Fall 2010

The Relationship Between Situational Crime Prevention Theory and Campus Employee Computer Misuse

M. Juliane Santiago

THE RELATIONSHIP BETWEEN SITUATIONAL CRIME PREVENTION THEORY AND CAMPUS EMPLOYEE COMPUTER MISUSE

by

M. JULIANE SANTIAGO

(Under the Direction of Teri Denlea Melton)

ABSTRACT

Computer misuse is a leading problem for all industry sectors, including higher education. However, much of the current research related to computer misuse has been conducted in the business sector, leaving higher education a relatively unstudied group. Many theories have been addressed in computer security literature, but only one theory offers a more holistic solution to combating computer misuse, Situational Crime Prevention Theory. Situational Crime Prevention Theory encompasses four categories of countermeasures: countermeasures that Increase the Perceived Effort of the offender, countermeasures that Increase the Perceived Risk of the offender, countermeasures that Reduce the Anticipated Rewards of the offender, and countermeasures that Remove the Excuses to offend. This study endeavored to investigate whether a relationship exists between the categories of countermeasures found in Situational Crime Prevention and the actual number of computer misuse incidents reported by CIO's of public, four-year colleges and universities. Using a web-accessible, anonymous questionnaire, CIO's of 442 public, four-year colleges and universities were asked to provide information related to the countermeasures that they have in place at their institutions and the number of

insider computer misuse incidents their institutions experienced in the year 2009. The data were analyzed with PLS-Graph software to include composite reliability, *t* statistic and critical value analysis, and R-square analysis. Results showed a significant relationship between two out of four categories of countermeasures and the actual number of computer misuse incidents. These results would be particularly useful to administrators in higher education who are responsible for designing a technology security plan that is focused and cost-effective.

INDEX WORDS: Computer misuse, Higher education, Situational crime prevention theory

The Relationship Between Situational Crime Prevention Theory And Campus Employee Computer Misuse

by

M. Juliane Santiago

B.A., Clemson University, 1992

MMIS, Georgia College and State University, 1999

A Dissertation Submitted to the Graduate Faculty of Georgia Southern University in Partial Fulfillment of the Requirements for the Degree

Doctor Of Education

Statesboro, Georgia

2010

THE RELATIONSHIP BETWEEN SITUATIONAL CRIME PREVENTION THEORY AND CAMPUS EMPLOYEE COMPUTER MISUSE

By

M. JULIANE SANTIAGO

Major Professor: Teri Denlea Melton

Committee Members: Terry J. Smith
Barbara J. Mallory

Electronic Version Approved:
December, 2010

DEDICATION

With gratitude that is hard to express, I dedicate this dissertation to my husband, Marc. You've been there every inch of the way, and I love you more than anything.

I would also like to thank my parents, Tom and Margaret Whitehead, for their continuous encouragement and support.

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank the following people for their invaluable contributions to this study:

First and foremost, I would like to thank Dr. Teri Denlea Melton for her support throughout this entire process. As my dissertation committee chair, you provided constructive guidance that helped my study evolve into something I never dreamed I could do. However, you may not know that you also became a role model to me through your attitude, your teaching, and your professionalism.

Dr. Terry J. Smith, as my methodologist, challenged me more than anyone ever has in my academic career. I am indebted to you for your guidance and your standard of excellence that shaped my research from the beginning.

Dr. Barbara J. Mallory provided excellent editorial guidance. I am grateful to you for turning my dissertation into a body of work that shows a cohesiveness of ideas and is professionally expressed.

Dr. Wynne Chin graciously allowed me to use his excellent software, PLS-Graph, in the analysis of my data.

TABLE OF CONTENTS

LIST OF TABLES

Page

List of Tables (continued) Page

LIST OF FIGURES

Page

CHAPTER I

Introduction

In September of 2008, hackers accessed an inner computer system of one of the most expensive pieces of experimental machinery in history. With a price tag of over $8 billion, the Large Hadron Collider was designed to reveal the secrets of dark matter, anti-matter, and possibly even hidden dimensions of space and time. But, armed only with a keyboard, individuals calling themselves Group 2600 of the Greek Security Team were stopped just short of acquiring complete control of one of the key subsystems for the Collider (Keim, 2008). This type of infrequent, high-profile type of computer misuse captures the attention of the public, but computer misuse happens everyday, in thousands of companies worldwide.

In his landmark study of computer misuse, Straub (1990) defined computer misuse as "unauthorized and deliberate misuse of assets of the local organizational information system by individuals" (p. 257). Examples of misuse might include unauthorized network access, tampering with or stealing sensitive data, abusing e-mail privileges, or installing unlicensed software. It is important to note that computer misuse can be divided into two categories: misuse committed by an outsider; and, misuse committed by an insider. Though outsiders, or "hackers" receive the most press attention, it is insider misuse that costs companies in terms of lost revenue, productivity, and image (Computer Crime and Security Survey, 2008; Department for Business Enterprise and Regulatory Reform, 2007). Insider computer misuse can be further divided into two categories: misuse that is unintentional in nature and stems from a lack

of understanding about current policies and procedures; and, misuse that is intentional in nature (Kesar & Rogerson, 1998). Therefore, insider computer misuse can be committed through acts of software piracy, theft or destruction of sensitive data, release of malicious software, and misuse of email and/or Internet services.

Insider computer misuse is not confined to the business sector. College and university campuses also experience this type of computer misuse. In the 2006 survey of information technology (IT) security in higher education, Kvavik and Voloudakis (2006), working with the Educause Center for Applied Research (ECAR), found that 26% of responding campuses reported compromise of confidential information, and 12.5% reported damage to data. It should be noted that ECAR does not differentiate between insider and outsider computer misuse in their findings, but they do report that Baccalaureate and Associate's institutions are more concerned with unlicensed use of digital products and employees' misuse of computers, respectively. Further, in their study of college students, Cronan, Foltz, and Jones (2006) found that 34% of responding students admitted to software misuse or piracy, and 22% admitted to committing data misuse.

Additionally, campus administrators are faced with implementing an effective security plan within the confines of a relatively small IT security budget. Therefore, a well-targeted, cost-efficient and effective security plan is at the forefront of the battle against insider computer misuse on college campuses. Situational Crime Prevention, a theory from criminology, offers several factors that have the potential to assist administrators in creating an effective security plan. However, little, if any, research exists to establish the relationship of Situational Crime Prevention to the IT security field.

Many researchers have outlined various countermeasures to help combat insider computer misuse (Aldhizer, 2008; D'Arcy & Hovav, 2007; Harrington, 1996; Kesar & Rogerson, 1998). These countermeasures can be divided into two broad categories: technical controls, such as passwords and firewalls; and, formal or management-type controls, such as codes of ethics and acceptable use policies. Researchers agree that the most effective security plan includes elements from both categories of countermeasures (Dhillon & Moores , 2001; Straub, 1990; Willison & Backhouse, 2006).

An examination of computer security literature reveals three theories, all originating from the field of criminology, that have captured the attention of researchers: General Deterrence Theory, Rational Choice Theory and Situational Crime Prevention. While these three theories share some commonalities in their basic assumptions, there are significant differences in their focus.

The foundation of General Deterrence Theory is the assumption that punishment should be "certain, swift and proportionately severe" (Paternoster & Bachman, 2001, p. 14). The general assumption behind the theory is that people tend to use cost/benefit analysis when making any important decision, whether that decision is related to their career, a major purchase, or even a criminal act. This cost/benefit analysis may include factors such as the ease of committing a crime, the likelihood of getting caught, and the potential rewards of success. Unlike other theories in criminology, this theory specifically supports the belief that an appropriately harsh punishment that is sure to follow a crime will tilt the scales more toward the cost end of the spectrum, in effect, deterring an individual from committing a crime (Paternoster & Bachman).

While General Deterrence Theory focuses on factors that may deter someone from committing a crime due to the fear of punishment, the Rational Choice Theory focuses on decisions that criminals make during the commission of a crime (Cornish & Clarke, 1986). The assumption of Rational Choice Theory is the idea that people make the decision to commit a crime much like they make a decision in other mundane tasks, such as buying a television or a car, a process described by the expected utility model (Paternoster & Bachman, 2001). They weigh the costs and benefits of a given action and then make a decision. It is through the study of criminals' decision-making process that researchers can devise ways to make crime more costly to the criminal, thereby preventing criminal behavior by tilting the costs to outweigh the benefits of the criminal act.

Finally, Situational Crime Prevention Theory shares a theoretical underpinning with Rational Choice Theory, in that both theories do not try to explain the criminal, only the criminal act itself (Clarke, 1997). Situational Crime Prevention Theory attempts to prevent crime by altering various situational factors that influence a criminal's decision to commit a crime. The theory does not address the detection or sanctioning of offenders, nor does it address the reduction of criminal tendencies through social means; its goal is to make a criminal act less appealing to offenders.

Clarke (1997) outlined 16 "opportunity-reducing" techniques in his original Situational Crime Prevention Theory. These 16 techniques are grouped into four categories (Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Reward, and Remove Excuses) which impact a criminal's decision to commit a crime through either increasing the cost or reducing the benefit, or removing the justification for

commission.

Beebe and Rao (2005) took Clark's (1997) original crime opportunity-reducing techniques and applied them to the field of computer security, creating a comprehensive and more holistic set of countermeasures that consist of both technical and formal, management-type controls. Table 1 aligns Clarke's original 16 opportunity reducing technique with a typical traditional crime countermeasure and a corresponding computer misuse countermeasure (Beebe & Rao).

Table 1

Situational Crime Prevention Techniques as Applied to Traditional Crime and Computer Misuse

	Technique	Traditional Crime Countermeasure	Computer Misuse Countermeasure
Increase Perceived Effort	1. Target hardening	Locks, safes, fences, armed guards	Firewalls, closed ports, vulnerability patches
	2. Access control	Gate codes, guard shack, receptionist, swipe cards	ID/authentication systems, digital certificates
	3. Deflecting offenders	Pedestrian/auto traffic redirection, no loitering	Honeypots/honeynets, information segregation
	4. Controlling facilitators	Gun control, limit ability to communicate	Masking IP addresses, leased lines, no broadcast
Increase Perceived Risk	5. Entry/exit screenings	Metal detectors, screeners, merchandise tagging	Intrusion detection system, virus scanning
	6. Formal surveillance	CCTV, security guards, police patrols	Auditing and log reviews, anomaly detection
	7. Surveillance by employees	Responsibility and/or ability to monitor	Resource usage info, user training, reporting policies
	8. Natural surveillance	Lights, etc. so passers-by can see activity in the building	Tamper-proof network cabling, visualization tools
Decrease Anticipated Rewards	9. Target removal	Electronic donations vs. cash, cash diverted to safe	Information and hardware segregation, DMZ's
	10. Identifying property	VIN etched into auto glass, write name in book	Information classification, watermarking
	11. Reducing temptation	Obscure valuables, gender neutral phonebook	Minimize reconnaissance info, no port bannering
	12. Denying benefits	Security coded car radios, ink tags on clothing	Encryption, automatic data destruction mechanisms
Remove Excuses	13. Rule setting/clarification	Acceptable use policy, clear laws, licensing procedures	Acceptable use policy, user agreements, clear laws
	14. Stimulating conscience	"Shoplifting is stealing" signs, "current speed is"	Multi-level warning banners, codes of ethics
	15. Controlling disinhibitors	Controlling drugs/alcohol, propaganda, violent TV	Cyber-ethics education, supervised computer use
	16. Facilitating compliance	"Graffiti boards", public urinals, shelters, barriers	"Hacker challenges," employment opportunities

(adapted from Beebe & Rao, 2005)

Situational Crime Prevention has proven successful in reducing crime in many types of situations including aircraft hijackings, post office robberies, and bank robberies

(Clarke, 1997; Ekblom, 1988; Gabor, 1990; Grandjean, 1990; Wilkinson, 1986). Its effectiveness in the field of computer security, however, has yet to be established, though the potential for success in reducing computer misuse is very promising. The theory's straightforward focus on situational factors that can prevent criminal behavior and, in a computer security setting, its holistic approach to technical and formal, management-type controls, offers an adaptable security plan that may be used to reduce insider computer misuse in many situations.

Implementation of any type of IT security in higher education is challenging. There is a constant struggle between an IT security specialist's need to implement a strong security plan and academia's need to exchange ideas and encourage exploration (Oblinger, 2003). Therefore, a higher education campus offers a unique setting to explore the relationship between Situational Crime Prevention and insider computer misuse, such as software piracy and inappropriate email and/or Internet usage. Additionally, much of the prior research on misuse countermeasures has focused on insider computer misuse in the business environment, leaving college campus employees a relatively unstudied group.

Statement of the Problem

Computer misuse is a leading problem for all industry sectors, including colleges and universities. Though many researchers have proposed different countermeasures to combat the problem, there is no clear solution. It could be argued that many of the countermeasures found in the literature are too one-sided; some countermeasures focus completely on technical countermeasures, such as passwords and firewalls, to the exclusion of administrative controls, such as a clearly stated Acceptable Use Policy, or

vice versa. A combination of the two types of countermeasures might prove to be the most effective solution.

Situational Crime Prevention Theory outlines a number of technical and administrative countermeasures to prevent insider computer misuse. When applied to the field of information technology, a more holistic approach to preventing insider computer misuse emerges. However, to date, there is no study in either the business environment or higher education environment regarding the relationship between Situational Crime Prevention and insider computer misuse.

Purpose Statement

The purpose of this study was to explore the relationship between the categories of countermeasures in Situational Crime Prevention Theory and the number of insider computer misuse incidents on college campuses.

College and university campuses are not immune to computer misuse incidents. Often, their information technology security budgets are smaller than most business budgets, necessitating use of the most effective security countermeasures. The researcher explored the above relationships as an effort to help campus IT departments choose the most efficient and effective security countermeasures. From this data, the researcher responded to the following research questions.

Research Questions

R_1 – To what extent are the countermeasures that increase the perceived effort to commit insider computer misuse related to the number of insider computer misuse incidents on campus?

R_2 – To what extent are the countermeasures that increase the perceived risk of committing insider computer misuse related to the number of insider computer misuse incidents on campus?

R_3 – To what extent are the countermeasures that decrease the anticipated reward for committing insider computer misuse related to the number of insider computer misuse incidents on campus?

R_4 – To what extent are the countermeasures that remove the excuses for committing insider computer misuse related to the number of insider computer misuse incidents on campus?

R_5 – What are the respondents' top five countermeasures in terms of perceived effectiveness?

Figure 1 shows the conceptual framework model, including independent and dependent constructs, and labeled research questions.

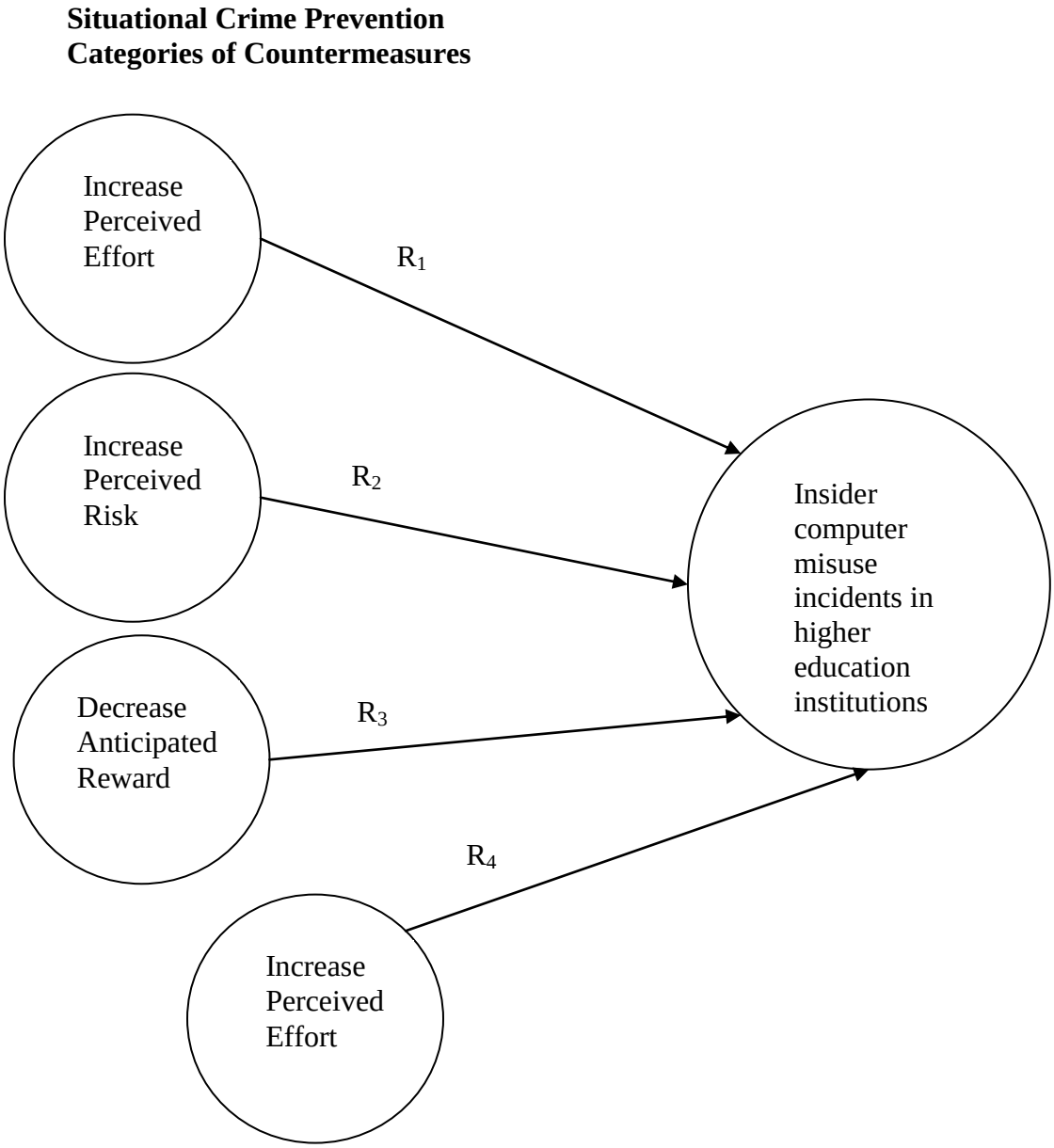

Figure 1: Conceptual Framework with Labeled Research Questions

Significance of the Study

The number of reported computer misuse incidents continues to be unacceptably high in industry surveys, both in the United States and the United Kingdom (Computer

Crime and Security Survey, 2008; Department for Business Enterprise and Regulatory Reform, 2007). Losses from computer misuse incidents can be categorized as monetary losses, often as much as hundreds of thousands of dollars, productivity losses, and damage to an institution's reputation if sensitive information is leaked. Despite the pervasive reports of security-related and computer misuse incidents, no one method or combination of methods, has proven consistently effective in preventing these incidents of misuse (Aldhizer, 2008; D'Arcy & Hovav, 2007; Harrington, 1996; Kesar & Rogerson, 1998; Straub, 1990). Additionally, most published research related to the prevention of computer misuse has concentrated on the business sector, not colleges and universities.

