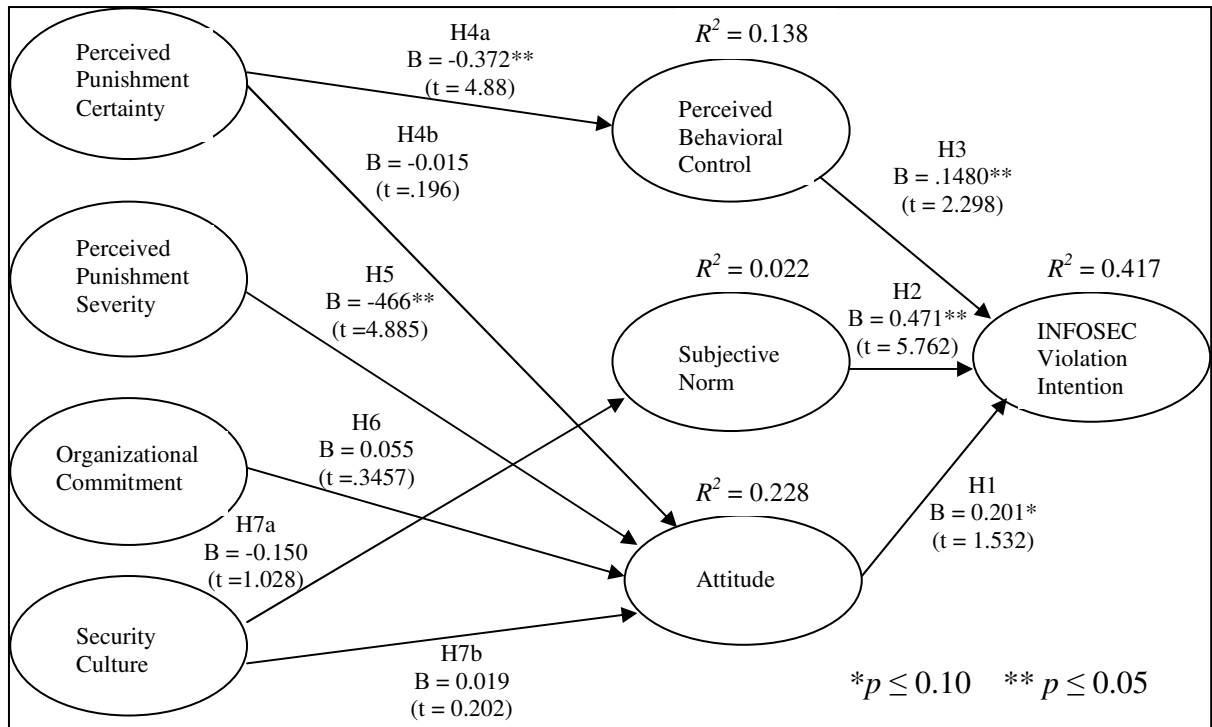
RELIABILITY

Reliability, in general, is the degree of consistency between repeated measurements of a variable (Hair, et al., 2006). Composite reliability is one measure of reliability of a group of measurement items and is the type of reliability calculated by the PLS-Graph program (Chin, 1988). According to Chin (1998), composite reliability is similar to another measure of reliability known as Cronbach's alpha. However, composite reliability differs from Cronbach's alpha in that it does not assume equal weights among the indicators. Refer to Table 10 for the composite reliabilities reported for the items used to measure each of the latent variables. All composite reliabilities calculated by PLS were well above the 0.70 minimum level suggested by Nunnally (1978).

STRUCTURAL MODEL ASSESSMENT

Having previously assessed the measurement model and determined that the model demonstrates acceptable levels of validity and reliability, the next step was to assess the structural paths of the model as a test of this study's posited hypotheses. When using PLS, the coefficient of determination (R^2) is the criterion for assessing the dependent variables in the structural model and one can interpret them in the same manner as with regression (Chin, 1998). To test the individual hypotheses, one examines the significance of the t -values reported for the standardized path coefficients calculated by the PLS software. We assessed the significance of the t -values using a one-tail test since the hypotheses were directional in nature. Figure 7 summarizes the PLS analysis of the structural model.

Figure 7 - Results of PLS Structural Model Analysis



The results of the structural model analysis revealed partial support for the study's hypotheses. Table 11 provides a summary for the results of the tests of the study's hypotheses.

Table 11- Tests of hypotheses results

Hypothesis	Result	<i>p</i>-value
H1	Weakly supported	≤ 0.10
H2	Supported	≤ 0.05
H3	Supported	≤ 0.05
H4a	Supported	≤ 0.05
H4b	Not supported	> 0.10
H5	Supported	≤ 0.05
H6	Not supported	> 0.10
H7a	Not supported	> 0.10
H7b	Not supported	> 0.10

SOCIAL DESIRABILITY BIAS ASSESSMENT

We assessed the level of each participant's social desirability (SD) using a shortened version of the Marlow-Crown Social Desirability Scale (MC(20)). To assess the validity of the scale, we first summed the indicators to create a SD score for each participant, then we performed a box plot of the scores to check for the presence of outliers; none was present. We then computed Cronbach's alpha using SPSS to assess the reliability of the MC(20) scale. The Cronbach's alpha computed for the MC(20) scale was 0.883 which was above the .70 cutoff suggested by Nunnally (1978) and compared favorably to those reported in studies conducted by Strahan & Gerbasi (1972).

To test if the social desirability of the participants possibly biased the way they responded to the other measures used in the survey, we conducted a correlation analysis between the SD scores (the summed MC(20) items) and the latent variable scores calculated by PLS-Graph. We utilized Spearman's rho for the correlation analysis since

we made no distributional assumptions concerning the data. The results of the correlation analysis revealed a significant positive correlation between social desirability and perceived punishment certainty (0.188, $p \leq .05$, 2-tailed), and a significant negative correlation (-0.226, $p \leq .05$, 2-tailed) between social desirability and perceived behavioral control.

Given the significant correlation between social desirability and at least one of the four endogenous variables in the model, we next introduced social desirability as a control variable by allowing it to load on each of the four endogenous variables in the model. To assess the impact of the control variable, we then examined the significance of the change in the R^2 values for the endogenous variables when the control variable was added to the original model. The resulting analysis revealed no significant changes ($p \leq .05$) in R^2 in any of the endogenous variables. Although the change in R^2 for perceived behavioral control exhibited a slight significant increase ($p \leq .10$), given that R^2 can only increase with the addition of a variable to a regression model (Kutner, Nachtstein, Neter, & Li, 2005), we concluded that social desirability did not significantly bias the predictive ability of any of the endogenous variables. Table 12 summarizes the results of the ΔR^2 analysis.