It was posited that the current research would provide empirical evidence for Situational Crime Prevention's application in the field of computer security within higher education. The data may yield the identification of effective countermeasures, thereby providing a roadmap for institutions seeking an effective plan for preventing computer misuse. An effective, well-targeted security plan should reduce the costs associated with incidents of computer misuse and the costs of plan implementation. While this reduction in cost should benefit all business sectors, it should be especially important to colleges and universities whose resources may be more limited.

In addition to the implications for reducing cost, data from the current research have implications for leaders in higher education in terms of security policy. Educational leaders in the area of IT security face an unprecedented amount of pressure to ensure the confidentiality of personal data and offer an extremely high level of system availability.

While an effective security plan will support both of these requirements, it is security policy that will ultimately drive the security plan.

Procedures

This correlational study was conducted using a quantitative approach. The target population was public four-year colleges and universities throughout the United States. Respondents were the Chief Information Officer (CIO) or an administrator of equivalent responsibility at each institution. Because of the large target population and the sensitive nature of reporting computer security and computer misuse information, an anonymous, web-accessible questionnaire was deemed the best method to collect data.

The researcher-developed instrument included questions related to the security measures in place at each college or university and the number of known insider computer misuse incidents in the last year. Additionally, data were collected regarding the CIO's top five countermeasures in terms of perceived effectiveness. Following IRB approval, a pilot test involving eight colleges and/or universities was performed to ensure face validity and that the questionnaire wording and definitions were clear to the respondents. The questionnaire was edited and invitations were sent to 442 CIO's. Resulting questionnaire data were analyzed using PLS Graph software. PLS Graph utilizes structural equation modeling using a partial least squares approach. Because PLS Graph places minimal demands on criteria such as sample size, it is an appropriate choice for theory confirmation in exploratory studies (Chin, 1998). Incomplete questionnaires were discarded.

Limitations and Delimitations

The researcher identified the following limitations of the study. Due to the sensitive nature of computer security incidents, respondents may be reluctant to share that information, and/or to be open and honest. However, the anonymity of the administration of the instrument helped to mitigate this limitation. Additionally, the questionnaire instrument was researcher-developed, and the researcher is making the assumption that the instrument measures what it proposes to measure. To lessen the effects of this limitation, a pilot test was performed to ensure face validity, and discriminant validity was completed. A final limitation was the use of categories to summarize the reported computer misuse incidents. To date, there is no set standard for the categorization of computer misuse incidents.

The study was delimited to include all public four-year institutions of higher education within the United States. Of 653 public four-year institutions, the researcher identified 442 CIO contact names and emails.

Definition of Key Terms

Computer misuse - Based on Straub's (1990) definition, this study defines computer misuse as the unauthorized and deliberate misuse of an organization's computer resources, including: hardware (computers, servers, storage devices and peripheral devices); software (theft and/or illegal copying); data (theft and/or modification or destruction of data); and, service (use of email or Internet access for non-work related activities). For the purposes of this study, computer misuse will be measured by the number of incidents in the last 12 months that each CIO reports on the survey.

Countermeasures – Based upon definitions found in the literature, countermeasures are the broad groups of controls that are utilized to guard against computer misuse (Backhouse & Dhillon, 1995; Dhillon & Moores, 2001; Dhillon, Silva, & Backhouse, 2004; Hoffer & Straub, 1994).

Insider - For the purposes of this study, an insider is a current or former employee of a college or university.

Insider computer misuse – For the purposes of this study, insider computer misuse is misuse of computer resources by a current or former employee of a college or university.

Public four-year college/university – For the purposes of this study, a public four-year college/university is an institution of higher education that is supported primarily by public funds and offers programs of at least four years duration or one that offers programs at or above the baccalaureate level.

Chapter Summary

Though high-profile computer security misuse, such as the attack on the Large Hadron Collider, is relatively infrequent, computer misuse committed by insiders is an ongoing problem that occurs every day and in every industry. Computer misuse is not simply a nuisance for administrators; consequences of insider computer misuse can range from damage to a company's reputation to considerable financial losses. Colleges and universities can be particularly vulnerable to these incidents because their IT security budgets may be smaller than most business' budgets and can, therefore, implement only the most cost-efficient and effective security countermeasures.

Situational Crime Prevention, a theory originating in criminology, outlines a number of technical and administrative countermeasures to prevent crime. When applied to the field of computer security, a more holistic and potentially effective approach to preventing insider computer misuse emerges. Situational Crime Prevention's relationship to insider computer misuse, however, has yet to be empirically explored.

Therefore, the purpose of this correlational study was to explore the relationship between the categories of countermeasures inherent in Situational Crime Prevention Theory and the number of known computer misuse incidents on college campuses. The researcher-developed instrument included questions related to the countermeasures in place at each college or university, the CIO's top five countermeasures in terms of perceived effectiveness, and the number of known insider computer misuse incidents in the year 2009.

A pilot test of eight colleges and/or universities was performed to ensure face validity and that the instrument questions were worded clearly. The target population was current CIO's or administrators of equivalent position within public four-year institutions of higher education in the United States. The questionnaire was made electronically available via the web. Data analysis was completed using PLS Graph. It was posited that the study has implication for higher education institutions in the creation of appropriate security policy to drive the most effective and cost-efficient security plan possible.

CHAPTER II

REVIEW OF LITERATURE

Introduction

The infiltration of an inner computer system of the Large Hadron Collider, an $8 billion piece of experimental machinery, captured worldwide attention in September of 2008. Armed only with a keyboard, individuals calling themselves Group 2600 of the Greek Security Team were stopped just short of acquiring complete control of one of the key subsystems for the Collider (Keim, 2008). This type of infrequent, high-profile exploit captures the attention of the public, but computer misuse happens everyday, in thousands of companies worldwide.

As this study sought to explore the issue of insider computer misuse within higher education, it is important to study computer misuse as a general area of research in the field of information technology and then frame the topic within higher education. Though higher education institutions face many of the same issues as business institutions, the topic of culture within higher education becomes an important issue, even within the field of computer misuse. Finally, an examination of three criminological theories often applied to computer misuse was presented.

Computer Misuse as a Pervasive Problem

In his landmark study of computer misuse, Straub (1990) defined computer misuse as "unauthorized and deliberate misuse of assets of the local organizational information system by individuals" (p. 257). Examples of misuse might include unauthorized network access, tampering with or stealing sensitive data, abusing e-mail

privileges, or installing unlicensed software. Though the field of information security has made progress in combating misuse, statistics show that the problem has not been curtailed and, in many cases, is still increasing. The Computer Security Institute distributed its Computer Crime and Security Survey (2008) to over five thousand computer security professionals in corporations, government agencies, financial institutions, medical facilities, and universities in the United States. Findings indicated that the average annual loss related to each incident of computer misuse was close to $300,000. Forty-three percent of respondents reported at least one security-related incident in the year 2008. Of these 43%, 49% of companies experienced a virus incident, and 46% of companies reported at least one incident of insider network misuse.

The Department for Business Enterprise and Regulatory Reform (2007) in the United Kingdom performed a security survey very similar to the Computer Security Institute. The methodology consisted of a structured questionnaire given by telephone survey to the person responsible for information security at randomly chosen businesses in the United Kingdom. The Department also considered the fact that the majority of businesses in the United Kingdom tend to be small in size. In order to provide equal representation for large size businesses, the Department chose to boost the sample for this group and weight the results. In total, 1,007 interviews were completed. The percentage of companies that reported a serious security-related incident in 2006 was 45% for small companies (less than 50 employees), 72% for large companies (greater than 250 employees), and 96% for very large companies (greater than 500 employees).

These incidence figures from the United States and United Kingdom are significant in two ways. First, the reported figures may be underrepresented because

many companies choose not to report computer misuse incidents due to the possibility of negative publicity (Hoffer & Straub, 1994). Second, the figures from the United Kingdom show a marked increase in security-related incidents in relation to company size. It could be that the larger companies pose a more lucrative target for a hacker, or outsider, seeking access to sensitive or financial data. More likely, however, it is the employee, or insider, that is committing the computer misuse. The Computer Security Institute's 2007 survey showed that insider misuse accounted for 59% of security incidents, and the Institute's 2008 survey showed that insider misuse accounted for 44% of security incidents.

Computer misuse can be divided into two categories: misuse committed by an outsider and misuse committed by an insider. Though the outside "hacking" incidents receive the most press attention, insider computer misuse accounts for a significant percentage of losses experienced each year. Statistics from both the Computer Security Institute's 2008 survey and the United Kingdom's Department for Business Enterprise and Regulatory Reform's 2007 survey support this assertion. While the most prevalent problem reported was virus infiltration, the second-most most prevalent security problem reported by the Computer Security Institute's survey was insider misuse, including e-mail misuse, trafficking pornography or pirated software, and unauthorized network access. The United Kingdom survey reported that 47% of large companies suffered some type of employee misuse of computer resources, with misuse of web access and email reported the most often.

Further, Fortiva, Inc. (2005) reported that 68% of U.S. employees who normally use email at work have sent or received at least one inappropriate email using their work

account. Though most people do not think that sending or receiving inappropriate email can have serious consequences for a company, Chevron Corporation was ordered to pay over $2 million to female employees in settlement of a sexual harassment lawsuit that originated with an inappropriate email that was circulated by male employees (Verespej, 2000).

The evidence shows that insider computer misuse is a problem. The next question becomes how to combat it.

Discussion of Countermeasures

Insider computer misuse is not a new phenomenon, and numerous studies have addressed the problem and discussed recommended countermeasures. When examined holistically, the countermeasures fall into two overall categories: technical controls and administrative controls.

Technical Countermeasures

Technical countermeasures are those controls which often are technology-based. The most common countermeasures found in the literature include authentication for resource access, monitoring software, and data access control using security levels (Aldhizer, 2008; D'Arcy & Hovav, 2007; Panko & Beh, 2002; Straub, 1990; Urbaczewski & Jessup, 2002). Authentication involves the appropriate use of a username and password combination in order to control access to a network or data. Monitoring software could be in the form of email filtering and monitoring for offensive words, or Internet surfing monitoring to ensure that employees do not access or download offensive material. Data access control involves classifying data according to its sensitivity and then assigning rights to those employees who can access it.

Data from the Computer Security Institute's 2008 survey supports the presence of these common technical controls. Following are some of the most common types of technical countermeasures to deter computer misuse followed by the percentage of companies that utilized them: account login and password: 46%; log management software: 51%; web monitoring software: 49%; and, email monitoring software: 49%. Table 2 below outlines some of the most common technical countermeasures to combat insider computer misuse with a corresponding reference in the literature. It should be noted, however, that the reference list is not meant to be exhaustive as the most common countermeasures are mentioned countless times in computer security literature.

Table 2

Common Technical Countermeasures with Corresponding Reference

Countermeasure	**Reference**
Firewalls	Beebe & Rao, 2005; Computer Security Institute, 2008; Johnson & Ugray, 2007; Kvavik & Voloudakis, 2006; Pfleeger & Pfleeger, 2007
Physical security	Beebe & Rao, 2005; Pfleeger & Pfleeger, 2007; Straub & Welke, 1998
Authentication*	Kvavik & Voloudakis, 2006; Pfleeger & Pfleeger, 2007; Straub & Welke, 1998
Kerberos*	Pfleeger & Pfleeger, 2007
Access control lists*	Kankanhalli, Teo, Tan & Wei, 2003; Pfleeger & Pfleeger, 2007
Proxy servers*	Pfleeger & Pfleeger, 2007
Virus scanning	Beebe & Rao, 2005; Computer Security Institute, 2008; Pfleeger & Pfleeger, 2007
Login/logout rules and procedures*	Pfleeger & Pfleeger, 2007
Email monitoring software*	Johnson & Ugray, 2007; Phyo & Furnell, 2004
Web usage monitoring software*	Johnston & Ugray, 2007; Phyo & Furnell, 2004
Database partitioning and use of data views*	Kankanhalli, Teo, Tan & Wei, 2003; Pfleeger & Pfleeger, 2007
Data sensitivity classification	Beebe & Rao, 2005
Auditing and log reviews	Beebe & Rao, 2005; Kvavik & Voloudakis, 2006; Phyo & Furnell, 2004
Review of resource information	Beebe & Rao, 2005
Cameras in data sensitive areas and/or video surveillance*	Booker & Kitchens, 2010; Hu, Tan, Wang & Maybank, 2004
Automatic data destruction	Beebe & Rao, 2005
Virtual Private Networks*	Computer Security Institute, 2007; Kvavik & Voloudakis, 2006; Pfleeger & Pfleeger, 2007
Encryption	Computer Security Institute, 2007; Beebe & Rao, 2005; Kvavik & Voloudakis, 2006; Pfleeger & Pfleeger, 2007
Network packet shaping*	Phyo & Furnell, 2004
Controlled distribution of software*	Kvavik & Voloudakis, 2006
Screen saver lock*	USDA security policies, n.d.

* countermeasure added by researcher

Though no one can refute the importance of technical security controls, many authors reflect upon the propensity of some companies to rely solely on these technical countermeasures (Osborne, 1998; Parker, 1997; von Solms, 2001). With a complete emphasis on technical controls, the problem of computer misuse becomes very one-sided, and the holistic nature of computer security is lost. The other side of the security coin is the presence of administrative controls, such as codes of ethics and employee security awareness training.

Administrative Countermeasures

Administrative countermeasures are not necessarily based on technology; they are rooted more in policy, ethics, and training. The field of ethics is an integral part of the study of insider computer misuse, and many companies put their faith into codes of ethics and acceptable use policies. These companies might also participate in employee security training. The Computer Security Institute's 2008 survey found that 82% of companies provide some type of awareness training for their employees. The United Kingdom's Department for Business Enterprise and Regulatory Reform's 2007 survey shows that 55% of companies surveyed have a documented security policy, and 40% provide employee security training. It also appears that 86% of large businesses surveyed provided an acceptable use policy to their employees. However, there is controversy over the effectiveness of acceptable use policies and codes of ethics without the presence of technical controls. Harrington (1996) did not find a uniform relationship between codes of ethics and computer misuse judgments and intentions of information systems employees. It appeared that, overall, the presence of a code of ethics did not greatly impact employees intentions to commit misuse. Similarly, von der Embse, Desai, and

Desai (2004) found that ethical codes and policies simply do not effectively guide ethical behavior. Table 3 shows some of the more common administrative or formal countermeasures with corresponding references in the literature. Like the technical countermeasures described previously, many countermeasures are mentioned in countless articles and textbooks. Therefore, the reference list provided here is not meant to be exhaustive.

Table 3

Common Administrative Countermeasures with Corresponding Reference

Countermeasure	**Reference**
Presence of and dissemination of Codes of Ethics, Acceptable Use Policies, User Agreements, Misuse Reporting Policies, and/or Internet Use Policies	Beebe & Rao, 2005; D'Arcy, Hovav & Galletta, 2009; Dhillon & Moores , 2001; Dominguez, Ramaswamy, Martinez & Cleal, 2010; Harrington, 1996; Johnson & Ugray, 2007; Straub, 1990
Supervised computer use	Beebe & Rao, 2005
Cyber-ethics education	Beebe & Rao, 2005
Clearly defined job duties and/or rules*	Backhouse & Dhillon, 1995; Dhillon & Moores, 2001
Password policies*	Pfleeger & Pfleeger, 2007; Straub & Welke, 1998
Required training for all new users*	Straub & Welke, 1998
Offer software to employees at reduced prices*	Chiang & Assane, 2002

* countermeasure added by researcher

Combination of Technical and Administrative Countermeasures

In order to implement the most effective security plan possible, there must be both technical controls and administrative-type controls in place. Many institutions choose to implement acceptable use polices or codes of ethics to enhance the effectiveness of deterring insider computer misuse through technical controls. Straub (1990) found that, in addition to technical controls, the process of informing users of what constitutes unacceptable computer behavior and the corresponding penalties for said misuse in

addition to computer awareness training sessions are effective deterrents. Similarly, Dhillon and Moores (2001) advocated the use of technical controls, such as controlling access to computer systems, in addition to written policies and employee security training and education. Willison and Backhouse (2006) compared effective security to a house of cards. Neglect in any one area will impact another area and possibly create an opportunity for misuse; thereby, reinforcing the need for a more cohesive approach involving both technical and policy controls.

With researchers demonstrating the effectiveness of a two-sided defense consisting of technical controls and policies against employee computer misuse, why does computer misuse still occur? The answer is that people, their behavior, and their motivations are at the heart of computer security, and what works in the business environment may be completely inappropriate and/or ineffective in higher education.

Computer Security in Higher Education

The studies and surveys mentioned so far originated within the business environment. A search of the literature revealed only two studies related to computer security in higher education. Kvavik and Voloudakis, through the Educause Center for Applied Research, surveyed higher education institutions within the United States and Canada regarding the state of computer security on their campuses (2006). Twenty-six percent of respondents reported compromise of confidential information, and 12.5% reported damage to data. It should be noted that Kvavik and Voloudakis do not differentiate between insider and outsider computer misuse in their findings, but they do report that Baccalaureate and Associate's institutions are more concerned with unlicensed use of digital products and employees' misuse of computers, respectively. Further, in

their study of college students, Cronan, Foltz, and Jones (2006) found that 34% of responding students admitted to software misuse or piracy, and 22% admitted to committing data misuse.

With the exception of Kvavik and Voloudakis' 2006 study and Cronan, Foltz, and Jones' 2006 study, computer security in higher education has been relatively unstudied. This could be due to the idea that effective implementation of computer security is difficult in a higher education setting, mainly due to environment and culture.