Table 12 - ΔR^2 analysis when adding social desirability as a control variable

Exogenous Variable	R^2_2 (Model with control variable added)	R^2_1 (Original model)	ΔR^2 ($R^2_2 - R^2_1$)	F-statistic⁴
Perceived behavioral control	0.164	0.138	0.026	3.421*
Subjective norm	0.028	0.022	0.006	0.667
Attitude	0.241	0.228	0.013	1.857
INFOSEC violation intention	0.423	0.417	0.006	1.200

* Significant at the $p \leq 1.0$ level

In sum, the analysis of the data revealed partial support for the study's hypotheses. The impact of social desirability bias did not appear to be a factor that significantly influenced the overall results.

⁴ Calculated using the following formula: $F_{(k_2 - k_1, n - k_2 - 1)} = [(R^2_2 - R^2_1)/(k_2 - k_1)] / [(1 - R^2_2)/(n - k_2 - 1)]$

DISCUSSION

This research yielded interesting results for researchers and managers. By focusing on constructs that theoretically related to the three principal theoretical constructs commonly used for predicting behavioral intention, this research suggests areas on which organizations can focus to reduce the insider threat to their organizations' information security. In this chapter, we first discuss the findings and conclusions of the study as they relate to the proposed hypotheses and the study's specific research questions. Next, we then discuss the implications that the study's findings and conclusions have for managers and then for researchers. Lastly, we conclude with a discussion of the study's limitations.

FINDINGS AND CONCLUSIONS

Hypotheses 1, 2, and 3 of this study proposed that an individual's attitude, subjective norm, and perceived behavioral control towards violations of organizational security policy positively relate to intention to commit an INFOSEC violation. The findings of this study were generally consistent with the Theory of Planned Behavior (Ajzen, 1991) and suggested that for individuals: 1. A favorable attitude towards intentional INFOSEC policy violations leads to an increase in intention to commit the violations (this hypothesis was only weakly supported ($p \leq 1.0$)); 2. The greater the subjective norm towards intentional INFOSEC policy violations, the greater the intention is to commit intentional INFOSEC policy violations; and 3. The higher the level of

perceived behavioral control with regards to intentional INFOSEC policy violations, the greater the intention to commit the violations.

The R^2 for violation intention was .417. Thus, attitude, subjective norm, and perceived behavioral control accounted for approximately 41% of the variance in behavioral intention. One could consider these three factors (taken together) as relatively significant predictors of behavioral intention. Given that behavioral intention mediates the actual related behavior (Ajzen, 1991), it is reasonable to suppose that the more individuals intended to commit INFOSEC policy violations, the more likely they would actually intentionally commit INFOSEC policy violations.

The remaining hypotheses in this study investigated possible factors that could theoretically relate to the three aforementioned principal constructs of the Theory of Planned Behavior. This study investigated those possible factors to address the four specific research questions (RQ1-RQ4) stated in Chapter 1.

Hypothesis 4a of this study proposed that the greater the perceived punishment certainty for intentionally violating INFOSEC policy, the lower the perceived behavioral control towards intentionally violating INFOSEC policy. This hypothesis also related to specific research question RQ4, which asked “Does the perceived certainty of punishment affect the insider threat to organizational security?” The results of the study provided support for this hypothesis and were consistent with similar findings regarding the deterrence of software piracy in the workplace (Peace, et al., 2003) and computer abuse (Straub, 1990). Therefore, this study supported the supposition that, when placed in the context of the Theory of Planned Behavior, an increased perceived certainty of punishment relates to lower intentional violations of security policy through perceived

punishment certainty's inverse relationship with an individual's perceived behavioral control for committing the behavior.

Hypothesis 4b proposed that the greater the perceived punishment certainty for intentionally violating INFOSEC policy, the less favorable is the attitude towards intentionally violating INFOSEC policy. This hypothesis also related to specific research question RQ4. The results of this study did not support this hypothesis. This finding is not consistent with related findings by Peace, et al., (2003), Kankanhalli, et al., (2003) and Hollinger (1993) described in Chapter 3, but is generally consistent with those of Skinner & Fream (1997) who found that certainty of apprehension was not useful for deterring software piracy.

One possible explanation for the finding of non-support for hypothesis 4b is the relatively numerous specific prohibited behaviors identified in the examples of security policy violations provided to the survey participants. It is possible that the relationship between punishment certainty and attitude varied greatly based on the specific prohibited behavior a participant had in the forefront of his/her mind when completing the survey. In addition, it is also possible that some individuals had considered themselves technically knowledgeable, and thus perceived they were unlikely to be caught violating INFOSEC policy (i.e., having low perceived punishment certainty). Yet their attitude toward intentionally violating INFOSEC policy was less favorable because of their increased awareness of the possible harm to the organization that may result. One possible example of this type of individual would be an INFOSEC expert within the organization.

Hypothesis 5 posited that the greater the perceived punishment severity for intentionally violating INFOSEC policy, the less favorable the attitude towards intentional violations of INFOSEC policy. This hypothesis also related to specific research question RQ3. The study's findings support this hypothesis, and this specific finding is consistent with that found by Peace et al., (2003) regarding software piracy in the work place.

Hypothesis 6 proposed that the greater the level of organizational commitment, the less favorable the attitude towards intentional violations of INFOSEC policy. This hypothesis related directly to specific research question RQ2. Although organizational commitment did not inversely relate to attitude as originally posited, the relationship was not significant. Comparing this result to those obtained by Stanton, et al., (2003), Stanton, et al., unexpectedly found that individuals with high levels of organizational commitment tended to report lower levels of compliance with acceptable use policies. In the same study, Stanton, et al., also found that individuals with higher levels of organizational commitment were less likely to engage in specific common counter-productive computer security-related behaviors when using company computers. These behaviors were identified as personal web surfing, personal e-mail, and personal gaming. In an attempt to explain this contradiction, Stanton, et al., offered two possible speculative explanations. The first possible explanation offered was that organizations that engender high levels of organizational commitment in their employees may have less need to promote and enforce acceptable use policies, as opposed to organizations who engender low levels of organizational commitment in their employees and thus may be forced to strongly promote and enforce their acceptable use policies. The second possible

explanation offered by Stanton, et al., was based on the psychological concept of “reaction formation” which basically states that if rules are imposed upon a person which then results in a reduction in personal choice, that individual will form a negative reaction to the restriction and work to surmount it. This then leads Stanton et al., to speculate that individuals having high levels of organizational commitment may feel entitled to “substantial freedom of action” and resent the restrictions the acceptable use policies impose upon them.

This study appeared to differ from Stanton et al.’s (2003) study in that we first referred the participants to a list of specific behaviors contained in their organization’s security policy. The first survey item then asked the participants if they felt they would recognize a policy violation if they saw one. Thus, we were confident that the participants included in the study knew what specific behaviors were prohibited by policy. Stanton et al., listed “abiding by acceptable use policies” as a specific behavior in itself in addition to specific low-skill security-related behaviors. In this current researcher’s opinion, it was unclear if the participants in the Stanton et al., study actually knew what specific behaviors were prohibited by their organization’s policy. The Stanton et al., study also utilized an OC measure different from the one used in this study, which could possibly explain the differing results.

On the other hand, the inconclusive results for this hypothesis may be due to some participants reacting to a specific listed behavior instead of the security policy as a whole. Given the results reported in the study by Stanton, et al., it is conceivable that a participant’s attitude toward security policy violations in general, may differ from that associated with a specific prohibited behavior, and that particular behavior may have

provoked a strong reaction in the participant and was reflected in their response to the attitude measures. For example, in this study a participant who is highly committed to the organization may have a more favorable attitude towards security violations because he/she resents the restrictions placed upon him/her by the security policy in general. On the other hand, a highly committed individual may have a less favorable attitude towards a specific security violation because they believe the risks they might expose the organization to for violating the specific behavior is so great, they that they would never contemplate violating it. This divergence in attitudes based on the participants' frame of reference (security policy as a whole, or specific prohibited behaviors) when they answered the questions may have had a cancellation effect and resulted in a non-significant beta coefficient for hypothesis 6.

Hypotheses 7a and 7b both related to specific research question RQ1 and posited that the stronger the security culture, both the weaker an individual's subjective norm (H7a) and attitude (H7b) towards intentional violations of INFOSEC policy. The data did not support either hypothesis.

For hypothesis 7a, the beta coefficient was in the expected direction, but the t-value was not significant. Furthermore, the R^2 for subjective norm was only .022, which suggests that security culture was not a significant predictor of an individual's subjective norm toward intentional violations of INFOSEC policy. The beta coefficient for hypothesis 7b was neither in the anticipated direction nor significant.

Culture, in part, reflects the attitudes and beliefs espoused by individuals of the organization (Schein, 2004). One plausible possibility for the unsupported findings for both hypotheses H7a and H7b is the long-standing debate between organizational culture

and organizational climate. It is possible that shorter-term organizational issues, which are more reflective of an organization's "climate", affect an individual's attitude and subjective norm more so than longer-term organizational issues more commonly attributed to organizational culture. In that case, although an individual may perceive his/her organization as having a strong security culture, recent observations or experiences concerning INFOSEC in the workplace may more strongly influence his/her attitude and subjective norm towards intentional violations of INFOSEC policy.

Although three of the four variables used in this study to predict the latent "attitude" construct did not prove significant, the R^2 for the attitude construct was .228. One can interpret this as perceived punishment severity accounted for 22.8% of the variance in an individual's attitude towards intentional violations of INFOSEC policy.

The assessment of social desirability bias using self-report data is essential to ascertain if the desire of the study participants to be socially acceptable biased their responses to the questions and thus lead to misleading study results. The assessment of social desirability bias in this study, and finding that it did not significantly bias the results was not surprising given that past studies concerning the Theory of Planned Behavior and the use of self-report information did not reveal systemic bias when the researchers controlled for social desirability (Beck & Ajzen, 1991). Because the survey was paper-based and totally anonymous, this likely had permitted the participants to answer the questions more truthfully than if their anonymity could not be guaranteed or if they had suspicions that their identity could be compromised if the data were collected by the researcher online using the Web or e-mail.

Having insight into several factors useful for predicting the insider threat to organizational INFOSEC, the following sections discuss the implications of the study's results for managers and researchers.

IMPLICATIONS FOR MANAGERS

Executives and managers should endeavor to make sure their management programs, policies, and procedures align with and focus on shaping the attitudes, subjective norms, and perceived behavioral control of their employees with respect to intentional violations of INFOSEC policy to attempt to lessen the insider threat to their organizations. Managers should realize the relationship that attitude, subjective norm, and perceived behavior control have with intention to violate security policy and strive to influence these factors to reduce employee intentions to violate said policy. Managers should conceivably accomplish this through an effective INFOSEC awareness program (see Spurling, 1995). Such a program should not only educate employees on what the security rules of the organization are, but also inform them of the potential consequences, both to the organization and the individual, for intentionally violating the security rules. Based on the expectancy-value model of attitudes (Fishbein and Ajzen, 1975), individuals who expect a negative outcome from a particular behavior are likely to develop an unfavorable attitude towards that particular behavior. If managers are successful in shaping the attitudes of its employees, it is reasonable to expect that an individual's subjective norm towards intentionally violating security policy will reflect the collective norm of the organization. That is, an individual should be less likely to intentionally violate security policy if the individual feels the other employees in the organization would greatly disapprove of that behavior (i.e., subjective norm).

Upon hiring, managers should provide a copy of the INFOSEC policy to users and require them to acknowledge by signature that they have read the policy and agree to abide by it. Mitnick & Simon (2002), stress that businesses must not only define security policies and rules, but they also should endeavor to ensure all who work with corporate information or IT systems follow them and also understand the reason behind the rules and policies so they do not circumvent them for the sake of convenience. This could be accomplished as part of a comprehensive on-going security awareness training program. Before granting permission to access organizational IT systems, organizations should “license” their users. This licensing process could include the completion of introductory INFOSEC awareness training. Managers should also consider implementing a formal process whereby technophiles and other early adopters of technology have a means to request the evaluation and possible approval of new and innovative IT technologies that they believe will make them more productive in the workplace. This could help reduce employee negative reaction to what may seem like overly restrictive rules that prohibit the use of newer technologies, and reduce employee temptation to intentionally circumvent the rules, which could place the organization at grave risk.