Higher Education Culture

With its roots in the early 1800's, the Germanic notion of academic freedom has permeated the culture of American higher education. One definition of academic freedom is "freedom for students to choose their own studies and freedom for professors to study and teach what they would [choose]" (Cohen, 1998, p. 128). Wolff (1969) probably best summed up the culture ideal of higher education institutions:

> [T]he fundamental purpose of this community (the university) is the preservation and advancement of learning and the pursuit of truth in an atmosphere of freedom and mutual respect, in which the intellectual freedoms of teaching, expression, research, and debate are guaranteed absolutely. (p. 131)

Though Wolff's views are, indeed, a cultural "ideal," the tenants of academic freedom juxtaposed against higher education taking on a more bureaucratic and business-like atmosphere are a reality, a trend that is expected to only increase in the future within the topic of accountability of higher education. As long as colleges and universities receive public funds, they will be expected to not only provide proof that specific outcomes have been attained, but that the attainment of those outcomes have been made in the most

efficient manner possible (Berdahl & McConnell, 1999). These demands represent the growing influence of business and industry on higher education, with the subsequent rules and procedures that follow. The constant battle between the ideal of academic freedom and the growing demand for business-like operations creates an environment that is inherently difficult for computer security professionals. Computer professionals would prefer to not allow anyone to install software on university computers or allow no off-campus access to the internal network, but university professors demand some type of autonomy regarding their classrooms and how they choose to work. From an organizational culture standpoint, this situation often creates subcultures within a college or university campus. These subcultures then create their own set of rules and practices that are not always in line with the larger university policy (Keup, Walker, Astin, & Lindholm, 2001).

Change is another factor to consider in a discussion of culture in higher education. Higher education is likely to include students from a very diverse population. This diverse population is likely to include students and employees of differing age, ethnicity, culture, and diverse learning needs (VanPatten, 2000). In most situations, this diversity can only enrich a campus' culture. But the needs of computer security are different; computer security craves a homogeneous environment as it is easier to control. There is a constant struggle between a computer security specialist's need to implement a strong security plan and academia's need to exchange ideas and encourage exploration (Oblinger, 2003).

A discussion of change in higher education is not complete without a discussion of technology. The availability of technology has created learning experiences that were

previously impossible. Consider a professor who conducts class from a classroom on a university's main campus but through the use of teleconferencing equipment and software, that lecture is broadcast to multiple classrooms at satellite campuses across the state, possibly across the globe. Students and faculty have access to untold amounts of research on the Internet. Technology is so ubiquitous that a full discussion of its application in higher education is beyond the scope of this research. Suffice it to say that technology has brought about numerous opportunities in higher education but, with these opportunities, come challenges, as well (Gumport & Chun, 1999). Challenges come in the form of controlling the technology: providing access while limiting inappropriate activities, providing software for learning while limiting piracy, and providing resources for faculty and staff to do their jobs while limiting misuse of those resources.

Though higher education campuses face some unique challenges when it comes to combating insider computer misuse, lessons can be learned by studying computer misuse in the business world. An even richer understanding comes from studying the problem from a criminological standpoint.

Computer Misuse from a Theoretical Perspective

Computer misuse, whether the misuse in question actually violates any laws, appears to mimic most types of crimes. There is the intent to commit misuse, weighing of costs and benefits, and the potential for punishment. Though most of the current research focuses on the technologies used to combat computer misuse, in order to learn more about the behavior of an employee who commits computer misuse, it is useful to look at the field of criminology and examine three theories that have been applied to the

research within computer security. These theories are: General Deterrence Theory, Rational Choice Theory, and Situational Crime Prevention.

General Deterrence Theory

The foundation of General Deterrence Theory is the idea that punishment should be "certain, swift and proportionately severe" (Paternoster & Bachman, 2001, p. 14). The roots of these attributes can be traced back to the writings of Cesare Beccaria who wrote an essay on penal reform entitled *Essay on Crimes and Punishments* during 18th century Italy (1985/1764). Through his essay, Beccaria (1985) hoped to reform the current legal system which was riddled with obscure laws, no uniform system of sentencing, and harsh and often cruel punishments. Beccaria posed the idea that punishment for crimes should be swift and certain, and only be harsh enough to deter someone from actually committing a crime. It is the certainty of punishment that is far more effective than the harshness of it. This idea appeals to human's natural sense of rationality. People tend to use cost/benefit analysis when making any important decision, whether that decision is related to their career, a major purchase, or even a criminal act. The idea that an appropriately harsh punishment is sure to follow a crime will tilt the scales more toward the cost end of the spectrum and effectively deter an individual from committing a crime (Paternoster & Bachman). It is this dependence upon swift, certain and appropriately harsh punishment that can cause General Deterrence Theory to lose its effectiveness in practice.

Empirical criminology research has shown that there is a modest relationship between crime rates and appropriately harsh punishment (Gibbs, 1975; Nagin, 1978). However, the evidence for a relationship between certain, observed punishment and

crime rates proved to be a bit stronger. The reasoning for this effect is fairly straightforward. Someone who is contemplating committing a crime must be fairly certain that he/she will be caught in order for deterrence to work. Moreover, if a criminal knows that a friend committed a crime and was not caught or punished, the credibility of the deterrent nature of punishment is eroded (Paternoster & Bachman, 2001).

Other researchers in the field of criminology have expanded General Deterrence Theory to include not only formal sanctions for committing a crime (i.e. incarceration and/or fines) but also informal sanctions such as disapproval from friends, co-workers, or a spouse (Anderson, Chiricos, & Waldo, 1977; Grasmick & Green, 1980; Nagin & Paternoster, 1991; Paternoster, Saltzman, Waldo, & Chiricos, 1983; Williams & Hawkins, 1986). Expanding the definition of punishment to include any negative consequence allows the possible application of General Deterrence Theory to many situations, including computer misuse, as many forms of computer misuse are not illegal, thereby eliminating the possibility of legal sanctions for their commission. Additionally, other researchers have found that crime rates decrease with the corresponding increase of police presence, thereby increasing the certainty that a criminal will be caught (Levitt, 1996; Marvell & Moody, 1994). If people know they are being watched, or "policed," they are much less likely to commit a crime.

General Deterrence Theory has often been applied in the field of computer security. Straub (1990) outlined the need for informing users about unacceptable computer usage and the penalties for noncompliance, along with the appropriate and consistent enforcement of these policies. In addition to the effectiveness of outlining acceptable use policies and corresponding penalties, Straub found that the number of

hours per week dedicated to data security by information systems personnel, as well as the use of software that monitors employees' activity, had a significant impact on employee computer misuse. This finding supports the deterrence approach of policing.

Harrington (1996) outlined the idea that codes of ethics take the place of laws within organizations. Even without the presence of formal or informal sanctions, it is possible that the very presence of a code of ethics and the dissemination of its contents suggests negative consequences will occur in the event of a violation (Tittle, 1980). Harrington's study, however, revealed that codes of ethics are generally ineffective deterrents for computer misuse, with information systems-specific codes only slightly more effective at deterring sabotage. One interesting finding of this study is that codes of ethics are effective in deterring those employees who possess a low degree of response deniability. Response deniability involves to what degree a person takes responsibility for his/her own actions. Therefore, someone with low response deniability generally accepts responsibility and lives up to moral commitments.

A third study that applied a slightly modified version of General Deterrence Theory reported results that were contrary to several previous studies (D'Arcy, Hovav, & Galletta, 2006). The authors proposed that user awareness of security countermeasures impacts their perceptions of the certainty and severity of punishment for computer misuse, thereby affecting information systems misuse intentions. In direct contrast to Gibbs (1975) and Nagin (1978), this study found that perceived severity of sanctions had a much greater influence on user intention to commit misuse than perceived certainty of sanctions. Also, in direct contrast to Harrington (1996) is this study's finding that the

presence of a security policy is an effective deterrent to employee computer misuse because these policies can increase users' perceptions of punishment severity.

In a follow up study, D'Arcy, Hovav, and Galletta (2009) surveyed 269 computer users in eight companies regarding user awareness of security countermeasures. They found that three practices deter misuse: user awareness of security policies; security education, training, and awareness programs; and, computer monitoring. Further, their results showed that the perceived severity of sanctions was more effective in deterring computer misuse than the certainty of sanctions.

The lack of consensus among research studies in the field of General Deterrence Theory reveals the difficulty in finding one deterrence that applies to criminal behavior due to the variance in personalities and behaviors that are innate within human beings. Adding to this complexity is the fact that many people who commit computer misuse, specifically hackers, feel they are simply pointing out a weakness to a company or that harming a company is vastly different than harming another person (Conger, Loch, & Helft, 1995; Hafner & Markoff, 1991; Krauss & MacGahan, 1979; Parker, 1989; Samuelson, 1989). Finally, companies are often reluctant to pursue people who violate laws because of the fear of negative publicity. This is supported by the Computer Security Institute's 2008 survey which found that only 27% of businesses who experienced a security incident actually reported it to the police. Additionally, the survey reported that only 60% of companies attempted to identify the perpetrator. These two factors undermine the reliance of General Deterrence Theory on swift, certain and appropriately harsh penalties.

Rational Choice Theory

While General Deterrence Theory focuses on the factors that can successfully deter someone from committing a crime, the Rational Choice Theory focuses on the decisions that criminals make during the commission of a crime. Rational Choice Theory presents the idea that people make the decision to commit a crime much like they make a decision in other mundane tasks such as buying a television or a car, a process described by the expected utility model (Paternoster & Bachman, 2001). Even when faced with uncertain conditions and without all necessary information, human beings choose an outcome that will be the most favorable for them. This decision-making process is described in a model known as the subjective utility model (Paternoster & Bachman). In the subjective utility model, it is not assumed that humans can gather, store, and process information perfectly; rather, they weigh the costs and benefits of their actions in order to make the most beneficial decision they can. Even though humans go through the process of gathering and processing information, it does not mean that they make good decisions, nor does it mean that their interpretation of the world around them is correct (Cornish & Clarke, 1986).

Cornish and Clarke (1986), within their subjective utility theory, described criminals as modestly rational and contend that they often perform some type of planning during their decision to commit a crime. It is important to note that the planning process for robbing a convenience store is vastly different than the process for stealing a car. The perceived benefits for each of the two aforementioned crimes are vastly different, as well. It is through the study of criminals' decision-making process that researchers can devise

ways to make crime more costly to the criminal, thereby preventing a crime from occurring.

Another important aspect of Cornish's (1994) research on the Rational Choice Theory is crime scripts. Originating in Gardner's (1985) study of the field of cognitive science, crime scripts describe the steps necessary to commit a crime. An example of a subway mugging script is shown below in Table 4. The procedural stages of the crime are listed under the "Scene/Function" heading and the behavior is listed under the "Script Function" heading.

Table 4

Subway Mugging Script

Scene/Function	**Script Function**
Preparation	Meet and agree on hunting ground
Entry	Entry into underground system
Pre-Condition	Travel to hunting ground
Pre-Condition	Waiting/circulating at hunting ground
Instrumental Pre-Condition	Selecting victim and circumstance
Instrumental Initiation	Closing-in/preparation
Instrumental Actualization	Striking at victim
Instrumental Actualization	Pressing home attack
Doing	Take money, jewelry, etc.
Post-Condition	Escape from scene
Exit	Exit from system

(Cornish, 1994)

The use of scripts has been quite useful in the field of criminology to model the commission of various crimes from check fraud to the stealing of cars for resale (Lacoste & Tremblay, 2003; Tremblay, Talon, & Hurley, 2001). Because computer crime or misuse involves some type of planning and a systematic method, the Rational Choice Theory and the use of scripts are appropriate vehicles for the study of this category of crime.

Just as breaking down a programming problem into individual steps of an algorithm can help a programmer create a program, breaking down the steps needed to commit a particular type of computer misuse can help the information systems security specialist define appropriate countermeasures. Using the details outlined in the 1998 U.K. Audit Report (Audit Commission, 1998), the crime outlined in the crime script in Table 5 below shows the steps taken by a council employee who committed computer fraud. Because his colleagues would often leave their computers unlocked during their absence, the council employee simply accessed their computers and processed £15,000 of fraud using fictitious invoices (Willison, 2006).

Table 5

Computer Fraud Script

Scene/Function	Script Function
Preparation	Gaining access to the organization
Entry	Already an employee with access
Pre-Condition	Wait for employees to leave their offices
Instrumental Pre-Condition	Access the unattended computers
Instrumental Initiation	Access the application needed to falsify invoices
Instrumental Actualization	Create false customer accounts
Doing	Authorization of fictitious invoices
Post-Condition	Exit the application
Exit	Exit the system

(adapted from Willison, 2006, p. 318)

Situational Crime Prevention Theory

Closely related to Rational Choice Theory is Situational Crime Prevention Theory, developed by Clarke (1997), a theory which also focuses on the decision-making process a would-be perpetrator goes through when deciding to commit a crime, but adds situational factors that might influence a criminal's decision to commit a crime. The main difference between Rational Choice Theory and Situational Crime Prevention Theory is that the latter focuses on the environmental factors that contribute to certain types of crime.

Situational Crime Prevention Theory has roots in research conducted during the 1960's and 1970's by the Home Office Research Unit, Britain's governmental criminological research department (Clarke & Cornish, 1983). In the course of researching different methods to reduce crime, it became apparent that opportunity reduction showed promise and warranted further investigation. For example, researchers found that the probability of a youth re-offending while residing at a probation hostel or training school was significantly reduced by addressing the opportunities for misbehavior in the institutional environment itself, and not necessarily addressing factors such as the youth's background or personality (Tizard, Sinclair, & Clarke, 1975).

Though a focus on opportunity reducing factors is not consistent with most current criminological research, support for this viewpoint is found in earlier studies. Burt (1925) found that longer hours of darkness in winter promoted higher incidence of property offending. Further, Hartshorne and May (1928) found that dishonest behavior in children is related to the amount of supervision they experience.

Psychological research in the area of personality traits also supports the inclusion of situational factors within the study of deviance. Overall, this research showed that criminal behavior was influenced by environmental factors such as opportunity and inducements rather than traditional dispositional factors (Briar & Piliavin, 1965; Matza, 1964; Short & Strodtbeck, 1965) .

From this body of research and additional research in the study of problem-oriented policing, the Rational Choice Theory, as discussed previously, emerged (Clarke & Cornish, 1985; Cornish & Clarke, 1986). It is through the combination of elements of Rational Choice Theory and elements of Routine Activity Theory that Situational Crime

Prevention Theory emerged. Routine Activity Theory, though not normally used to explain computer crime, is an important theory in explaining the opportunity portion of crime commission.

Situational Crime Prevention does not attempt to provide a panacea for the elimination of all types of crime. Rather, it encompasses three measures that "(1) are directed at highly specific forms of crime, (2) involve the management, design or manipulation of the immediate environment in as systematic and permanent way as possible, (3) make crime more difficult and risky, or less rewarding and excusable as judged by a wide range of offenders" (Clarke, 1997, p. 4).

Likely without realizing it, many people incorporate Situational Crime Prevention into their everyday lives. People lock their doors when leaving their homes; they install burglar alarms; and, tell their children not to talk to strangers (Clarke, 1997). It is within this realm that Situational Crime Prevention operates, but with a highly targeted focus. Due to differences in certain environmental or situational factors, the same measures would not be used to combat both a convenience store robbery and a home robbery.

Most criminological theories focus on the offender and his/her motivations, which are variable. Likewise, when these traditional theories are moved into the area of computer security, their application becomes much more complex. The motivations of those who misuse computers can vary greatly, as can their knowledge and skills. Several researchers have developed taxonomies to describe the numerous types of computer criminals or hackers (Hollinger, 1988; Landreth, 1985; Smith & Rupp, 2002). In direct contrast to the more traditional criminology theories, Situational Crime Prevention does

not attempt to explain criminal behavior or motivations. It simply attempts to make a crime less attractive to a criminal.

In his early development of the theory, Clarke (1997) outlined 16 "opportunity-reducing" techniques in his Situational Crime Prevention Theory. These 16 techniques are grouped into four categories (Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Reward and Remove Excuses), which impact a criminal's decision to commit a crime through either increasing the cost or reducing the benefit, or removing the justification for commission. For example, a countermeasure that falls under the Increase Perceived Effort category would discourage the commission of a crime by increasing a potential criminal's perception that the crime would involve more effort than he/she is willing to expend. A countermeasure that falls under the Increase Perceived Risk category would discourage the commission of a crime by increasing the potential criminal's perception that a crime involves more risk than he/she is willing to tolerate. A countermeasure that decreases a potential criminal's anticipated reward reduces the benefit that a criminal believes he/she will receive as a result of the crime. Lastly, a countermeasure that removes excuses reduces a potential criminal's ability to justify his/her actions. Beebe and Rao (2005) added a typical traditional crime analogy and corresponding computer misuse analogy for each of Clarke's 16 opportunity reducing factors, as seen in Table 1.

The success of Situational Crime Prevention Theory has been noted in several studies. Situational measures have proven successful in practically eliminating aircraft hijackings by screening baggage (Wilkinson, 1986) and reducing post office and bank robberies by target hardening (Clarke, 1997; Ekblom, 1988; Gabor, 1990; Grandjean,

1990). Application of this theory in the field of computer security, however, has yet to be empirically explored, though the potential for success in reducing insider computer misuse is very promising. Clarke (1997) has also noted that Situational Crime Prevention Theory is constantly evolving and its potential for applicability in many situations remains strong.

Situational Crime Prevention offers a holistic view of crime prevention that can be applied to computer security that previous theories have been unable to fulfill. Beebe and Rao (2005) proposed that previous theories and strategies have concentrated disproportionately on a criminal's perceived cost of committing a crime by utilizing strategies that would increase the chances of being discovered. These strategies would include countermeasures, such as firewalls, network monitoring software and physical security. An effective strategy would implement countermeasures that would affect both the criminal's perceived cost (likelihood of being discovered and punished) and benefit (rewards of perpetrating the crime). This strategy closely mimics previous research which stresses the need for a combination of technical (e.g. firewalls, passwords, encryption), formal (e.g. policies and procedures), and informal controls (e.g. education and training programs) (Beebe & Rao).