Managers should also act appropriately to increase their employees’ perceived punishment certainty in an attempt to reduce employees’ perceived behavioral control towards intentional violations of INFOSEC policy. Managers could possibly accomplish this through several means to include recurrently informing their employees that their IT related activities are subject to monitoring at all times, and that security procedures have been put in place to detect and log unauthorized user activity on the organization’s IT systems. Where possible, security systems should provided users with an automatically

generated security system warning if their unauthorized activity is detected by the monitoring system to deter them from further unauthorized activity. Managers and security personnel should monitor the security logs and take appropriate actions against violators. The old security mantra “deny all that is not specifically permitted” should be put into practice. For example, if INFOSEC policy prohibits downloading and installing unapproved software on organizational IT systems, then the ability to install executable files onto IT systems should be limited (using operating system user profiles) only to system administrators or other authorized individuals. The use of Internet gateway proxy servers can also restrict users from browsing objectionable websites or using specific prohibited services such as telnet or Internet relay chat.

Managers should work closely with their Human Resources departments to ensure that hiring, promotion, and disciplinary policies address INFOSEC violations and that all employees understand these policies and management consistently enforces them. To increase perceived punishment severity, managers should clearly communicate the possible punishments for intentional violations of INFOSEC policy and apply the punishments in a fair and consistent manner to all violators. Often in disciplinary actions, the severity of punishment, or if any punishment is administered at all, depends on the actual outcome resulting from the violation. Instead, managers should consider taking appropriate disciplinary actions based on the worst potential outcome of the violation.

Lastly, computer crime committed by an employee is theorized as a rational act (Dhillon & Moores, 2001), and it is therefore reasonable to assume that people usually intentionally commit INFOSEC policy violations using a rational decision process influenced in part by the certainty and severity of punishment. Therefore, managers and

supervisors should be vigilant to situations or events that could cause their employees to behave irrationally. These situations or events could be employee terminations, financial, legal, and other personal matters. In such cases, managers should consider promptly restricting employee access (especially those employees with access to highly sensitive information) to certain information assets.

IMPLICATIONS FOR RESEARCHERS

This study demonstrated that the Theory of Planned Behavior can serve as a valid core framework for examining the insider threat to organizational INFOSEC. In addition, this study provided supporting evidence for the role punishment certainty and severity plays in shaping the core predictors of behavioral intention. Given the R^2 values reported for the endogenous constructs in this study, there clearly is room to investigate additional predictive factors. Researchers can draw from other criminology theories such as General Deterrence Theory (see Blumstein, 1978; Beccaria, 1995), Social Control Theory (see Hirschi, 1969), Social Learning Theory (see Akers, 1985) for additional insights.

In this study, the data failed to support the hypothesized role organizational commitment and organizational security culture in the framework of the Theory of Planned Behavior. Additional data collection drawing from randomized samples from different organizations may yield different results and provide better insight as to the predictive power of these theoretically important constructs. The use of different scales for measuring organizational commitment or security culture may also produce results that are more conclusive.

Lastly, the specific behaviors prohibited by organizational INFOSEC policies can be numerous and vary by organization and even the specific position within the

organization. Perhaps it would be useful to identify the one specific prohibited behavior common to most INFOSEC policies that employees are most likely to commit. This may lead to responses that are more consistent from study participants, as the specific behavior they had in mind when responding to the survey questions about violations of policy would not be in question. To accomplish this, researchers could possibly survey organizations to identify and rank the most commonly reported violations and identify the one specific behavior employees are most likely to violate.

LIMITATIONS OF THE STUDY

Like all studies, this one also has its limitations. When generalizing the results of this study to the population of organizational IT users, a randomized sample of organizational IT users drawn from various geographical areas, from the private sector, and from across various industries would lend greater support for generalizing the results.

Secondly, the use of self-report measures has its inherent limitations, and common method bias presents a potential problem when collecting data on the independent and dependent variables at the same point in time (Spector, 1994). As previously indicated, we selected the participants based on their self-reported knowledge of specific behaviors prohibited by their organization's INFOSEC policy, and only included participants who either agreed or strongly agreed that they would recognize a security policy violation if they saw one. However, in the survey packet, we included a list of specific behaviors prohibited by the organization's security policy and we instructed the participants to refer to the list before answering the survey questions.

Lastly, the usable sample size we obtained, was sufficient for the use of the PLS analysis technique. However, a larger sample size (>200) would have permitted the use of

more common structural equation modeling (SEM) analysis methods such as AMOS or LISREL which report goodness of fit indices that one can compare with generally accepted heuristics for structural model assessment.

REFERENCES

- 18 USC 794. Retrieved December 1, 2005, from
[http://www4.law.cornell.edu/uscode/html/
uscode18/usc_sec_18_00000794----000-.html](http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000794----000-.html).
- Alder, G., Noel, T., & Ambrose, M. (2006). Clarifying the effects of Internet monitoring on job attitudes: the mediating role of employee trust. *Information & Management*, 43, 894-903.
- Allen, N. & Meyer, J. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of Occupational Psychology*, 63, 1-18.
- Allen, N. & Meyer, J. (1996). Affective, continuance, and normative commitment to the organization: an examination of construct validity. *Journal of Vocational Behavior*, 49, 252-276.
- Allen, D., Shore, L., & Griffeth, R. (2003). The role of perceived organizational support and supportive human resource practices in turnover process. *Journal of Management*, 29(1), 99-118.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50, 179.
- Ajzen, I & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Upper Saddle River: Prentice-Hall, Inc.
- Akers, R. (1985). *Deviant behavior* (Third ed.). Belmont: Wadsworth Publishing Co.

- Anderson, J. & Gerbing, D. (1988). Structural equation modeling in practice: a review and recommended two-step approach. *Psychological Bulletin*, 103, 411-423
- ATIS Telecom Glossary (2000). Retrieved December 1, 2005 from <http://www.atis.org/tg2k/>.
- Balasubramanian, S., Konana, P., & Menon, N. M. (2003). Customer satisfaction in virtual environments: a study of online investing. *Management Science*, 49(7), 871.
- Baroudi, J. & Orlikowski, W. (1989). The problem of statistical power in MIS research. *MIS Quarterly*, 13(1), 87-106.
- Beccaria, C. (1995). *On crimes and punishments and other writings*. Cambridge: Cambridge University Press.
- Beck, L. & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality*, 25, 285.
- Benkhoff, G. (1996). Disentangling organizational commitment. *Personnel Review*, 26(1/2), 114-131.
- Bisson, J., & Saint-Germain, R. (n.d.). Implementation of security policies based on the bs7799 / iso 17799 standard-for a better approach to information security (white paper). Retrieved July 19, 2005, from <http://www.infoedge.com/samples/CA-0001free.pdf>
- Blumstein A. (1978). Summary. In: Blumstein A, Cohen J, Nagin D, editors. *Deterrence and incapacitation: estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

- Bock, G., Robert, W., Kim, Y., & Lee, J. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate. *MIS Quarterly*, 29(1), 87.
- Bozeman, D. & Perrewé, P. (2001). The effect of item content overlap on organizational commitment questionnaire-turnover cognition relationships. *Journal of Applied Psychology*, 86(1), 161-173.
- Chin, W. (1988). The partial least squares approach to structural equation modeling. In: Marcoulides, G., editor. *Modern Methods for Business Research*. Mahwah: Lawrence Erlbaum Associates.
- Chin, W. (2000). Frequently Asked Questions – Partial Least Squares & PLS-Graph. Home Page.[On-line]. Retrieved October 15, 2006 from <http://discnt.cba.uh.edu/chin/plsfaq.htm>.
- Chin, W. & Newsted, P. (1999). Structural equation modeling analysis with small samples using Partial Least Squares. In Hoyle, R. (1999), *Statistical Strategies for Small Sample Research*. Thousand Oaks: Sage Publications, 307-341.
- Cohen, J. (1969). *Statistical power analysis for the behavior sciences*. New York: Academic Press.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd edition). Hillsdale: LEA Publishers.
- CSO Magazine (2006). Online glossary. Retrieved September 1, 2006 from <http://www.csoonline.com/glossary/>.

- CSO Magazine, U.S. Secret Service, CERT Coordination Center, Microsoft Corp. 2006
e-crime watch survey (2006). Retrieved December 2, 2006, from
www.cert.org/archive/pdf/ecrimesurvey06.pdf
- Dalen, L., Stanton, N., & Roberts, A. (2001). Faking personality questionnaires in
personnel selection. *Journal of Management Development*, 20(8), 729-741.
- Denning, D.E. (1999). *Information warfare & security*. New York: Addison-Wesley.
- Detert, J., Schroeder, R., & Mauriel, J. (2000). A Framework for Linking Culture and
Improvement Initiatives in Organizations. *Academy of Management Review*,
25(4), 850-863
- Dhillon G. & Moores, S. (2001). Computer crimes: theorizing about the enemy within.
Computers & Security, 20(8), 715.
- Dillman, D. (2000). *Mail and Internet surveys: The tailored design method* (2nd Ed.).
New York: John Wiley & Sons.
- DoD 5200.1-R, (1997), *Information Security Program*, Retrieved December 1, 2005 from
<http://www.dtic.mil/whs/directives/corres/html/52001r.htm>
- Ernst, & Young. (2004). Ernst & young global information security survey 2004.
Retrieved July 18, 2005, from www.ey.com.
- Fernandes, M. & Randall, D. (1992). The nature of social desirability response effects in
ethics research. *Business Ethics Quarterly*, 2(2). 183-205.
- Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior*. Reading:
Addison-Wesley.

- Fornell, C. & Larcker, D. (1981). Evaluating structural equation models with unobservable variable and measurement error. *Journal of Marketing Research* 18(1), 39-50.
- Gagliardi, P. (1986). The creation and change of organizational cultures: A conceptual framework. *Organization Studies*, 7(2), 117-134.
- Gefen, D. & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: tutorial and annotated example. *Communications of the Association for Information Systems*, 16. 9-109.
- Guel, M. (2001). A short primer for developing security policies. Retrieved October 1, 2006 From http://www.sans.org/resources/policies/Policy_Primer.pdf?portal=6bb5823efb94b0c631f1a37109ad625d.
- Hair, H., Black, W., Babin, B, Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis*. Upper Saddle River: Pearson-Prentice Hall.
- Hatch, M. J. (1993). The dynamics of organizational culture. *Academy of Management Review*, 18(4), 657.
- Hirschi, T. (1969). *Causes of delinquency*. Berkley: Univ. of California Press.
- Hollinger, R. (1993). Crime by computer: correlates of software piracy and unauthorized account access. *Security Journal*, 4(1), 2.
- Igbaria, M., Greenhaus, J., & Parasuraman, S. (1991). Career orientations of MIS employees: an empirical analysis. *MIS Quarterly* (June), 151-169.

- Igbaria, M. & Greenhaus, J. (1992). Determinants of MIS employees' turnover intentions: a structural equation model. *Communications of the ACM*, 35(2), 35-49.
- Igbaria, M. & Guimaraes, T. (1993). Antecedents and consequences of job satisfaction among information center employees. *Journal of Management Information Systems*, 9(4), 145-174.
- Igbaria, M., Parasuraman, S, & Badaway, M. (1994). Work experiences, job involvement, and quality of work life among information systems personnel. *MIS Quarterly* (June), 175-201.
- Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139.
- Klein, A., Masi, R., & Weidner, C. (1995). Organization culture, distribution and amount of control, and perceptions of quality. *Group & Organization Management*, 20(2), 122-148.
- Knapp, K. (2005). A model of managerial effectiveness in information security from grounded theory to empirical test. *Dissertation Abstracts International*, 66 (12), p. 4444. (UMI No. 3201451)
- Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, 41(3), 377.
- Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, 41(5), 597.

- Kutner, M., Nachtsheim, C., Neter, J., & Li, W. (2005). *Applied Linear Statistical Models*. New York: McGraw-Hill/Irwin
- Lee, J. & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2/3), 57
- Lee, S., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*, 707.
- Leite, W. & Beretvas, N. (2005). Validation of scores on the Marlow-Crowne Social Desirability Scale and the balanced inventory of desirable responding. *Educational and Psychological Measurement, 65*(1), 140-154.
- Liao, Z. & Cheung, M. T. (2001). Internet-based e-shopping and consumer attitudes: An empirical study. *Information & Management, 38*(5), 299.
- Liao, Z. & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: An empirical study. *Information & Management, 39*(4), 283.
- Loch, K. & Cogner, S. (1996). Evaluating ethical decision making and computer use. *Communications of the ACM, 39*(7), 74.
- Malhotra, M. & Grover, V. (1998). An assessment of survey research in POM: from constructs to theory. *Journal of Operations Management, 16*, 407-425.
- Mandell, R. (n.d.). Evaluating shorter versions of the Marlowe-Crowne Social Desirability Scale. Retrieved October 15, 2006 from:
http://www1.od.nih.gov/behaviorchange/measures/PDF/MC10_scoring.pdf