While a number of researchers have proposed the application of Situational Crime Prevention to combat computer misuse (Beebe & Rao, 2005; Willison, 2006; Willison & Siponen, 2009), as of this writing, there are no empirical studies that test the relationship. Previous theories such as General Deterrence Theory and Rational Choice Theory have not consistently proven their empirical effectiveness, nor do they offer a holistic approach to computer security. Moreover, with the incidents of computer misuse still at

unacceptably high rates, especially among insiders, it is imperative that researchers explore this relatively new theory and test its effectiveness in the field of computer security.

As this study endeavored to explore insider computer misuse, it was necessary to further update Beebe and Rao's (2005) application of Situational Crime Prevention Theory to computer security. A closer examination of the items listed in the Computer Misuse Countermeasure column of Table 1 revealed countermeasures that are not appropriate for a situation involving insider computer misuse, such as honeypots or honeynets, which typically are unprotected servers that deliberately lure outside hackers into uploading code and/or hacking tools in order to learn more about their attacks. Therefore, the researcher updated the Computer Misuse Countermeasure column to include countermeasures that are more appropriate for combating insider computer misuse. The updated table appears below.

Table 6

Updated Table with Appropriate Countermeasures for Insider Computer Misuse.

	Technique	Traditional Crime Countermeasure	Computer Misuse Countermeasure
Increase Perceived Effort	1. Target hardening	Locks, safes, fences, armed guards	External firewall(s), internal firewall(s), servers under lock and key
	2. Access control	Gate codes, guard shack, receptionist, swipe cards	ID/authentication systems, Kerberos, access control lists
	3. Deflecting offenders	Pedestrian/auto traffic redirection, no loitering	Clearly defined job duties, proxy servers
	4. Controlling facilitators	Gun control, limit ability to communicate	Strong password policy, required password change policy
Increase Perceived Risk	5. Entry/exit screenings	Metal detectors, screeners, merchandise tagging	Virus scanning, use of software such as Clean Access Agent for student network access, network log-in and log-out procedures
	6. Formal surveillance	CCTV, security guards, police patrols	Auditing and log reviews, email and web usage monitoring
	7. Surveillance by employees	Responsibility and/or ability to monitor	Review of resource usage, user training, reporting policies
	8. Natural surveillance	Lights, etc. so passers-by can see activity in the building	Workstations located in visible area, cameras in data-sensitive areas
Decrease Anticipated Rewards	9. Target removal	Electronic donations vs. cash, cash diverted to safe	Database partitioning/segmentation, use of database views, VPN's for off-campus network access
	10. Identifying property	VIN etched into auto glass, write name in book	Data classification, tagged identification of campus hardware and software
	11. Reducing temptation	Obscure valuables, gender neutral phonebook	Controlled distribution of campus software, software inventory system, use of screen saver lock on workstations
	12. Denying benefits	Security coded car radios, ink tags on clothing	Encryption, automatic data destruction mechanisms, network packet shaping

	Technique	Traditional Crime Countermeasure	Computer Misuse Countermeasure
Remove Excuses	13. Rule setting/clarification	Acceptable use policy, clear laws, licensing procedures	Acceptable use policy, user agreements, clear rules and procedures
	14. Stimulating conscience	"Shoplifting is stealing" signs, "current speed is"	Dissemination of anti-misuse information, codes of ethics
	16. Facilitating compliance	"Graffiti boards", public urinals, shelters, barriers	Offer software at reduced prices, required new user training on proper use of systems

The majority of the countermeasures in the updated table above were derived from an extensive review of computer security literature. Please see Tables 2 and 3 for appropriate references.

One of the main tenets of Situational Crime Prevention Theory is that it can be tailored to individual environments, making it an ideal base for computer security in higher education. The unique mixture of environments in higher education demands a scalable and flexible solution to computer misuse. Therefore, this study explored the relationships between insider computer misuse countermeasures that fall under Situational Crime Prevention's 16 opportunity-reducing techniques and the number of known incidents of insider computer misuse for certain institutions of higher education.

Chapter Summary

Straub (1990) defined computer misuse as "unauthorized and deliberate misuse of assets of the local organizational information system by individuals" (p. 257). Examples of misuse might include unauthorized network access, tampering with or stealing sensitive data, abusing e-mail privileges, or installing unlicensed software. Many industry surveys have shown that insider computer misuse, or misuse that is committed by an employee, is a pervasive problem for businesses (Computer Security Institute,

2007; Computer Security Institute, 2008; Department for Business Enterprise and Regulatory Reform, 2007). Insider computer misuse has also been identified as a problem, though with fewer incidents, in higher education (Kvavik & Voloudakis, 2006).

Numerous studies have recommended a number of different countermeasures to combat the problem of insider computer misuse. Countermeasures can either be classified as technical or administrative. The most common technical countermeasures found in the literature include authentication for resource access, monitoring software, and data access control using security levels (Aldhizer, 2008; D'Arcy & Hovav, 2007; Panko & Beh, 2002; Straub, 1990; Urbaczewski & Jessup, 2002).

Though technical countermeasures are extremely important, many authors reflect upon the propensity of some companies to rely solely on these technical countermeasures (Osborne, 1998; Parker, 1997; von Solms, 2001). With a complete emphasis on technical controls, the administrative category of countermeasures is ignored, creating a very one-sided security plan. The most common administrative countermeasures are Acceptable Use Policies, Codes of Ethics, password policies, and employee training.

Despite the presence of countermeasures, insider computer misuse still occurs. In a higher education environment, this could be due to the idea that effective implementation of computer security is difficult in a higher education setting, mainly due to environment and culture. Academic freedom is a tradition in higher education, but does not blend with the controlling nature of computer security. There is a constant struggle between an computer security specialist's need to implement a strong security plan and academia's need to exchange ideas and encourage exploration (Oblinger, 2003).

Though higher education campuses face some unique challenges when it comes to combating insider computer misuse, lessons can be learned by studying computer misuse in the business world. An even richer understanding comes from studying the problem from a criminological standpoint.

Situational Crime Prevention Theory appears to be a good fit for preventing insider computer misuse in higher education because of its inherent flexibility. As the environment and culture of higher education can vary from institution to institution, and even within a single institution, this flexibility allows computer security specialists to tailor a security plan based on a campus' individual needs. Therefore, this study explored the relationship between Situational Crime Prevention Theory and insider computer misuse on campuses of public, four-year colleges and universities in the United States.

CHAPTER III

METHODS

Introduction

Insider computer misuse is a problem in every industry, with consequences ranging from financial losses and loss of productivity to reputation damage. Although research has shown that insider computer misuse is a problem on college and university campuses (Cronan, Foltz, & Jones, 2006; Kvavik & Voloudakis, 2006), the bulk of computer security research has been conducted in the business sector. Further, while researchers agree that insider computer misuse is a problem, no one method for combating this misuse emerges in the literature. Most authors recommend a mixture of technical countermeasures, such as network and email monitoring, and administrative countermeasures, such as Acceptable Use Policies.

Situational Crime Prevention Theory assumes a number of technical and administrative countermeasures to prevent computer misuse. When applied to the field of information technology, a more holistic approach to preventing insider computer misuse emerges. However, to date, there does not appear to be a study in either the business environment or higher education environment regarding the relationship between Situational Crime Prevention and insider computer misuse.

Therefore, the purpose of this study was to explore the relationship between the categories of countermeasures in Situational Crime Prevention Theory and the number of insider computer misuse on college campuses. The researcher explored the above relationships as an effort to help campus technology departments choose the most

efficient and effective security countermeasures. From this data, the researcher responded to the following research questions and null hypotheses.

Research Questions

R_1 – To what extent are the countermeasures that increase the perceived effort to commit insider computer misuse related to the number of insider computer misuse incidents on campus?

H1: There is no relationship between the countermeasures that increase the perceived effort to commit insider computer misuse and the number of insider computer misuse incidents on campus.

R_2 – To what extent are the countermeasures that increase the perceived risk of committing insider computer misuse related to the number of insider computer misuse incidents on campus?

H2: There is no relationship between the countermeasures that increase the perceived risk of committing insider computer misuse and the number of insider computer misuse incidents on campus.

R_3 – To what extent are the countermeasures that decrease the anticipated reward for committing insider computer misuse related to the number of insider computer misuse incidents on campus?

H3: There is no relationship between the countermeasures that decrease the anticipated reward for committing insider computer misuse and the number of insider computer misuse incidents on campus.

R_4 – To what extent are the countermeasures that remove the excuses for committing insider computer misuse related to the number of insider computer misuse incidents on campus?

H4: There is no relationship between the countermeasures that remove the excuses for committing insider computer misuse and the number of insider computer misuse incidents on campus.

R_5 – What are the respondents' top five countermeasures in terms of perceived effectiveness?

Research Design

As this study aimed to explore the relationship Situational Crime Prevention Theory's four categories of countermeasures and the number of known insider computer misuse incidents in the year 2009, a quantitative approach was the most appropriate. Further, the collected data were numeric in nature and there was no need for open-ended questions. Therefore, the data were collected using a web-accessible questionnaire created in *SurveyMonkey*©.

The researcher posited that a relationship exists between the number of countermeasures in place at each institution and the number of computer misuse incidents experienced at each institution. Therefore, the independent variables are the categories of countermeasures from Situational Crime Prevention Theory: countermeasures to increase the perceived effort of the offender, countermeasures to increase the perceived risk of the offender, countermeasures to decrease the anticipated reward of the offender, and countermeasures to remove the excuses for the offender. The dependent variable is the number of known incidents of insider computer misuse in the year 2009.

Figure 2 below shows this study's conceptual framework with labeled hypotheses between the constructs.

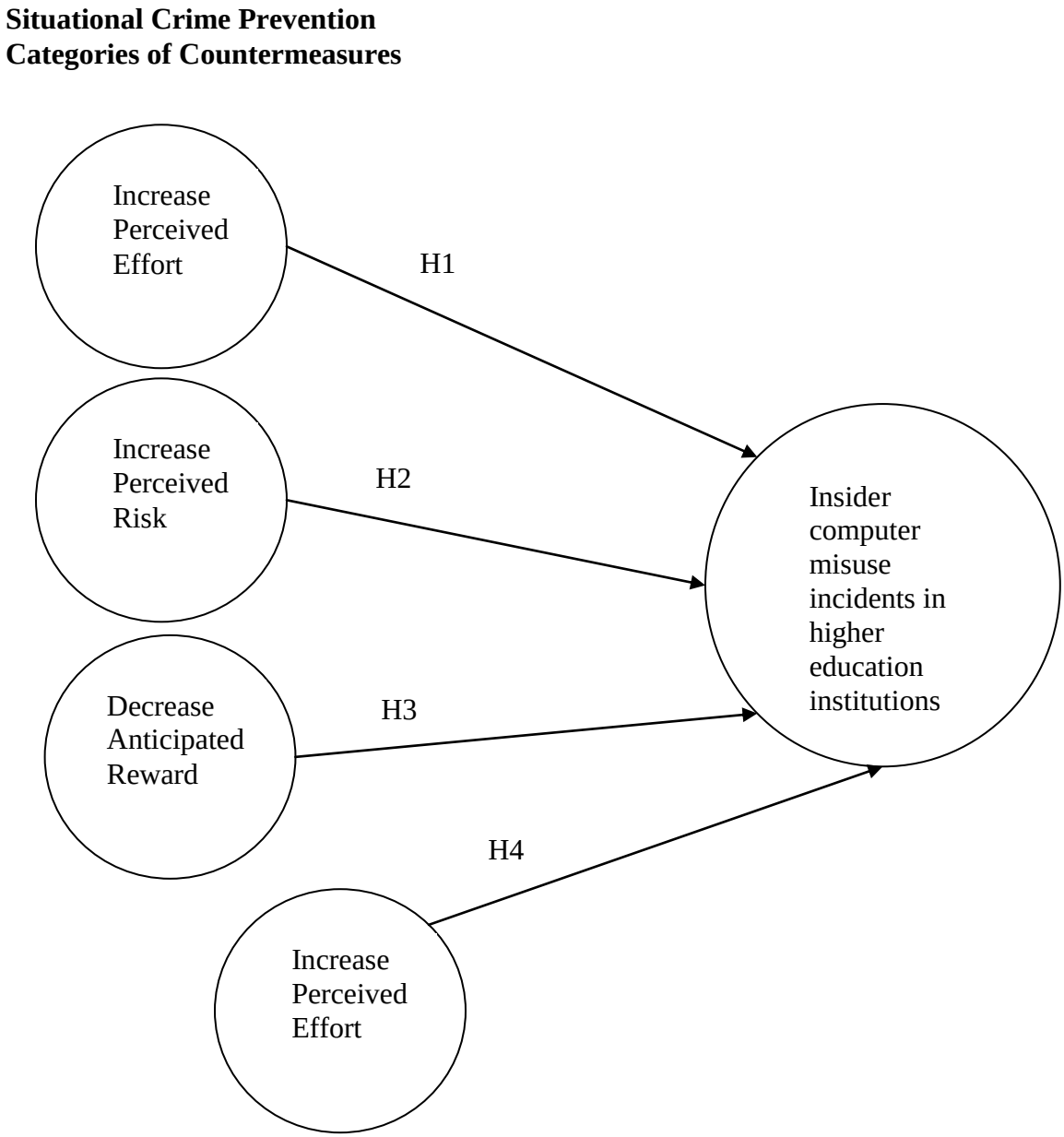

Figure 2: Conceptual Framework with Labeled Hypotheses

Sample and Sampling

The population for the current research study was public, four-year colleges and universities in the United States. By targeting only public, four-year colleges and universities and not including two-year or private institutions, it was hoped that differences in extraneous variables such as budget, size of technology staff, and mission of the institution would be mitigated. According to the National Center for Education Statistics, there are currently 652 public, four-year colleges and universities in the United States.

The respondents for the current research were Chief Information Officers (CIO's) or administrators of equivalent position at public, four-year colleges and universities within the United States. As the survey requested data regarding countermeasures found within the field of computer security, a CIO or equivalent administrator at each campus was identified as the most knowledgeable person to participate in the study. The names and email addresses of each CIO were gathered using information on each campus' website, from the governing body for higher education in each state, from *Educause*, an organization for the advancement of technology in higher education, and, failing all of the above, a phone call to each institution. The researcher found 442 names and email addresses for CIO's or administrators of equivalent position at public, four-year institutions across the United States.

In return for their response, each respondent was offered a copy of the results so that he/she can compare the countermeasures in place at his/her campus with those in place at other institutions. In order to provide the most useful data possible to each CIO,

the results were categorized based on institution size. Institution size was included solely for the purpose of providing data to the participants and was not used for analysis.

Instrumentation

As there is currently no instrument available to properly measure the variables in this study, the instrument was researcher-developed. Initial development of the instrument began by using a modified version of Beebe and Rao's (2005) initial mapping of Clarke's (2007) original 16 Situational Crime Prevention countermeasures to the field of computer security. A listing of the countermeasures with the corresponding questionnaire items appears below in Table 7.

Table 7

Countermeasures and Corresponding Questionnaire Items

Increase Perceived Effort

Technique	Traditional Crime Countermeasure	Computer Misuse Countermeasure	Question/Item Numbers
1. Target hardening	Locks, safes, fences, armed guards	External firewall(s), internal firewall(s), servers under lock and key	Question 3, items 1-3
2. Access control	Gate codes, guard shack, receptionist, swipe cards	ID/authentication systems, Kerberos, access control lists	Question 3, items 4-6
3. Deflecting offenders	Pedestrian/auto traffic redirection, no loitering	Clearly defined job duties, proxy servers	Question 3, items 7-8
4. Controlling facilitators	Gun control, limit ability to communicate	Strong password policy, required password change policy	Question 3, items 9-10

Increase Perceived Risk

Decrease Anticipated Rewards

Technique	Traditional Crime Countermeasure	Computer Misuse Countermeasure	Question/Item Numbers
5. Entry/exit screenings	Metal detectors, screeners, merchandise tagging	Virus scanning, use of software such as Clean Access Agent for student network access, network log-in and log-out procedures	Question 3, items 11-13
6. Formal surveillance	CCTV, security guards, police patrols	Auditing and log reviews, email and web usage monitoring	Question 3, items 14-16
7. Surveillance by employees	Responsibility and/or ability to monitor	Review of resource usage, user training, reporting policies	Question 3, items 17-19
8. Natural surveillance	Lights, etc. so passers-by can see activity in the building	Workstations located in visible area, cameras in data-sensitive areas	Question 3, items 20-21
9. Target removal	Electronic donations vs. cash, cash diverted to safe	Database partitioning/segmentation, use of database views, VPN's for off-campus network access	Question 3, items 22-24
10. Identifying property	VIN etched into auto glass, write name in book	Data classification, tagged identification of campus hardware and software	Question 3, items 25-27
11. Reducing temptation	Obscure valuables, gender neutral phonebook	Controlled distribution of campus software, software inventory system, use of screen saver lock on workstations	Question 3, items 28-30
12. Denying benefits	Security coded car radios, ink tags on clothing	Encryption, automatic data destruction mechanisms, network packet shaping	Question 3, items 31-33

Remove Excuses

Technique	Traditional Crime Countermeasure	Computer Misuse Countermeasure	Question/Item Numbers
13. Rule setting/clarification	Acceptable use policy, clear laws, licensing procedures	Acceptable use policy, user agreements, clear rules and procedures	Question 3, items 34-36
14. Stimulating conscience	"Shoplifting is stealing" signs, "current speed is"	Dissemination of anti-misuse information, codes of ethics	Question 3, items 37-38
15. Controlling disinhibitors	Controlling drugs/alcohol, propaganda, violent TV	Cyber-ethics education, supervised computer use, employee access to approved websites only	Question 3, items 39-41
16. Facilitating compliance	"Graffiti boards", public urinals, shelters, barriers	Offer software at reduced prices, required new user training on proper use of systems	Question 3, items 42-43

The countermeasures used in the updated table were derived from an extensive literature review. Appropriate references for each countermeasure are seen in Tables 2 and 3. After reviewing the data gathered from Beebe and Rao's (2005) table and the literature, the researcher constructed the questionnaire, as presented in Appendix A.

The respondents were given a list of specific countermeasures and asked if they utilize any of those countermeasures on their campus. If a CIO checks the box next to a particular countermeasure indicating that this countermeasure is in place at his/her campus, that data was recorded as a 1. The absence of a checkmark was recorded as a 0. The last question on the questionnaire asked the respondents to rank their top five countermeasures in terms of perceived effectiveness. This data provided additional insight into the state of computer security in higher education by identifying the most popular countermeasures that CIO's have implemented on their campuses.

Pilot Study

As the instrument used in this study was researcher-developed, a pilot study was required to ensure the listed countermeasures and wording are appropriate. A pilot study consisting of CIO's from eight colleges and universities within the state of Georgia was conducted. Data from these institutions were not included in the final data collection.

The CIO's from these eight institutions were sent an email containing a link to the questionnaire, information about the research, and the expectations regarding their participation in the pilot study. Separate from the questionnaire, pilot study respondents were asked to provide feedback based on their experiences when responding to the questionnaire. In particular, they were asked to identify any terms that were unclear or needed additional clarification. A representative copy of the email sent to each CIO is found in Appendix B. Based on this feedback, the researcher updated the questionnaire.

Data Collection

Data collection began with an email to each CIO in the population. A copy of the email is in Appendix C. The email contained a link to the questionnaire in *SurveyMonkey*©. All of the collected data were numeric in nature, and there were no open-ended questions to code.

In its electronic format, the questionnaire was five pages in length with a total of 4 questions. Questions 3 and 4 each contained 43 items. None of the questions required a free-form answer except for the question which asked the number of known computer misuse incidents in the year 2009. Therefore, it was estimated that each respondent should have completed the questionnaire quickly with a minimum time commitment of no more than 15 minutes. It is also important to note that each question in the

questionnaire required a response. Therefore, there should have been no incomplete questionnaires. However, incomplete questionnaires were still recorded and were subsequently discarded.

In order to maintain absolute anonymity for the respondents, the option to collect IP addresses was turned off in *SurveyMonkey*©. Therefore, the researcher could not utilize the address book feature in *SurveyMonkey*© for follow-up requests. However, a repeat email to each of the CIO's was completed approximately five days after the initial invitation requesting response. As an incentive to fill out the questionnaire, the researcher offered, by request, a copy of the data results to each CIO. Twelve CIO's requested a copy of the results.

Data Analysis

The collected data were analyzed using PLS-Graph, a software package for statistical analysis. As this study aimed to explore the relationship between the four categories of countermeasures and the number of known insider computer misuse incidents in the year 2009, PLS-Graph was deemed an ideal software package for analysis. PLS-Graph utilizes latent variable path modeling using the Partial Least Squares approach. Additionally, PLS-Graph is less sensitive to matters such as sample size and data distributions when compared to other structural equation modeling software and SPSS (Chin, 1998). In its analysis, PLS-Graph estimates the loadings between items and constructs, the path coefficients, and the correlations between the constructs in the proposed framework. Finally, PLS-Graph calculates *t*-values, which, when compared to calculated critical values, provides a basis for exploring the relationship between the constructs (Gefen, Straub, & Boudreau, 2000).

Reporting the Data

The data were reported in tabular format, as a tabular format was most suitable for reporting the numeric results of the statistical tests. Finally, the four hypotheses and one research question were addressed individually and grouped with supporting data.

Chapter Summary

Insider computer misuse is a problem for all industries, including colleges and universities. With ever-shrinking resources, institutions of higher education must implement an effective and efficient security plan to combat this particular type of computer misuse. In an effort to help colleges and universities adopt an appropriate security policy and plan, the current research explores the relationship between categories of countermeasures outlined in Situational Crime Prevention Theory, and the number of known insider computer misuse incidents experienced in the year 2009.

The population of the current research was all Chief Information Officers (CIO's) of public, four-year colleges and universities in the United States, effectively rendering the population and sample equivalent. The number of public, four-year colleges and universities in the United States is 652. However, the researcher was able to find CIO or equivalent administrator names and email addresses for 442 institutions.

The questionnaire was web-accessible using *SurveyMonkey*©. Each CIO received an invitation to complete the questionnaire, with an offer to share certain aspects of the data in return for their participation.

The instrument was researcher-developed, necessitating thorough use of expert review and a pilot study of eight campuses. Results of the pilot study were used to improve the clarity of the questionnaire, with an emphasis on appropriate terminology.

Further, composite reliability and factor analysis was completed to ensure that the questions within each category are appropriately related.

Data analysis was completed using PLS-Graph. Descriptive statistics were computed followed by computation of path coefficients, *t* statistic analysis, and R-square analysis to determine the relationship between the latent constructs and predictive utility.

CHAPTER IV

REPORT OF DATA AND DATA ANALYSIS

Introduction

Insider computer misuse is a problem for all industry sectors, including higher education, and consequences can range from financial losses to reputation damage (Computer Crime and Security Survey, 2008; Cronan, Foltz, & Jones, 2006; Department for Business Enterprise and Regulatory Reform, 2007; Kvavik & Voloudakis, 2006). Though many researchers have addressed the prevention of computer misuse, no clear solution exists. Most authors recommend a mixture of technical and administrative countermeasures to best combat the issue, though there is little agreement among the authors' findings. Moreover, much of the literature on computer misuse is limited to the business sector, leaving colleges and universities a relatively unstudied group. Therefore, the current research proposed to apply a theory which offers a balanced mixture of administrative and technical controls, Situational Crime Prevention, and investigate whether a relationship exists between Situational Crime Prevention's controls and the number of campus insider computer misuse incidents.

Using a questionnaire administered through *SurveyMonkey*©, the researcher asked the CIO's of 442 public, four-year institutions of higher education in the United States about the number of insider computer misuse incidents in the year 2009, the countermeasures they have in place on their campus, and to rank their top five countermeasures in terms of effectiveness. A complete copy of the questionnaire is found in Appendix A.

Using the data gathered through the questionnaire described above, the researcher endeavored to answer the research questions and corresponding null hypotheses listed in Chapter III. In this chapter, the researcher presented findings from the pilot study, changes made to the instrument as a result of the pilot study, and analysis of findings from the data collection.

Research Design

Pilot Study Procedures

As described in Chapter III, CIO's from eight colleges and universities within the University System of Georgia participated in the pilot study. Over a two-week period, the respondents were contacted individually with an email almost identical to Appendix B. The only changes to the invitation email were some personalization. After one reminder email, the response rate was 100%.

As clear and unambiguous terminology is particularly important to this questionnaire, pilot study respondents were asked to provide feedback to the researcher outlining any recommended changes to the questionnaire terminology and an estimation of how long it took each of them to complete the questionnaire. Six out of eight respondents provided feedback. Based on the pilot study respondents' suggestions, some of the wording was changed in the questionnaire, but the essential format of the questionnaire remained unchanged. Specifically, questions 1, 3, and 4 were modified slightly to reflect recommendations from the pilot study respondents. Question 1 was edited to specify from which term the respondent should report his/her institution's FTE's. In question 3, the item "Encryption" was changed to add different types of encryption, such as SSL (Secure Sockets Layer), PGP (Pretty Good Privacy), and

password encryption. The Encryption item was identically changed in question 4. The last page of the questionnaire was also changed. The last sentence originally read "You may now close your browser." As the page included a "Done" button, one respondent felt that sentence was confusing. The sentence was changed to state "You may now click the Done button below or close your browser." Finally, all respondents who indicated how long it took to fill out the questionnaire stated that the process took less than 10 minutes.

Data Results from Pilot Study

Data results for each respondent are shown in Table 8. The number represented under the category is a count of the number of countermeasures within that category that the CIO reported he/she had in place on his/her campus.

Table 8

Pilot Study Data by Respondent

Respondent	Misuse Incidents	Increase Perceived Effort	Increase Perceived Risk	Decrease Anticipated Rewards	Remove Excuses
1	10	6	3	2	2
2	5	5	5	6	5
3	20	7	6	5	5
4	15	9	6	8	6
5	5	7	4	5	2
6	2	7	7	7	2
7	1	9	5	8	4
8	8	7	4	3	3

Tables 9, 10, 11, and 12 show each countermeasure within the categories of Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Rewards and Remove Excuses and the percentage of institutions that utilizes each countermeasure.

Table 9

Percentage of Institutions That Utilizes Each Countermeasure in Increase Perceived Effort

Technique	**Countermeasure**	**Percentage of Institutions that Utilize the Countermeasure (n =8)**
Target Hardening	External firewalls	100%
	Internal firewalls	88%
	Servers under lock and key	100%
Access Control	ID Authentication	100%
	Kerberos	25%
	Access control lists	63%
Deflecting Offenders	Clearly defined job duties	50%
	Proxy Servers	13%
Controlling Facilitators	Strong password policy	88%
	Required password change policy	88%

Table 10

Percentage of Institutions That Utilizes Each Countermeasure in Increase Perceived Risk

Technique	**Countermeasure**	**Percentage of Institutions that Utilize the Countermeasure (n =8)**
Entry/Exit Screenings	Virus scanning	100%
	Rules regarding joining campus network	88%
	Network log in/log out procedures	63%
Formal surveillance	Auditing and log reviews	50%
	Email usage monitoring	0%
	Web usage monitoring	13%
Surveillance by employees	Review of resource usage	13%
	User training	13%
	Reporting policies	13%
Natural surveillance	Workstations located in visible areas	63%
	Cameras in data sensitive areas	63%

Table 11

Percentage of Institutions That Utilizes Each Countermeasure in Decrease Anticipated Rewards

Technique	**Countermeasure**	**Percentage of Institutions that Utilize the Countermeasure (n =8)**
Target removal	Database partitioning/ Segmentation	25%
	Database views	50%
	Virtual Private Networks	88%
Identifying property	Data classification	25%
	Tagged identification of campus hardware	75%
	Tagged identification of campus software	13%
Reducing temptation	Software inventory system	38%
	Controlled distribution of campus software	75%
	Use of screen saver locks	50%
Denying benefits	Encryption	50%
	Automatic data destruction mechanisms	0%
	Network packet shaping	63%

Table 12

Percentage of Institutions That Utilizes Each Countermeasure in Remove Excuses

Technique	**Countermeasure**	**Percentage of Institutions that Utilize the Countermeasure (n =8)**
Rule setting/ Clarification	Acceptable use policy	100%
	User agreements	50%
	Clear rules and procedures	38%
Stimulating conscience	Dissemination of anti-misuse information	0%
	Codes of ethics	50%
Controlling disinhibitors	Cyber-ethics education	13%
	Supervised computer use	25%
	Employee access to approved websites only	13%
Facilitating compliance	Offer software at reduced prices	50%
	Required new user training on proper use of systems	25%

As research question five is concerned with the respondent's top five countermeasures in terms of perceived effectiveness, Table 13 below shows a ranking of the top five countermeasures. The score was determined by first transposing the data. For example, if the countermeasure External Firewalls received a score of 5 from one of the respondents, that particular respondent ranked External Firewalls as one of his/her top five countermeasures but at the bottom of the effectiveness scale. Therefore, the score of 5 would be converted to a 1. Similarly, a score of 4 would be converted to a 2, a 3 would remain a 3, a 2 would become a 4 and a 1 would become a 5. In essence, the scores

would simply be reversed so that, when summed, an accurate ranking could be determined. As a result of the pilot study, the questionnaire was changed to make scoring of this item simpler. The respondents were asked to rank their most effective countermeasure with a 5, their next most effective countermeasure with a 4, and so on.

Table 13

Top Five Countermeasures in Terms of Perceived Effectiveness

Countermeasure	**Score**
External firewalls	26
ID and password authentication	20
Virus scanning	16
Servers under lock and key	13
Acceptable use policy	5

Following completion of the pilot study, IRB approval from Georgia Southern University was obtained. Official approval is attached as Appendix D. The researcher then began the data collection process.

Respondents

The respondents were CIO's or persons of equivalent position at public, 4-year colleges and universities in the United States. The researcher did not request any demographic information about the respondents within the questionnaire.

Response Rate

The researcher was able to find 442 contact names out of 652 public, 4-year institutions in the United States. Therefore, emails were sent to the CIO's or persons of

equivalent position at 442 institutions. Of these 442 invitation emails, 101 attempted the questionnaire, for a response rate of 23%. Two emails were sent to each respondent, an initial invitation and a follow-up email.

To assure that enough responses were received to perform data analysis, the researcher referenced Cohen's (1992) table for power analysis. According to Cohen's table, for a medium effect size at the .05 significance level for four independent variables, a total of 84 responses would be adequate for data analysis

Findings and Analysis

At the end of the data collection period, the researcher began analysis by downloading the data into an Excel spreadsheet. A copy of the raw data is included in Appendix E. The data were then examined, and unusable or incomplete records were deleted. An unusable record is one where, most often, a respondent would type "don't know" or "test" for the question that asked about the number of computer misuse incidents their institution experienced in the year 2009. After eliminating unusable records, the number of complete responses was 89.

Next, variable names were created based on the technique being implemented. For example, in Table 7, the first technique in column 1 is target hardening. The corresponding computer misuse countermeasures for target hardening are external firewalls, internal firewalls, and servers under lock and key. Therefore, the respondents answer to whether his/her institution utilized external firewalls would be represented by TH1 (target hardening, first question), and his/her answer to whether the institution utilized internal firewalls would be TH2 (target hardening, second question). The same

naming scheme was used for each countermeasure within each technique. An answer of "yes" was recorded as a 1, and an answer of "no" was recorded as a 0.

As the hypotheses are concerned with overall categories of countermeasures, i.e. Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Rewards, and Remove Excuses, the responses for each countermeasure under each category were assigned to a variable representing each category, i.e. IPE for Increase Perceived Effort, IPR for Increase Perceived Risk, DAR for Decrease Anticipated Rewards, and RE for Remove Excuses.

The final part of preparing the data for analysis involved creating categories for the number of computer misuse incidents each institution reported on the questionnaire. This was completed because of the excessive number of outliers in the original data. The category instead of the reported number was used for data analysis. The categories appear below in Table 14.

Table 14

Categories of Computer Misuse Incidents

Category	Number of Incidents
0	0
1	Between 1 and 25, inclusive
2	Between 26 and 50, inclusive
3	Between 51 and 75, inclusive
4	Between 76 and 100, inclusive
5	Greater than 100

Descriptive Statistics

It is important to look at the data as a whole before any analysis is completed for each research question and hypothesis. Table 15 below shows how many of the 89 respondents utilize each countermeasure listed on the questionnaire.

Table 15

Number of Respondents that Utilize Each Countermeasure (n=89)

Category	Technique	Countermeasure	Item	Yes	No
Increase Perceived Effort	Target Hardening	External firewall	TH1	86%	14%
		Internal firewall	TH2	84%	16%
		Servers under lock and key	TH3	90%	10%
	Access Control	ID/password authentication	AC1	97%	3%
		Kerberos	AC2	35%	65%
		Access control list(s)	AC3	87%	13%
	Deflecting Offenders	Clearly defined job duties	DO1	81%	19%
		Proxy servers	DO2	45%	55%
	Controlling Facilitators	Employees must use strong passwords	CF1	81%	19%
		Employees must change passwords regularly	CF2	78%	22%
Increase Perceived Risk	Entry/Exit Screenings	Virus scanning	EES1	98%	2%
		Rules regarding joining campus network	EES2	73%	27%
		Network log-in and log-out procedures	EES3	57%	43%
	Formal Surveillance	Auditing and log reviews	FS1	70%	30%
		Employee email monitoring	FS2	8%	92%
		Employee web usage monitoring	FS3	3%	97%
	Surveillance by Employees	Review of resource usage information	SE1	35%	65%
		User training related to security policy	SE2	70%	30%
		Reporting policies for misuse incidents	SE3	78%	22%
	Natural Surveillance	Workstations located in visible areas	NS1	37%	63%
		Cameras in data-sensitive areas	NS2	33%	77%

Category	Technique	Countermeasure	Item	Yes	No
Decrease Anticipated Rewards	Target Removal	Database partitioning/segmentation	TR1	62%	38%
		Use of database views	TR2	67%	33%
		Use of virtual private networks	TR3	91%	9%
	Identifying Property	Data classification	IP1	64%	36%
		Tagged identification of campus hardware	IP2	73%	27%
		Tagged identification of campus software	IP3	20%	80%
	Reducing Temptation	Use of software inventory system	RT1	38%	62%
		Controlled distribution of campus software	RT2	71%	29%
		Use of screen saver lock on workstations	RT3	72%	28%
	Denying Benefits	Encryption	DB1	89%	11%
		Automatic data destruction mechanisms	DB2	15%	85%
		Network packet shaping	DB3	67%	33%
Remove Excuses	Rule Setting/ Clarification	Acceptable use policy	RSC 1	94%	6%
		User agreements	RSC 2	63%	37%
		Clear rules and procedures	RSC 3	67%	33%
	Stimulating Conscience	Multiple dissemination methods of anti-misuse information	SC1	40%	60%
		Code(s) of ethics	SC2	40%	60%
	Controlling Disinhibitors	Cyber-ethics education	CD1	21%	79%
		Supervised computer use	CD2	11%	89%
		Employee access to only approved websites	CD3	8%	92%
	Facilitating Compliance	Offer software at reduced prices	FC1	69%	31%
		Required user training on proper use of campus systems	FC2	37%	63%

Finally, the data were imported into PLS-Graph. Analysis began with construct validity and discriminant validity calculations, and calculation of composite reliability.

Next, path coefficients and *t* statistics were calculated for addressing hypotheses one though four. Though the majority of the data in this study is dichotomous, it is appropriate to analyze dichotomous data in the same manner as interval data. Interval data is defined as having a set measurement scale of known magnitude. Likewise, dichotomous data can be defined as having two scales of known magnitude (Nunnally & Bernstein, 1984).

Construct Validity

Construct validity was calculated based on examination of item loadings to construct correlations. The steps utilized to complete construct validity are outlined in Gefen and Straub (2005). In general terms, the item loadings on the latent constructs were calculated in PLS-Graph. The output from this calculation was imported into an Excel spreadsheet, and this spreadsheet data were then imported into SPSS, software designed specifically for statistical analysis. Excel was needed because data cannot be directly transferred from PLS-Graph to SPSS. Once in SPSS, bivariate correlations were calculated, and the item loadings on each construct were examined. Table 16 below shows each construct with its corresponding items and loadings. Composite reliability with all items included is shown, as well as composite reliability with low loading items removed. Some items are denoted with an asterisks (*), which indicates that the item was removed from the construct due to a low loading value. Tabachnick and Fidell (2001) assert that each item should possess a loading value of at least .32 in relation to its construct.