- Mathieu, J. & Zajac, D. (1990). A review and meta-analysis of the antecedents, correlates, and consequences of organizational commitment. *Psychological Bulletin*, 108(2), 171-194.
- McGrath, J. (1981). Dilemmatics-the study of research choices and dilemmas. *American Behavioral Scientist*, 25(2). 179-210.
- Messmer, E. (2003). Security spending up. *Network World*. Retrieved July 18, 2005, from <http://www.networkworld.com/weblogs/security/003595.html>.
- Meyer, J. & Allen, N. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*, 1(1), 61-89.
- Mitnick, D. & Simon, W. (2002). *The art of deception*. Indianapolis: Wiley Publishing, Inc.
- Moran, E., Volkwein, J. (1992). The cultural approach to the formation of organizational climate. *Human Relations*, 45(1), 19-47.
- Mowday, R., Porter, L., & Steers, R. (1982). *Employee-organization linkages*. San Diego: Academic Press.
- Mowday, R., Steers, R., & Porter, L. (1979). The measurement of organizational commitment. *Journal of Vocational Behavior*, 14, 224-247.
- Nahm, A., Vonderembse, M., Koufteros, X. (2004). The impact of organizational culture on time-based manufacturing and performance. *Decision Sciences*, 34(4), 579-607.
- Nunnally, J. (1978). *Psychometric theory* (2nd Ed.). New York: McGraw-Hill.
- Organ, D & Bateman, T. (1986). *Organizational behavior: an applied psychological approach* (Third ed.). Plano: Business Publications, Inc.

- Park, H., Ribiere, V. & Schulte, W. (2004). Critical attributes of organizational culture that promote knowledge management technology implementation success. *Journal of Knowledge Management*, 8(3), 106
- Parker, D. B. (1998). *Fighting computer crime*, New York: John Wiley & Sons, Inc.
- Payne, S. & Huffman, A. (2005). A longitudinal examination of the influence of mentoring on organizational commitment and turnover. *Academy of Management Journal*, 48(1), 158-168.
- Peace, G, Galletta, D., & Thong, J. (2003). Software piracy in the workplace: a model and empirical test. *Journal of Management Information Systems*, 20(1), 153-177
- Pinsonneault, A. & Kraemer, K. (1993). Survey research methodology in management information systems. *Journal of Management Information Systems*, 10(2), 75-105.
- Podsakoff, P.M., MacKenzie, S.B., Lee, J., & Podsakoff, N.P. (2003). Common method biases in behavioral research. *Journal of Applied Psychology*, 88(5), 879-903.
- 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.
- SANS (2006). The SANS security policy project. Retrieved October 1, 2006 from <http://www.sans.org/resources/policies/#hipaa>.
- Schein, E. H. (2004). *Organizational culture and leadership* (Third ed.). San Francisco: Jossey-Bass.
- Schneier, B. (2000). *Secrets & lies*. Indianapolis: Wiley Publishing, Inc.
- Schwartz, H. & Davis, S. (1981). Matching corporate culture and business strategy. *Organizational Dynamics*, Summer, 30-48.

- Simsek, Z. & Veiga, J. (2001). A primer on internet organizational surveys. *Organizational Research Methods*, 4(3), 218-235.
- Siponen, M. (2000). A conceptual foundation for organizational security awareness. *Information Management & Computer Security*, 8(1), 31-41.
- Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society*, 24-29.
- Skinner, W. & Fream, A. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, 34, 495.
- Spector, P. (1994). Using self report questionnaires in OB research: a comment on the use of a controversial method. *Journal of Organizational Behavior*, 15, 385-392.
- Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2), 20-26.
- Stanton, J. M., Stam, K. R., Guzman, I., & Caldera, C. (2003). Examining the linkage between organizational commitment and information security. Retrieved December 1, 2005, from <http://sise.syr.edu/StantonIEEE1.pdf>
- Steers, R. (1977). Antecedents and outcomes of organizational commitment. *Administrative Science Quarterly*, 22, 48.
- Strahan, R. & Gerbasi, K. (1972). Short, homogeneous versions of the Marlowe-Crowne Social Desirability Scale. *Journal of Clinical Psychology*, 28, 191-193.
- Straub, D. (1990). Effective IS security: an empirical study. *Information Systems Research*, 1(3), 255.
- Straub D. & Nance, W. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, 14(1), 45.

- Straub, D. & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4), 441.
- Thatcher, J., Stepina, L., & Boyle, R. (2002). Turnover of information technology workers: Examining empirically the influence of attitudes, job characteristics, and external markets. *Journal of Management Information Systems*, 19(3), 231-261.
- Theoharidu, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24, 472.
- 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.
- U.S. Secret Service & CERT Coordination Center (2005). Insider threat study: computer system sabotage in critical infrastructure sectors. Retrieved December 1, 2005 from http://www.secretservice.gov/ntac/its_report_050516_es.pdf
- Verbeke, W., Volgering, M., & Hessels, M. (1998). Exploring the conceptual expansion within the field of organizational behavior: organizational climate and organizational culture. *Journal of Management Studies*, 35(3), 303-329.
- von Solms, R. & von Solmes, S. (2004). From policies to culture. *Computers & Security*, 23, 275-279.

APPENDICES

APPENDIX A – SECURITY POLICY (ACCEPTABLE USE)

DOCUMENT TEMPLATE ⁵



InfoSec Acceptable Use Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>. established culture of openness, trust and integrity. InfoSec is committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

⁵ Source: SANS Institute (2006), available at http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf. Last accessed on November 9, 2006.

4.0 Policy

4.1 General Use and Ownership

1. While <Company Name>'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of <Company Name>. Because of the need to protect <Company Name>'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Company Name>.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.
5. <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the <Company Name> Internet/Intranet/Extranet, whether owned by the employee or <Company Name>, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term Definition

Spam Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

APPENDIX B – SECURITY POLICY (ACCEPTABLE USE) EXAMPLE⁶

ACCEPTABLE USE POLICY (AUP)

Reference: AR25-2 (Information Assurance). A well-protected DoD/Army network enables organizations to easily handle the increasing dependence on the Internet. For a DoD/Army organization to be successful, it needs to integrate information that is secure from all aspects of the organization. The purpose of this policy is to outline the acceptable use of computer equipment within a DoD/Army organization. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD/Army units to risks including attacks, compromise of network systems and services, and legal issues. This policy applies to all employees, contractors, consultants, temporary employees, and other workers assigned to the DoD/Army organizations.