Composite reliability was developed by Werts, Linn, and Jöreskog (1974) and is a measure of internal consistency similar to Cronbach's alpha. The difference is that

composite reliability does not assume *tau* equivalency among the measures. The values of computed composite reliability and computed Cronbach's alpha should be interpreted similarly. Per Nunnally (1967), an alpha level as low as .6 can be considered sufficient for the early stages of basic research.

Table 16

Constructs with Associated Loadings and Composite Reliability

Construct	**Items**	**Loadings**	**Composite Reliability with All Items**	**Composite Reliability with Low Items Deleted**
Increase Perceived Effort			.651	.770
	TH1	.332		
	TH2*	.066		
	TH3	.787		
	AC1	.741		
	AC2*	.166		
	AC3*	.264		
	DO1	.462		
	DO2	.377		
	CF1	.559		
	CF2*	.093		
Increase Perceived Risk			.572	.743
	EES1	.500		
	EES2	.418		
	EES3*	.059		
	FS1	.468		
	FS2*	.159		
	FS3*	.036		
	SE1*	.023		
	SE2*	.191		
	SE3*	.029		
	NS1*	.235		
	NS2	.541		

Construct	Items	Loadings	Composite Reliability with All Items	Composite Reliability with Low Items Deleted
Decrease Anticipated Rewards			.625	.695
	TR1	.344		
	TR2*	.265		
	TR3	.604		
	IP1*	.027		
	IP2*	.035		
	IP3*	.273		
	RT1*	.279		
	RT2	.531		
	RT3	.443		
	DB1	.541		
	DB2	.516		
	DB3*	.265		
Remove Excuses			.541	.679
	RSC1*	.014		
	RSC2*	.079		
	RSC3*	.089		
	SC1	.378		
	SC2*	.153		
	CD1	.718		
	CD2	.350		
	CD3	.394		
	FC1	.583		
	FC2	.411		

* item removed from analysis due to low loading value

Discriminant Validity

Following removal of the low loading items, discriminant validity was conducted to verify that each item correlates highest with the construct that it purports to measure (Gefen & Straub, 2005). Table 17 shows each item and its correlation value for each

construct. The values in bold confirm that each item correlates highest with its associated construct.

Table 17

Discriminant Validity Correlation Values

Item	IPE	IPR	DAR	RE
TH1	**.332**	.127	.183	.086
TH3	**.787**	.242	.403	.094
AC1	**.741**	.385	.539	.031
DO1	**.462**	.248	.229	.086
DO2	**.377**	.053	.202	.095
CF1	**.559**	.210	.278	.035
EES1	.451	**.500**	.513	.050
EES2	.210	**.418**	.213	.045
FS1	.259	**.468**	.255	.060
NS2	.121	**.541**	.328	.095
TR1	.142	.139	**.344**	.252
TR3	.474	.198	**.604**	.047
RT2	.324	.258	**.531**	.058
RT3	.200	.221	**.443**	.110
DB1	.306	.268	**.541**	.035
DB2	.101	.260	**.516**	.048
SC1	.338	.122	.272	**.378**
CD1	.158	.237	.219	**.718**
CD2	.098	.295	.233	**.350**
CD3	.021	.327	.251	**.394**
FC1	.179	.026	.152	**.583**
FC2	.225	.177	.237	**.411**

Data Analysis

Using PLS-Graph, path coefficients and *t*-statistics were computed using a bootstrapping resampling technique. In PLS-Graph, bootstrapping involves resampling with replacement from the original sample. The following analysis was conducted using 200 resamples as recommended by Chin (1998). The licensing agreement for PLS-Graph is included in Appendix F. A screenshot of the resulting graphical representation of the model constructs with associated survey questions is included below in Figure 3.

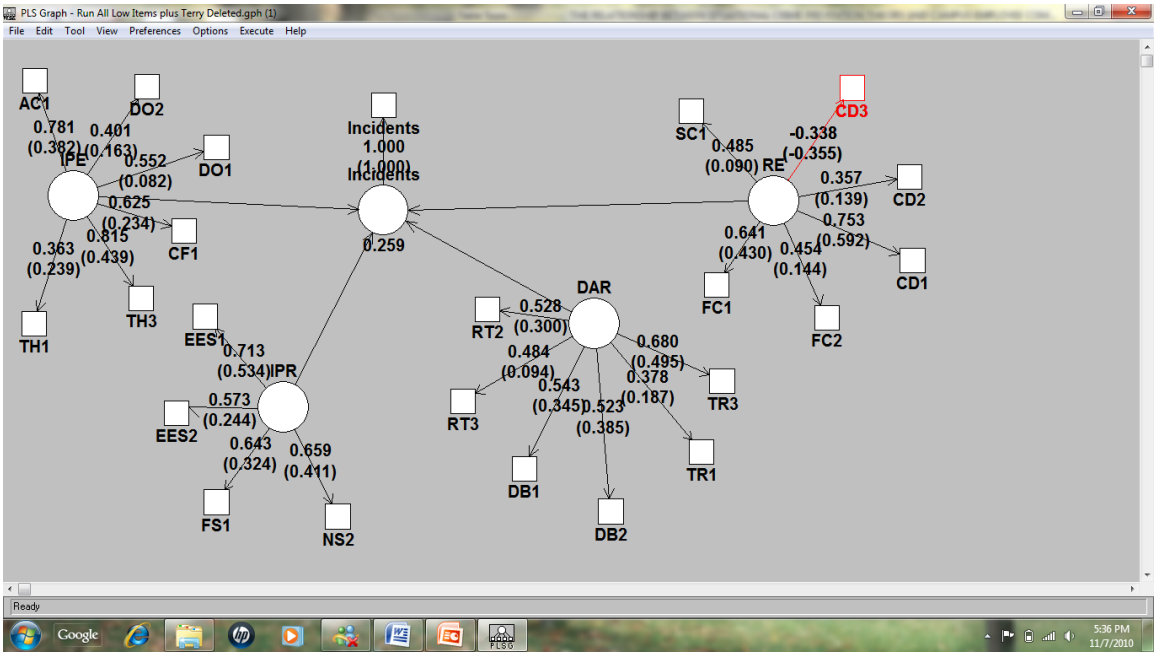

Figure 3: Screenshot of PLS-Graph Model Construct with Associated Survey Questions

The model complete with independent and dependent constructs, their path coefficients, and R-square value were included below in Figure 4.

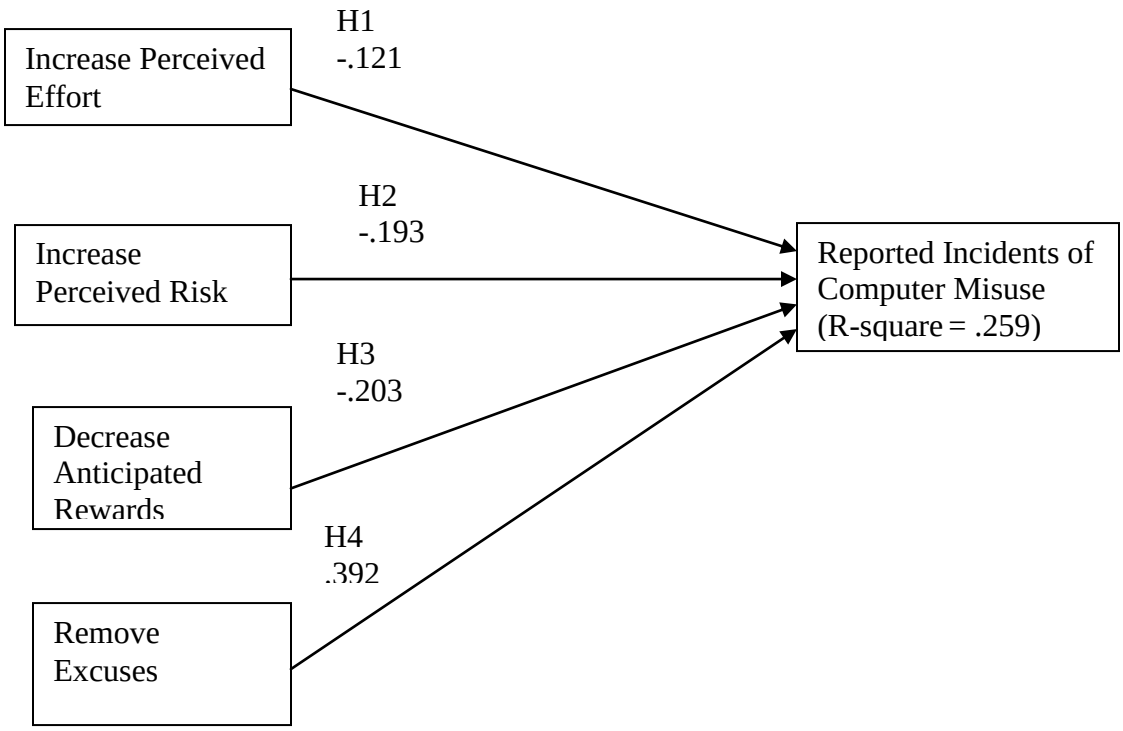

Figure 4: Model Representation from PLS-Graph with Path Coefficients and R-Square Value

The next step in analysis was to compute the critical value using the *t* distribution table, $\alpha = .05$, a one-tailed test, and degrees of freedom of 88 ($n - 1$). Using these parameters, the critical value was 1.662. To determine whether or not to reject hypotheses one through five, the *t* statistic generated by PLS-Graph was compared with the critical value. Therefore, if the *t* statistic was greater than the critical value of 1.662, a relationship between the construct and the dependent variable existed and the hypothesis was rejected. If the *t* statistic was less than or equal to the critical value of 1.662, there was no relationship between the construct and the dependent variable, and the hypothesis was not rejected.

Hypothesis 1.

H1: There is no relationship between the countermeasures that increase the perceived effort to commit insider computer misuse and the number of insider computer misuse incidents on campus.

Finding and Discussion.

The path coefficient between the construct of Increase Perceived Effort and the dependent variable of Number of Computer Misuse Incidents was negative at .121. The *t* statistic was 1.019, which is less than the critical value of 1.662. Therefore, H1 should not be rejected.

Hypothesis 2.

H2: There is no relationship between the countermeasures that increase the perceived risk to commit insider computer misuse and the number of insider computer misuse incidents on campus.

Finding and Discussion.

The path coefficient between the construct of Increase Perceived Risk and the dependent variable of Number of Computer Misuse Incidents was negative at .193. The *t* statistic was 1.621, which is just under the critical value of 1.662. Therefore, H2 should not be rejected.

Hypothesis 3.

H3: There is no relationship between the countermeasures that decrease the anticipated rewards to commit insider computer misuse and the number of insider computer misuse incidents on campus.

Finding and Discussion.

The path coefficient between the construct of Decrease Anticipated Rewards and the dependent variable of Number of Computer Misuse Incidents was significant with a negative value of .203. The *t* statistic was 1.919, which is greater than the critical value of 1.662. Therefore, hypothesis 3 should be rejected.

Hypothesis 4.

H4: There is no relationship between the countermeasures that remove the excuses to commit insider computer misuse and the number of insider computer misuse incidents on campus.

Finding and Discussion.

The path coefficient between the construct of Remove Excuses and the dependent variable of Number of Computer Misuse Incidents was significant at .368. The *t* statistic was 2.697, which is greater than the critical value of 1.662. Therefore, H4 should be rejected.

P**redictive Value of Model.**

In order to examine the predictive value of the model, it was necessary to look at the R-square value computed by PLS-Graph. For the current model, the R-square value is .26, which is interpreted as 26% of the variance in the Number of Computer Misuse Incidents is explained by the constructs Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Rewards, and Remove Excuses. Additionally, the construct that appears to have the greatest negative influence on the Number of Computer Misuse Incidents is Decrease Anticipated Rewards, with a negative path coefficient of .203.

Research Question 5.

R_5 – What are the respondents' top five countermeasures in terms of perceived effectiveness?

Finding and Discussion.

Respondents were asked to identify their top five countermeasures in terms of perceived effectiveness and then rank those five using a scale of 5 to 1, with 5 corresponding to the countermeasure with the most perceived effectiveness. The top five countermeasures with the corresponding score are shown in Table 18 below.

Table 18

Respondents' Top Five Countermeasures in Terms of Perceived Effectiveness with Score Ranking

Countermeasure	**Score**
ID and password authentication	142
External firewalls	121
Employees must use strong passwords	121
Virus scanning	114
User training related to security policy	103

It is interesting to note that three out of the five top countermeasures would fall into the Increase Perceived Effort category, which did not demonstrate a significant relationship with the number of computer misuse incidents. The fact that three of the five countermeasures are technical in nature supports Beebe and Rao's (2005) assertion that most security plans are imbalanced in favor of technical countermeasures, while often overlooking the more human or administrative controls.

Calculated Observed Power.

A Type II error occurs when a researcher fails to reject a false null hypothesis. To calculate the probability of a Type II error, the researcher calculated the power of the current test using the parameters of $\alpha = .05$, number of predictors = 4, R-square = .259, and sample size = 89. The calculated power was .997 (Soper, 2010). Therefore, the probability of failing to reject a false null hypothesis for this study is .3%.

Chapter Summary

Data analysis began with the completion of a pilot study consisting of eight colleges and universities within the University System of Georgia. Pilot study respondents were also asked to provide feedback regarding the terminology used in the questionnaire and whether it was clear and appropriate, and how long it took them to complete the questionnaire. Using suggestions from the pilot study group, the questionnaire was edited.

After acquiring IRB approval, the researcher sent out invitation emails asking CIO's of 442 public, 4-year colleges and universities for their participation in the study. From these 442 invitations, a total of 101 people responded, with 89 responses deemed usable. This low response rate prompted the researcher to perform power analysis, which indicated that 84 responses would be sufficient for analysis.

For the remaining hypotheses, based on comparison of *t* statistics and critical values, H3 and H4 should be rejected, and H1 and H2 should not be rejected. The calculated power of the current test was .997. The predictive value of the model was examined using the calculated R-square value of .259, which is interpreted as 26% of the variance in Number of Computer Misuse Incidents is explained by the model.

The respondents' top five countermeasures in terms of perceived effectiveness were, in order, ID and password authentication, external firewalls, employee use of strong passwords, virus scanning, and user training related to security policy. It is interesting to note four of the five top countermeasures are technology-dependent, while only one addressed the more human or administrative side of security controls.

CHAPTER V

SUMMARY, CONCLUSIONS, AND IMPLICATIONS

Summary

High-profile computer misuse incidents, such as the compromise of the Large Hadron Collider, tend to capture the media's attention. However, the truth is that these types of incidents are relatively infrequent. It is the day-to-day incidents of computer misuse that erode efficiency and damage reputations of both businesses and educational institutions. Combating this misuse using countermeasures has been a common topic for information security research, with many different authors proposing recommendations.

Countermeasures can be divided into two overall categories: technical and administrative. Most authors recommend a balanced security plan with countermeasures taken from both categories (Dhillon & Moores , 2001; Straub, 1990; Willison & Backhouse, 2006). These recommendations, however, were for the business environment. Higher education institutions have remained a relatively unstudied group. Further, many studies favor one category of countermeasure over another instead of offering a blend of both categories.

Examining computer security literature from a theoretical perspective reveals three theories that have captured the attention of researchers: General Deterrence Theory, Rational Choice Theory, and Situational Crime Prevention Theory. This researcher chose Situational Crime Prevention Theory as a basis for study, due to its flexible, balanced framework that can be readily applied to computer security.

Situational Crime Prevention has proven successful in reducing crime in many types of situations including aircraft hijackings, post office robberies, and bank robberies

(Clarke, 1997; Ekblom, 1988; Gabor, 1990; Grandjean, 1990; Wilkinson, 1986). However, its efficacy in the area of computer security has yet to be studied empirically in either the business sector or higher education sector. Therefore, this researcher endeavored to study the relationship between categories of countermeasures in Situational Crime Prevention Theory and the number of reported insider computer misuse incidents on college campuses. It was posited that the data collected would assist higher education administrators to create an effective security plan.

Data were collected with a web-based, anonymous questionnaire. The questionnaire contained questions related to institution size, the number of computer misuse incidents known in the year 2009, and countermeasures in place on each campus. Participants were the Chief Information Officers (CIOs) or administrators of equivalent responsibility at public, four-year institutions of higher education. After a pilot study was completed to test the survey instrument, this researcher requested the participation of 442 higher education institutions, with a final, usable response count of 89.

Analysis of Research Findings

For hypotheses one through four, analysis using PLS-Graph produced the following results. Using *t* statistic and critical value analysis, H1 and H2 were not rejected, while H3 and H4 were rejected. Out of the four independent variables of Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Rewards, and Remove Excuses, Decrease Anticipated Rewards appeared to exert the greatest negative influence on the dependent variable of Number of Computer Misuse Incidents. Further, regression analysis using computed R^2 value showed that 26% of the variance in computer misuse incidents is explained by the current model.

The respondents' top five countermeasures in terms of perceived effectiveness were, in order, ID and password authentication, external firewalls, employee use of strong passwords, virus scanning, and user training related to security policy.

Discussion of Research Findings

As of this writing, no researcher has reported data analysis on computer security with Situational Crime Prevention Theory as a foundation. Therefore, it is not possible to compare data results with any previous research. The reasons for this lack of data are not clear. However, some authors have asserted that research in the area of information security is particularly difficult due to the intrusive nature of the research and the general mistrust of anyone seeking to gain information about information security (Kotulic & Clark, 2004).

While the current research found a relationship between two of the independent variables and the dependent variable of Incidents of Computer Misuse, only one of those independent variables, the construct Decrease Anticipated Rewards, showed a negative relationship. The relationship between the construct Remove Excuses and the number of computer misuse incidents was positive, indicating that increasing the number of countermeasures within the category of Remove Excuses would actually increase the number of computer misuse incidents. This finding is counterintuitive. However, Harrington (1996) found that a Code of Ethics, a countermeasure found in the Remove Excuses category, has no effect on a user's intention to commit misuse. Though intention to commit misuse is not identical to actual incidents of misuse, it is reasonable to assume that the intention to commit misuse precedes an incident of computer misuse.

With one study finding a positive relationship between controls that would be within the category of Remove Excuses and computer misuse, and another study finding no relationship, it is possible that these types of countermeasures should not be considered of upmost importance when creating a security plan.

Putting aside the overall lack of empirical data for comparison, it is interesting to examine the list of countermeasures on the questionnaire through the lens of computer security literature. The researcher compiled the list of countermeasures on the questionnaire using information gathered from the body of research related to computer security. The technical countermeasures were compiled using the research literature outlined in Table 2, while the administrative countermeasures were compiled using the research literature outlined in Table 3. Technical countermeasures tend to rely on some type of technology while administrative countermeasures rely more on policies.

Though some of the recommended countermeasures appear in literature that is more than five years old, respondents to the current researcher's questionnaire indicated that these countermeasures were in use on their campuses. This finding presents an interesting conclusion. While the purpose of the current research was not to investigate new trends in computer and information security, it would appear that many of the countermeasures in place at colleges and universities represent old technologies. The top five countermeasures in place are ID and password authentication, external firewalls, strong password policies, virus scanning, and user training, technologies that have been commonly used for a number of years. Perhaps it is feasible to consider the idea that the field of computer security in higher education is in need of newer ideas and technology.

Beebe and Rao (2005) discussed the imbalance of common computer security countermeasures as found in Table 1. They found that 79% of commonly utilized countermeasures affected the perceived cost/risk of the crime, while only 16.3% of the countermeasures affect the perceived benefit of the crime, and only 4.7% removed the criminal's excuses for possibly committing the crime. Using data from Table 18 of the present study, it is interesting to note the categories of countermeasures that are not widely utilized in higher education. Countermeasures that are related to surveillance and monitoring are not widely used. For example, only seven of 89 institutions reported that they monitored employees' email, and only three of 89 institutions reported that they monitored employees' web usage. Despite literature related to inappropriate use of email (Fortiva, 2005), higher education institutions appear to be reluctant to use monitoring as a countermeasure. This is most likely due to the culture of higher education, balancing academic freedom with the need for control of technology. While higher education professors demand a certain amount of autonomy in terms of technology, campus technology security professionals must continue to exert control over classroom computers and other technology resources. Therefore, there is a constant struggle between a computer security specialist's need to implement a strong security plan and academia's need to exchange ideas and encourage exploration (Oblinger, 2003).

In terms of this study, countermeasures related to surveillance and monitoring would fall under the construct of Increase Perceived Effort. Though the null hypothesis was not rejected, the *t* statistic was 1.621, just under the critical value of 1.662. This relationship warrants further study. Perhaps refinement of the survey instrument would uncover a relationship with the proper associated significance.

Discussion of the categories of countermeasures would not be complete without addressing the rapid pace of change within technology. A countermeasure that is considered current at the time of this study may be outdated within a year or two. Readers of the overall findings of this study need to be cognizant of the passage of time and its relationship to technology.

Conclusions

The most obvious conclusion from this study could be that the lack of strong predictive findings for each category of Increase Perceived Effort, Increase Perceived Risk, Decrease Anticipated Rewards, and Remove Excuses suggests that Situational Crime Prevention Theory is not an ideal model for combating insider computer misuse on college campuses. However, it cannot be ignored that this particular study is exploratory in nature. Further, the respondents' inconsistent nature of reported incidents of insider computer misuse, as noted by the number of outliers in the data, complicated the correlational data analysis for this particular study. With this in mind, the current researcher is reluctant to dismiss Situational Crime Prevention Theory as an ineffective model within the study of insider computer misuse. It is possible, however, that the manner in which the data were collected and analyzed could be improved upon.

One of the most significant conclusions from the current study is the apparent lack of knowledge related to the number of insider computer misuse incidents on each campus. The variability of the number of reported incidents combined with those who responded with a "don't know" to that particular question gives the impression that CIO's are making security decisions based on incomplete or incorrect data. Though the CIO's could simply be reluctant to share that particular piece of data, it is not likely that a

respondent would be willing to share information about the countermeasures in place at their campus by answering that part of the survey and then not be willing to share information about the number of computer misuse incidents. This area warrants further study.

From a security plan standpoint, this research provides some insight on the categories of countermeasures that exert an influence on reported incidents of computer security. A relationship exists between countermeasures that fall under the categories of Decrease Anticipated Rewards and Remove Excuses and the reported incidents of computer misuse, noting a positive relationship with Remove Excuses and a negative relationship with Decrease Anticipated Rewards. In light of Beebe and Rao's (2005) finding that only 16.3% of commonly utilized countermeasures would fall under the category of Decrease Anticipated Rewards, it would appear that security plans could be enhanced by the addition of countermeasures within this category.

Finally, it would appear from the data as a whole that colleges and universities are utilizing the most common countermeasures found in the literature. Additionally, the pilot study group was specifically asked if they utilized any countermeasures that were not listed on the questionnaire and none indicated an omission. With the assumption that the list of countermeasures on the questionnaire was complete, the glaring lack of monitoring utilization on campuses is important. Because of its innate culture, it could be that what necessarily works and is acceptable in the business world is not necessarily appropriate or acceptable in higher education. There is more study needed in this area.

Implications

Higher education administrators are taxed with creating efficient computer security plans that guard their electronic data and computer resources against misuse. Therefore, the data contained in this study can provide a benchmark for CIO's within higher education institutions to compare their countermeasures with those of other institutions. To date, most studies related to computer security have been conducted in the field of business and not within higher education. With access to a body of data related to computer security research within the field of higher education, administrators can create effective policies regarding computer security that more efficiently utilize ever-shrinking budgets.

Recommendations

Based on the experience gained during this research study, the current researcher makes four recommendations.

1. As this is an exploratory study, a future researcher may choose to alter the instrument or methodology in a way that makes correlational comparisons more feasible. Instead of asking respondents about the number of insider computer misuse incidents their campus has experienced, a series of questions about the effectiveness of groups of countermeasures may prove more fruitful for analysis. Additionally, utilizing the categories of computer misuse incidents in the instrument rather than asking for an exact number of incidents may improve the quality of the reported data.
2. A higher response rate would be ideal in a future study.

3. As factor analysis revealed construct loadings that were comparably low, a future study should revisit the categorization of countermeasures in order to build a stronger instrument.
4. Though the pilot study respondents did not indicate any omissions in the list of countermeasures on the current questionnaire, it might prove interesting to collect qualitative data that specifically asks the population if they utilize any other or newer technologies that are not present on the current questionnaire to combat computer misuse on their campus.

Dissemination

The data in this research study is valuable to a number of audiences within higher education. First, *Educause* was the first organization to complete a similar study of information technology security in higher education. Therefore, this subject matter would be of interest at one of their conferences. Second, the peer-reviewed *Journal of Higher Education Policy and Management* might provide an appropriate avenue for the dissemination of these results. According to the journal's aim and scope, their readership includes those higher education administrators who have the responsibility of developing policy. Third, the peer-reviewed *Informing Science Journal of an Emerging Transdiscipline* would be an additional avenue for publication. *Informing Science* aims to inform its readership about information systems through a lens of many different disciplines, including education.

The researcher plans to submit the results of this study within the next 12 months. After initial publication, the researcher plans to further refine the instrument and re-collect data using the same CIO contact list. This would serve two purposes. First,

refinement of the data instrument could yield stronger relationships and predictive value within the model. Second, utilizing the same CIO contact list could alleviate the problem of the researcher being viewed as an “outsider” gathering sensitive information security information.

REFERENCES

Aldhizer, G. R. (April, 2008). The insider threat. *Internal Auditor*, 71-73.

Anderson, L. S., Theodore, G. C., & Waldo, G. P. (1977). Formal and informal sanctions: A comparison of deterrent effects. *Social Problems, 25*, 103-114.

Audit Commission. (1998). *Ghost in the machine: An analysis of IT fraud and abuse*. London. Audit Commission Publications.

Backhouse, J., & Dhillon, G. (1995). Managing computer crime: A research outlook. *Computers & Security*, *14*(7), 645-651.

Beccaria, C. (1985). *Essay on crimes and punishments.* (H. Paolucci, Trans.). New York: Macmillan. (Original work published 1764).

Beebe, N. L., & Rao, V. S. (2005). Using situational crime prevention theory to explain the effectiveness of information systems security. *Proceedings of the 2005 SoftWars Conference.* Las Vegas, NV.

Berdahl, R. O., & McConnell, T. R. (1999). Autonomy and accountability. In P.G. Altbach, R.O. Berdahl & P.J. Gumport (Eds.), *American higher education in the twenty-first century* (pp. 70-88). Baltimore: The Johns Hopkins University Press.

Booker, Q. E. & Kitchens, F .L. (2010). Changes in employee intention to comply with organizational security policies and procedures factoring risk perception: A comparison of 2006 and 2010. *Issues in Information Systems, 11(*1), 649-658.

Briar, S., & Piliavin, I. (1965). Delinquency, situational inducements, and commitment to conformity. *Social Problems*, *13*(1), 35-45.

Burt, C. (1925). *The young delinquent*. London: University of London Press.

Chiang, E., & Assane, D. (2002). Copyright piracy on the university campus: Trends and lessons from the software and music industries. *The International Journal on Media Management, 4*(3), 145-149.

Chin, W. H. (1998). Partial least squares approach to structural equation modeling. In G.A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.

Clarke, R., (Ed). (1997). *Situational crime prevention: Successful case studies (2nd ed.).* Albany, NY: Harrow and Heston.

Clarke, R. V., & Cornish, D. B. (1983). *Crime control in Britain: A review of policy research.* Albany, NY:State University of New York Press.

Clarke, R. V., & Cornish, D. B. (1985). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933-948.

Cohen, A. M. (1998). *The shaping of American higher education.* San Francisco: Jossey-Bass.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112*(1), 155-159.

Cornish, D., & Clarke, R. V. (1986). *The reasoning criminal.* New York: Springer-Verlag.

Computer Security Institute Survey (2007). Retrieved September 15, 2008, from http://www.gocsi.com/.

Computer Security Institute Survey (2008). Retrieved September 20, 2009, from http://www.gocsi.com/.

Conger, S., Loch, K. D., & Helft, B. L. (1995). Ethics and information technology use: A factor analysis of attitudes to computer use. *Information Systems Journal, 5*(3), 161-184.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. Clarke (Ed.), *Crime prevention studies* (pp. 151-196). Monsey, NY: Criminal Justice Press.

Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, computer crime, and IS misuse at the university. *Communications of the ACM, 49*(6), 85-90.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

Department for Business Enterprise and Regulatory Reform Survey (2007). Retrieved September 18, 2008, from http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, *20*(8), 715-723.

Dominguez, C. M. F., Ramaswamy, M., Martinez, E. M., Cleal, M. G. (2010). A framework for information security awareness programs. *Issues in Information Systems, 11(*1), 402-409.

von der Embse, T. J., Desai, M. S., & Desai, S. (2004). How well are corporate ethics codes and policies applied in the trenches? *Information Management & Computer Security, 12*(2), 146-153.

Ekblom, P. (1988) ¨Situational crime prevention: Effectiveness of local initiatives. In P. Goldblatt, & C. Lewis (Eds.), *Reducing offending: An assessment of research evidence on ways of dealing with offending behaviour*. Home Office: London.

Fortiva, Inc. (2005). Risky business: New survey shows almost 70 percent of e-mail-using employees have sent or received e-mail that may pose a threat to businesses. Retrieved October 31, 2009, from http://www.harrisinteractive.com/news/newsletters/clientnews/fortiva2005.pdf.

Gabor, T. (1990). Preventing crime: current issues and debates. *Canadian Journal of Criminology, 32*(1).

Gardner, H. (1985). *The mind's new science: A history of the cognitive revolution.* New York: Basic Books.

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the AIS, 16*, 91-109.

Gefen, D., Straub, D. W., & Boudreau, M. (2000). Structural equation modeling and regression: Guidelines for research and practice. *Communications of the AIS, 4*(7), 2-77.

Gibbs, J. P. (1975). *Crime, punishment and deterrence*. New York: Elsevier.

Grandjean, C. (1990). Bank robberies and physical security in Switzerland: A case study of the escalation and displacement phenomena, *Security Journal, 1*(1), 155-159.

Grasmick, H. G., & Green, D. E. (1980). Legal punishment, social disapproval, and internalization as inhibitors of illegal behavior. *Journal of Criminal Law and Criminology, 71*, 325-335.

Gumport, P. J., & Chun, M. (1999). Technology and higher education. Opportunities and challenges for the new era. In P. G. Altbach, R. O. Berdahl, & P. J. Gumport (Eds.), *American higher education in the twenty-first century* (pp. 370-395). Baltimore: The Johns Hopkins University Press.

Hafner, K., & Markoff, J. (1991). *Cyberpunk: Outlaws and hackers on the computer frontier*. New York: Simon & Schuster.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Hartshorne, H., & May, M. A. (1928). *Studies in the nature of character. Vol. 1: Studies in deceit*. New York: Macmillan.

Hoffer, J., & Straub, D. (1994). The 9 to 5 underground: Are you policing computer crimes? In P. Gray, W. King, E. Mclean, & H. Watson (Eds.), *Management of information systems* (pp. 388-401). Fort Worth, TX: Harcourt Brace.

Hollinger, R. (1988). Computer hackers follow a guttman-like progression. *Social Sciences Review, 72*, 199-200.

Hu, W., Tan, T., Wang, L., & Maybank, S. (2004). A survey on visual surveillance of object motion and behaviors. *IEEE Transactions on Systems, Man, and Cybernetics, 34*(3), 334-352.

Johnson, J. J., & Ugray, Z. (2007). Employee internet abuse: Policy vs. reality. *Issues in Information Systems, 8*(2), 214-219.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Keim, B. (2008). Large hadron collider's hacker infiltration highlights vulnerabilities. Retrieved September 30, 2008, from http://abcnews.go.com/Technology/story?id=5804254&page=1

Kesar, S., & Rogerson, S. (1998). Developing ethical practices to minimize computer misuse. *Social Science Computer Review, 16*(3), 240-251.

Keup, J., Walker, A., Astin, H., & Lindholm, J. (2001). Organizational culture and institutional transformation. (ERIC Digest No. ED 464521).

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*, 597-607.

Krauss, L., & MacGahan, A. (1979). *Computer fraud and countermeasures*. Englewood Cliffs, NJ: Prentice Hall, Inc.

Kvavik, R. B., & Voloudakis, J. (2006). *Safeguarding the tower: IT security in higher education 2006.* Retrieved October 3, 2009, from the EDUCAUSE Center for Applied Research Web site: http://net.educause.edu/ir/library/pdf/ecar_so/ers/ers0606/Ekf0606.pdf

Lacoste, J., & Tremblay, P. (2003). Crime and innovation: a script analysis of patterns in check forgery. In M. Smith, & M. Cornish (Eds.), *Theory for practice in situational crime prevention* (169-196). Monsey, NY: Criminal Justice Press.

Landreth, B. (1985). *Out of the inner circle.* Redmond, WA: Microsoft Books.

Levitt, S. (1996). The effect of prison population size on crime rates: Evidence from prison overcrowding litigation. *Quarterly Journal of Economics, 111,* 319-352.

Marvell, T., & Moody, C. (1994). Prison population growth and crime reduction. *Journal of Quantitative Criminology, 10,* 109-140.

Matza, D. (1964). *Delinquency and drift*. New York: John Wiley and Sons Inc.

Nagin, D. S. (1978). General deterrence: A review of the empirical evidence. In A. Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanction on crime rates* (95-139). Washington, D.C.: National Academy Press.

Nagin, D. S., & Paternoster, R. (1991). Preventative effects of the perceived risk of arrest: testing an expanded conception of deterrence. *Criminology, 29,* 561-585.

Nunnaly, J. (1967). *Psychometric theory*. New York: McGraw-Hill.

Nunnaly, J. & Bernstein, I. (1984). *Psychometric theory* (3rd ed.). New York: McGraw-Hill.

Oblinger, D. (2003). IT security and academic values. In M. Luker & R. Petersen (Eds.), *Computer and network security in higher education*. Retrieved October 17, 2009 from http://net.educause.edu/ir/library/pdf/pub7008e.pdf.

Osborne, K. (1998). Auditing the IT security function. *Computers & Security, 17*(1), 34-41.

Panko, R. R., & Beh, H. G. (2002). Monitoring for pornography and sexual harassment. *Communications of the ACM, 45*(1), 84-87.

Parker, D. (1997). The strategic values of information security in business. *Computers & Security, 16*(7), 572-582.

Parker, D. B. (1989). *Computer crime: Criminal justice resource manual.* National Institute of Justice, U.S. Department of Justice, 7-9.

Paternoster, R., & Bachman, R. (2001). *Explaining criminals and crime.* Los Angeles: Roxbury Publishing Co.

Paternoster, R., Saltzman, L. E., Waldo, G. P., & Chiricos, T. G. (1983). Perceived risk and social control: Do sanctions really deter? *Law and Society Review, 17,* 457-480.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in computing* (4th ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Soper, D. S. (2010) "The Free Statistics Calculators Website," Online Software, http://www.danielsoper.com/statcalc/

Samuelson, P. (1989). Can hackers be sued for damages caused by computer viruses? *Communications of the ACM, 32*(6), 666-669.

Short, J. F., & Strodtbeck, F. L. (1965). *Group process and gang delinquency.* Chicago: University of Chicago Press.

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity: Understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security, 10*(4), 178-183.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-464.

Tabachnick, B. G., & Fidell, L. S. (2001). *Using multivariate statistics*. Boston: Allyn and Bacon.

Tittle, C. R. (1980). *Sanctions and social deviance: The question of deterrence.* New York: Praeger Publishers.

Tizard, J., Sinclair, I. A, & Clarke, R.V. (1975). *Varieties of residential experience.* London: Routledge and Kegan Paul.

Tremblay, P., Talon, B., & Hurley, D. (2001). Bodyswitching and related adaptations in the resale of stolen vehicles. *British Journal of Criminology, 41*(4), 561-579.

Urbaczewski, A., & Jessup, L. M. (2002). Does electronic monitoring of employee Internet usage work? *Communications of the ACM, 45*(1), 80-83.

USDA security policies (n.d.). Security expectations and rules of behavior. Retrieved September 10, 2010 from ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures/SecurityExpectationsFlyer_Final.pdf.

VanPatten, J. J. (2000). *Higher education culture: Case studies for a new century.* Lanham, MD: University Press of America, Inc.