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the Secret Internet Protocol Router Network (SIPRNET) and/or Non-secure Internet Protocol Router Network (NIPRNET) from unauthorized or inadvertent modification, disclosure, destruction, denial or service, and use.
2. **Access.** Access to this network is for official use and authorized purposes and as set forth in DOD Directives 5500.7-R (Joint Ethics Regulation) AR 25-2 (Information Assurance) and Army network policy and accreditation.
3. **Revocability.** Access to Army Information Systems resources is a revocable privilege and is subject to content monitoring and security testing.
4. **Classified information processing.** SIPRNET is the primary classified Information System (IS) for Army units. SIPRNET is a classified only system and approved to process SECRET collateral information as SECRET and with SECRET handling instructions.
 - a. The SIPRNET provides classified communication to external DoD agencies and other U.S. Government agencies via electronic mail.
 - b. The SIPRNET is authorized for SECRET level processing in accordance with accredited SIPRNET ATO.
 - c. The classification boundary between SIPRNET and NIPRNET requires vigilance and attention by all users.
 - d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.
5. **Unclassified information processing.** NIPRNET is the primary unclassified information system for Army units. NIPRNET is an unclassified system.
 - . NIPRNET provides unclassified communication to external DOD and other United States Government organization. Primarily, this is done via electronic mail and Internet networking protocols such as Web Access, Virtual Private Network, and Terminal Server Access Controller System (TSACS).

⁶ Source: <https://ia.gordon.army.mil/iss/cua.htm>. Last accessed on November 9, 2006.

- a. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2 and local automated information system security management policies. A DAA has accredited this network for processing this type of information.
 - b. The NIPRNET and the Internet, for the purpose of the AUP, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet, as well as all inbound/outbound data, external threats (e.g., worms, denial of service, hacker) and internal threats.
 - c. Public Key Infrastructure (PKI) Use:
 - 1. Public Key Infrastructure provides a secure computing environment utilizing encryption algorithms (Public/Private-Keys).
 - 2. Token/Smart Card (or CAC). The Cryptographic Common Access Card Logon (CCL) is now the primary access control mechanism for all Army users (with very few exceptions). This is a two phase authentication process. First, CAC is inserted in to a middleware (reader), and then a unique user PIN number provides the validation process.
 - 3. Digital Certificates (Private/Public Key). CAC is used as a means to sending digitally signed e-mail and encrypted e-mail.
 - 4. Private Key (digital signature), as a general rule, should be used whenever e-mail is considered "Official Business" and contains sensitive information (such as operational requirements). The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail.
 - 5. Public Key is used to encrypt information and verify the origin of the sender of an email. Encrypted mail should be the exception, and not the rule. It should only be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act (HIPPA).
 - 6. Secure Socket Layer (SSL) technology should be used to secure a web based transaction. DoD/Army Private (Intranet) web servers should be protected by using this technology IAW DoD/Army PKI implementation guidance.
6. **User Minimum-security rules and requirements.** As a SIPRNET and/or NIPRNET system user, the following minimum security rules and requirement apply:
- . I understand personnel are not permitted access to SIPRNET or NIPRNET unless in complete compliance with the DOD, Army personnel security requirement for operating in a SECRET system-high environment.
 - a. I have completed the required security awareness-training (e.g., Annual AT Awareness Training Level I or Computer Security for Users and provided proof of completion to my IASO. IAW AR25-2, prior to receiving network/system access, I will participate in all DoD/Army sponsored Security Awareness Training and Certification program (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering). I understand that my initial training will expire in one year and that I will be required to take an annual

refresher training (IAW AR 25-2) and my account will be disabled until I have met this requirement.

- b. I will generate, store, and protect my logon credentials (passwords or pass-phrases). Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.), IAW AR25-2, Chapter 4, Section IV, Para 4-12 passwords should be changed at least every 90 days to 150 days.
- c. When I use my CAC to logon to the network, I will make sure it is removed prior to leaving the computer that I logged on.
- d. I will use only authorized hardware and software on the DoD/Army networks to include wireless technology. I will not install or use any personally owned hardware, software, shareware, or public domain software.
- e. To protect the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb storage device, or other storage media.
- f. I will not attempt to access or process data exceeding the authorized IS classified level.
- g. I will not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized.
- h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.
- i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.
- j. I will not utilize Army- or – DOD – provided ISs for commercial financial gain or illegal activities.
- k. Maintenance will be performed by the System Administrator (SA) only.
- l. I will use screen locks and log off the workstation when departing the area.
- m. I will immediately report any suspicious output, files, shortcuts, or system problems to the SA and /or the Information Assurance Security Officer (IASO) and cease all activities on the system.
- n. I will address any questions regarding policy, responsibilities, and duties to my IASO and/or DOIM SA.
- o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realized that I should not store data on the IS that I do not want others to see.

- p. I understand that monitoring of SIPRNET and NIPRNET will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions. I understand that the following activities are prohibited uses of an Army IS:
1. Unethical use (e.g., Spam, profanity, sexual misconduct, gaming, extortion).
 2. Accessing and showing unauthorized sites (e.g., pornography, streaming videos, E-Bay, chat rooms).
 3. Accessing and showing unauthorized services (e.g., peer-to-peer, distributed computing).
 4. Unacceptable use of e-mail include exploiting list servers or similar group broadcast systems for purposes beyond intended scope to widely distribute unsolicited e-mail (SPAM); sending the same e-mail message repeatedly to interfere with recipient's use of e-mail; sending or broadcasting, e-mail messages of quotations, jokes, etc., to multiple addressees; sending or broadcasting unsubstantiated virus warnings from sources other than IAMs (e.g., mass mailing, hoaxes, auto-forwarding).
 5. Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).
 6. To show what is deemed proprietary or not releasable (e.g., Use of keywords, phrases or data identification).
- q. I understand that I may use an Army IS for limited personal communications by e-mail and brief internet searches provided they are before or after duty hours, break periods, or lunch time or IAW local policies and regulations, as long as they do not cause an adverse impact on my official duties; are of reasonable duration, and causes no adverse reflection on DOD. Unacceptable use of services or policy violations may be a basis for disciplinary actions and denial of services for any user.
- r. The authority for soliciting your social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to DoD/Army information systems.
- s. I understand that repetitive violation of this AUP or AR 25-2 security measures will result in the lost of my privilege. I further understand that I will receive a written counseling statement from my first line supervisor, and in order to lift this restriction a memorandum from my Commander/Director (or designated representative) will be required. This request will be routed via the IASO to the installation Information Assurance Manager (IAM).
7. **Acknowledgement.** I have read the above requirements regarding use of the DoD/Army access systems. I understand my responsibilities regarding these systems and the information contained in them.

Directorate/Division/Branch

Date


Last Name, First, MI (print)

Rank/Grade and SSN
(SSN: Last four digits)

Signature

Area Code and Phone Number

APPENDIX C – PARTICIPANT INFORMATION LETTER



1856 2006
AUBURN
 UNIVERSITY
Sesquicentennial

01 LOWDER BUSINESS BLDG.
 AUBURN, AL 36849-5241

TELEPHONE:
 334-844-4071

FAX:
 334-844-5159

www.auburn.edu

COLLEGE OF BUSINESS
DEPARTMENT OF MANAGEMENT

**INFORMATION SHEET
for Research Study Entitled
“Information Technology Usage in Organizations”**

You are invited to participate in a research study investigating information technology usage in organizations. I, Todd Dugo, am conducting the study under the supervision of Kelly Rainer, Ph.D. I hope to learn about information technology use in organizations. You were selected as a possible participant because you regularly utilize information technology products and services (e.g. computers, Internet access, electronic mail, etc.) within your organization.

If you decide to participate, you will only be required to fill out a simple survey that will take approximately 15-20 minutes of your time to complete. The information gleaned from this study will aide future researchers and managers concerned with information technology use in organizations.

Any information obtained in connection with this study will remain anonymous. Information collected through your participation will be used to fulfill an educational requirement (e.g. doctoral dissertation), and may be published in a professional journal, and/or presented at a professional meeting, etc. You may withdraw from participation at any time, without penalty, however, after you have provided anonymous information you will be unable to withdraw your data after participation since there will be no way to identify individual information.

Your decision whether or not to participate will not jeopardize your future relations with Auburn University or the Department of Management. If you have any questions about this study, I invite you to contact me at dugotod@auburn.edu, (334) 567-0546, or Dr. Kelly Rainer at rainerk@auburn.edu, (334) 844-6527 and we will be happy to answer them.

For more information regarding your rights as a research participant, you may contact the Auburn University Office of Human Subjects Research or the Institutional Review Board by phone (334) 844-5966 or e-mail at hsubjec@auburn.edu or IRBChair@auburn.edu.

HAVING READ THE INFORMATION PROVIDED, YOU MUST DECIDE WHETHER TO PARTICIPATE IN THIS RESEARCH PROJECT. IF YOU DECIDE TO PARTICIPATE, THE DATA YOU PROVIDE WILL SERVE AS YOUR AGREEMENT TO DO SO. THIS LETTER IS YOURS TO KEEP.

Todd M. Dugo 16 Feb 07
Investigator's signature Date

Todd Dugo

Print Name

HUMAN SUBJECTS
OFFICE OF RESEARCH
PROJECT # 06-260 EX 0702
APPROVED 2/5/07 TO 2/4/08

Owing much to the past, Auburn's greater debt is ever to the future.

APPENDIX D – MEASURES

Security policy violation knowledge self-assessment (1=strongly disagree; 2=disagree; 3=neutral; 4=agree; 5=strongly agree).								
Spka	I would recognize a security policy violation if I saw one?							
Punishment severity (adapted from Peace, et al., 2003)								
Sev1	If I were caught intentionally violating security policy, I think the punishment would be:*	VERY HIGH	1	2	3	4	5	VERY LOW
Sev2	If I were caught intentionally violating security policy, I would be severely punished.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Punishment certainty (adapted from Peace, et al., 2003)								
Cert1	If I intentionally violated security policy, the probability I would be caught is:	VERY LOW	1	2	3	4	5	VERY HIGH
Cert2	If I intentionally violated security policy, I would probably be caught.	STRONGLY AGREE	1	2	3	4	5	STRONGLY AGREE
Attitude (adapted from Peace, et al., 2003)								
Att1	To me, intentionally violating security policy is:*	GOOD	1	2	3	4	5	BAD
Att2	To me, intentionally violating security policy is:*	PLEASANT	1	2	3	4	5	UNPLEASANT
Att3	To me, intentionally violating security policy is:	FOOLISH	1	2	3	4	5	WISE
Att4	To me, intentionally violating security policy is:	UNNATtractive	1	2	3	4	5	ATTRACTIVE
Subjective norm (adapted from Peace, et al., 2003)								
Norm1	If I intentionally violated security policy, most of the people who are important to me would:*	APPROVE	1	2	3	4	5	DISAPPROVE
Norm2	Most people who are important to me would look down on me if I intentionally violated security policy.	LIKELY	1	2	3	4	5	UNLIKELY
Norm3	No one who is important to me thinks it is okay to intentionally violate security policy.	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Perceived behavioral control (adapted from Peace, et al., 2003)								
Pbc1	If I want to, I can intentionally violate security policy.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Pbc2	Technically, for me to intentionally violate security policy is:*	EASY	1	2	3	4	5	DIFFICULT
Violation intention (adapted from Peace, et al., 2003)								
Vint1	I may intentionally violate security policy in the future.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Vint2	If I had the opportunity, I would intentionally violate security policy.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE

Vint3	I would never intentionally violate security policy.	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Security culture (Knapp, 2005). SD=strongly disagree; D=disagree; N= neutral, A=agree; SA=strongly agree. Beginning with the phrase: <i>In the organization...</i>								
Cult1	Employees value the importance of security.							
Cult2	Security has traditionally been considered an important organizational value.							
Cult3	Practicing good security is an accepted way of doing business.							
Cult4	The overall environment fosters security-minded thinking.							
Cult5	Information security is a key norm shared by organizational members.							
Organizational commitment (Mowday, Steers, in Porter, 1979; In Mowday, Porter, & Steers, 1982, p. 221). Items OC1-OC15: 1=strongly agree; 2=moderately disagree; 3=slightly disagree; 4=neither disagree nor agree; 5=slightly agree; 6=moderately agree; 7=strongly agree.								
M-C (20) Social Desirability Scale (Strahan & Gerbasi, 1972, p. 192). Items SD1-SD20: T=true; F=false. A value of 1 is assigned for each item when the respondent provides a response that matches the given response below. A value of 0 is assigned for each discordant participant response. The total possible score is 20 (all participant responses match correctly).								
Demographics**								
Gender: Male, Female								
Which of the following best describes your current position within the organization?:								
Student Faculty Management Administrative or Support Staff Other								
The total length of time you have been a member of the organization:								
Less than 1 year 1 year to less than 5 years 5 years to less than 10 years 10 years to less than 15 years 15 years to less than 20 years More than 20 years								
* Reversed scale.								
** This information will be requested for the sole purpose of assessing nonresponse bias.								