Verespej, M. A. (2000). Inappropriate internet surfing. *Indus. Week, 29*(3), 59-64.

von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.

Werts, C. E., Linn, R. L., & Jöreskog, K. G. (1974). Intraclass reliability estimates: Testing structural assumptions. *Educational and Psychological Measurement, 34*(1), 25-33.

Wilkinson, P. (1986). *Terrorism and the liberal state.* New York: New York University Press.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: a critical overview. *Law and Society Review, 20*, 545-572.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*(4), 304-324.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems, 15*, 403-414.

Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133-137.

Wolff, R. P. (1969). *The ideal of the university.* Boston: Beacon Press.

Appendices

Appendix A

Survey Instrument

1. Cover Letter

Please read the information provided below carefully. If you have any questions or concerns at this point or in the future, please feel free to contact:

Julie Santiago
Assistant Professor
Macon State College
(478) 471-2808
julie.santiago@maconstate.edu

WHAT IS THE PURPOSE OF THIS QUESTIONNAIRE?
The purpose of this questionnaire is to anonymously collect information about certain aspects of IT security and computer misuse in higher education. The data is to be utilized in a doctoral dissertation at Georgia Southern University.

WHAT WILL I NEED TO DO AS A RESPONDENT?
You will be presented with a series of questions regarding certain aspects of computer security on your campus. Please answer the questions as honestly as possible.

WHAT ARE THE RISKS AND BENEFITS TO ME?
The risks associated with participation in this study are minimal. It is possible that you may be reluctant to answer some of the questions. If this occurs, you may end the questionnaire at any time. To protect the participants, I have limited the information that I ask you to provide so neither you nor your institution can be identified in any way.

The results of my questionnaire may be beneficial to you by providing you, upon request, with information on what other colleges and universities are doing in the area of computer security. While my results are not able to be traced back to any particular institution, I can provide you with the data reported from schools of similar size.

ARE MY ANSWERS CONFIDENTIAL?
This questionnaire is completely anonymous. There are no questions on the questionnaire that could identify you in any way.

WHAT IF I DON'T WANT TO PARTICIPATE?
Your participation in this questionnaire is completely voluntary.

2.

* **1. What is the FTE (full-time equivalent enrollment) at your campus for the Fall 2009 semester? FTEs are calculated by adding the number of full-time students (normally a student taking 12 or more hours) to one-third the number of part-time students.**

* **2. This questionnaire is concerned with certain aspects of computer security, specifically computer misuse committed by insiders.**

For the purposes of this questionnaire, an insider is a current or former staff or faculty member.

For the purposes of this questionnaire, computer misuse includes activities such as inappropriate use of email or internet resources, software piracy, theft or destruction of data or hardware, and other activities usually noted in an Acceptable Use Policy or Code of Ethics. It should also be noted that computer misuse can be accidental, such as not following proper procedures.

With the above definitions in mind, how many insider computer misuse incidents did your campus experience in the year 2009?

3.

* **3. Please choose the countermeasures that are currently in place at your campus.**

- [ ] External firewall(s)
- [ ] Internal firewall(s)
- [ ] Servers with sensitive data under lock and key
- [ ] ID and password authentication systems
- [ ] Kerberos
- [ ] Access control list(s)
- [ ] Clearly defined job duties for employees
- [ ] Proxy servers
- [ ] Employees must use strong passwords
- [ ] Employees must change their passwords regularly
- [ ] Virus scanning
- [ ] Rules regarding joining the campus network
- [ ] Network log-in and log-out procedures for all employees
- [ ] Auditing and log reviews
- [ ] Employee email monitoring
- [ ] Employee web usage monitoring
- [ ] Review of resource usage information
- [ ] User training related to security policy
- [ ] Reporting policies for misuse incidents
- [ ] Workstations located in visible areas
- [ ] Conspicuously-placed cameras in data-sensitive areas
- [ ] Database partitioning/segmentation
- [ ] Use of database views
- [ ] Use of Virtual Private Networks
- [ ] Data classification based on sensitivity
- [ ] Tagged identification of campus hardware
- [ ] Tagged identification of campus software
- [ ] Use of a software inventory system

- [ ] Controlled distribution of campus software
- [ ] Use of screen saver lock on workstations
- [ ] Encryption (SSL, PGP, SSH, password encryption, etc.)
- [ ] Automatic data destruction mechanisms
- [ ] Network packet shaping
- [ ] Acceptable Use Policy
- [ ] User Agreements
- [ ] Clear rules and procedures
- [ ] Multiple dissemination methods of anti-misuse information
- [ ] Code(s) of ethics
- [ ] Cyber-ethics education
- [ ] Supervised computer use
- [ ] Employee access to only approved categories of web sites
- [ ] Offer software at reduced prices
- [ ] Required user training on proper use of campus systems

4.

* **4. In terms of effectiveness, choose the top five countermeasures for combating insider computer misuse in place at your campus from the list below. Then, rank those five using the drop-down menu at the right. Don't rank all the countermeasures, just your top five.**

	Rank
External firewall(s)	
Internal firewall(s)	
Servers with sensitive data under lock and key	
ID and password authentication systems	
Kerberos	
Access control list(s)	
Clearly defined job duties for employees	
Proxy servers	
Employees must use strong passwords	
Employees must change their passwords regularly	
Virus scanning	
Rules regarding joining the campus network	
Network log-in and log-out procedures for all employees	
Auditing and log reviews	
Employee email monitoring	
Employee web usage monitoring	
Review of resource usage information	
User training related to security policy	
Reporting policies for misuse incidents	
Workstations located in visible areas	
Conspicuously-placed cameras in data-sensitive areas	
Database partitioning/segmentation	

Use of database views	
Use of Virtual Private Networks	
Data classification based on sensitivity	
Tagged identification of campus hardware	
Tagged identification of campus software	
Use of an software inventory system	
Controlled distribution of campus software	
Use of screen saver lock on workstations	
Encryption	
Automatic data destruction mechanisms	
Network packet shaping	
Acceptable Use Policy	
User Agreements	
Clear rules and procedures	
Multiple dissemination methods of anti-misuse information	
Code(s) of ethics	
Cyber-ethics education	
Supervised computer use	
Employee access to only approved categories of web sites	
Offer software at reduced prices	
Required user training on proper use of campus systems	

5.

Thank you very much for your participation. Your contribution to this study is invaluable.

You may now click the Done button below or close your browser.

Appendix B

Pilot Study Invitation Letter

Dear Dr. _____:

Thank you so much for agreeing to participate in the pilot study for my dissertation at Georgia Southern University

I am conducting research related to IT security in higher education and the questionnaire asks questions related to certain computer security countermeasures and, therefore, clear terminology is very important. My pilot study will consist of responses from eight institutions within the University System. Your answers are completely anonymous as I ask no identifying information.

In addition to the questions that you answer as part of the questionnaire, I ask that you send me an email regarding any survey terms that you found confusing or that need more clarification, and give an estimation of the time it took you to complete it. Because your institution would be involved in the pilot study, I will not use your data in my final analysis.

Thank you again for your participation in the pilot study. Please do not hesitate to contact me if you have any questions. My contact information is through Macon State College, where I am also a faculty member in the School of Information Technology.

The link to the survey is: http://www.surveymonkey.com/s/5ZTMH2P
The password is: tdsbger94

Julie Santiago
Assistant Professor, School of Information Technology
Macon State College
100 College Station Drive
Macon GA 31206
(478) 471-2808

julie.santiago@maconstate.edu

Appendix C

Study Invitation Letter

Dear Dr. _____:

I am conducting research related to IT security in higher education as part of my doctoral studies at Georgia Southern University. I am specifically surveying public, four-year colleges and universities in the United States in order to learn more about the state of IT security on campuses nationwide.

If you would like to participate in the study, please click the following link. <insert SurveyMonkey link>. The survey is rather short and should only take about 10 minutes to complete. Additionally, your responses are completely anonymous and it is not possible to specifically identify your institution through the survey.

In exchange for your participation, I am willing to share my data with you upon request. Though I cannot identify specific colleges or universities, I can categorize the data based on institution size. Therefore, I can provide you with data related to colleges and universities that are similar in size to your own. Please email me at the address below if you would like a copy of this data.

Thank you again for your consideration. Please do not hesitate to contact me if you have any questions. My contact information is through Macon State College, where I am also a School of Information Technology faculty member. You may also contact Dr. Teri A. Melton, my research advisor at Georgia Southern University, at tamelton@georgiasouthern.edu or 912-478-0510 if you have any questions.

Julie Santiago
Assistant Professor, Macon State College
School of Information Technology
100 College Station Drive
Macon GA 31206

(478) 471-2808
julie.santiago@maconstate.edu

Appendix D

IRB Approval Letter

Georgia Southern University
Office of Research Services & Sponsored Programs

Institutional Review Board (IRB)

Phone: 912-478-0843
Fax: 912-478-0719 IRB@GeorgiaSouthern.edu
Veazey Hall 2021
P.O. Box 8005
Statesboro, GA 30460

To: Julie Santiago
169 Cambridge Way
Macon, GA 31220

cc: Charles E. Patterson
Associate Vice President for Research

From: Office of Research Services and Sponsored Programs
Administrative Support Office for Research Oversight Committees
(IACUC/IBC/IRB)

Date: January 28, 2010

Subject: Status of Application for Approval to Utilize Human Subjects in Research

After a review of your proposed research project numbered: **H10187**, and titled **"The Relationship Between Situational Crime Prevention Theory and Campus Employee Computer Misuse"**, it appears that your research involves activities that do not require full review by the Institutional Review Board according to federal guidelines. **You are approved to enroll 637 subjects.**

According to the Code of Federal Regulations Title 45 Part 46, your research protocol is determined to be exempt from full IRB review under the following exemption category(s):

- ☐ Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless: (I) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (II) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

Therefore, as authorized in the Federal Policy for the Protection of Human Subjects, I am pleased to notify you that your research is exempt from IRB approval. **You may proceed with the proposed research.**

Sincerely,

Eleanor Haynes
Compliance Officer

Appendix E

Raw Data

Raw Data for Incidents and Increase Perceived Effort
Records 1 – 47

Incidents	TH1	TH2	TH3	AC1	AC2	AC3	DO1	DO2	CF1	CF2
1	1	0	1	1	0	0	1	1	1	1
1	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	0	0	1	1	1	0
3	1	0	1	1	1	1	1	0	1	1
1	1	1	1	1	1	1	1	0	1	1
1	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1
5	1	1	0	1	0	0	0	0	0	1
3	1	1	1	1	1	1	1	0	1	0
0	1	1	1	1	1	1	1	0	1	0
0	1	1	1	1	0	1	1	1	1	0
1	1	1	1	1	0	1	1	1	1	1
5	0	1	1	1	1	1	1	0	1	1
1	1	1	1	1	0	1	1	0	1	1
1	0	1	0	1	0	1	1	0	1	1
1	1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	0	0	1	0	1	1
1	1	0	1	1	0	1	1	0	1	1
1	1	0	1	1	0	1	1	1	1	1
0	1	1	1	1	0	1	0	1	1	1
4	1	1	1	1	0	1	1	1	1	1
0	1	0	1	1	1	1	1	0	1	1
0	1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	1	0	0	0	0
0	1	1	1	1	0	1	1	0	0	1
0	0	1	1	1	0	1	0	0	0	0
0	1	1	1	1	0	1	1	0	1	1
0	1	1	1	1	0	0	1	0	0	1
1	1	0	0	1	1	1	0	0	0	0
5	0	1	1	1	1	1	1	1	1	0
2	1	1	1	1	0	1	1	1	1	1
0	1	1	1	1	0	1	0	0	0	1
4	0	1	0	0	1	1	0	1	0	1
1	1	1	1	1	0	1	1	1	1	1
0	1	0	0	1	0	1	1	0	1	1
0	1	1	1	1	1	1	1	1	1	0
1	0	1	1	1	1	1	1	0	1	1
1	1	1	1	1	1	1	1	0	1	1
1	1	1	1	1	1	1	1	1	1	0
3	1	1	1	1	0	1	1	0	1	1
5	1	1	1	1	1	1	1	0	1	1
0	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	0	1	1	1	1	1
2	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	0	1	1	0	1	0

Raw Data for Incidents and Increase Perceived Effort
Records 48 – 89

Incidents	TH1	TH2	TH3	AC1	AC2	AC3	DO1	DO2	CF1	CF2
1	1	1	1	1	0	1	1	1	1	0
1	0	1	1	1	1	1	1	0	1	0
0	0	1	1	1	0	1	1	0	0	1
1	0	1	1	1	1	1	1	0	1	0
1	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	1	1
1	1	1	1	1	0	1	1	0	1	1
2	1	1	1	1	0	1	1	0	0	1
5	1	0	1	1	1	0	1	1	1	1
4	1	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	1	0	1	1	1
1	1	1	1	1	0	1	0	0	1	1
5	1	1	0	1	1	1	1	0	1	1
1	1	1	1	1	1	1	1	1	1	1
0	1	0	1	1	0	0	1	1	1	0
4	1	1	1	1	0	1	1	1	1	1
0	1	1	1	1	0	1	0	0	1	1
4	1	1	1	1	0	1	1	0	1	1
1	1	1	1	1	0	1	1	0	0	1
1	1	1	0	1	1	1	0	0	1	0
1	1	0	1	1	0	1	0	1	0	1
1	1	0	1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1	0	1	0
5	1	1	1	1	0	0	1	0	0	1
2	1	1	1	1	0	1	1	0	1	1
1	1	0	1	1	0	1	0	0	0	0
2	1	1	1	1	0	1	1	1	1	1
0	1	0	1	1	0	1	1	0	1	1
0	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	0	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1
1	0	1	1	1	0	1	1	0	1	1
1	1	1	1	1	0	0	1	1	1	1
0	1	1	1	1	1	1	1	0	1	1
5	1	1	1	1	0	1	0	0	0	1
3	0	1	1	1	0	1	1	0	1	1
0	1	1	1	1	0	0	1	1	1	1
1	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1	0	1	1
1	1	1	1	1	0	1	1	0	0	1
2	1	1	1	1	1	1	0	1	1	1
1	0	1	1	1	0	1	0	1	1	1

Raw Data for Increase Perceived Risk
Records 1 – 47

EES1	EES2	EES3	FS1	FS2	FS3	SE1	SE2	SE3	NS1	NS2
1	1	1	1	1	1	1	0	0	1	1
1	0	0	1	0	0	0	1	1	0	0
1	0	1	1	0	0	0	1	1	0	0
1	1	0	1	0	1	0	0	1	1	0
1	1	1	1	0	0	0	1	1	1	1
1	1	1	1	0	0	0	1	1	0	0
1	1	1	0	0	0	0	1	1	1	0
1	0	0	0	0	0	0	0	0	0	0
1	1	1	1	0	0	1	1	1	0	0
1	1	1	1	0	0	1	1	1	0	0
1	1	0	1	0	0	0	1	1	0	1
1	0	0	1	1	1	1	1	1	1	0
1	1	0	1	0	0	1	0	1	0	0
1	1	1	1	0	0	0	1	0	0	0
1	1	0	1	0	0	0	1	0	0	1
1	1	1	1	0	0	1	1	1	1	1
1	1	1	1	0	0	1	1	1	1	1
1	1	1	1	0	0	1	1	0	1	0
1	1	1	1	0	0	1	0	1	1	0
1	1	1	1	0	0	0	1	0	1	0
1	0	1	1	0	0	0	1	1	0	0
1	0	0	1	0	0	0	0	0	1	0
1	1	1	1	0	0	0	1	1	1	1
1	1	0	1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	1	1	0	1
1	1	0	1	0	0	0	0	0	0	1
1	1	1	1	0	0	0	1	1	1	1
1	1	1	0	0	0	0	0	1	1	0
1	1	0	0	0	0	1	0	1	0	1
1	1	1	1	0	0	0	1	1	0	0
1	1	1	1	1	0	0	1	1	1	1
1	1	0	1	0	0	0	0	1	0	1
0	0	0	0	0	0	0	0	1	0	0
1	1	0	1	0	0	0	1	1	0	0
1	1	0	1	1	0	0	1	1	0	0
1	1	1	1	0	0	1	1	1	0	1
1	1	0	1	0	0	1	1	1	0	1
1	1	1	0	0	0	0	0	1	1	0
1	1	1	1	0	0	1	1	1	1	1
1	1	0	1	0	0	0	1	1	0	1
1	1	1	1	0	0	1	1	1	0	1
1	1	0	1	0	0	0	0	0	0	1
1	1	0	1	0	0	0	1	1	0	0
1	1	1	1	1	0	1	1	1	1	1
1	0	1	1	0	0	1	1	1	1	1

Raw Data for Increase Perceived Risk
Records 48 – 89

EES1	EES2	EES3	FS1	FS2	FS3	SE1	SE2	SE3	NS1	NS2
1	1	1	0	0	0	1	0	1	0	0
1	0	0	0	0	0	1	1	0	0	0
1	1	0	1	0	0	0	0	1	0	0
1	1	1	1	0	0	0	0	1	0	0
1	0	1	1	0	0	1	1	1	0	1
1	1	1	1	0	0	1	1	1	0	1
1	1	1	1	0	0	0	0	0	0	0
1	1	1	1	0	0	1	1	1	1	0
1	1	0	1	0	0	1	0	1	0	0
1	1	1	1	0	0	0	1	1	1	0
0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	1	1	0	0
1	0	0	0	0	0	0	1	1	0	0
1	0	0	0	0	0	0	1	1	0	0
1	0	1	1	0	0	1	1	1	1	0
1	1	1	0	0	0	0	1	0	0	0
1	1	1	1	0	0	1	1	1	0	0
1	0	0	0	0	0	0	1	0	0	0
1	1	1	0	0	0	1	1	1	1	0
1	0	0	1	0	0	0	0	1	0	0
1	0	1	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1	0	0	0
1	1	1	1	1	0	0	1	1	1	1
1	0	0	1	1	0	0	1	1	1	0
1	0	1	0	0	0	0	1	1	1	0
1	1	0	0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	1	1	0	1
1	1	1	0	0	0	1	1	1	0	0
1	1	1	0	0	0	0	1	1	0	0
1	0	1	0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	1	1	1	0
1	1	1	1	0	0	1	1	1	0	1
1	1	0	0	0	0	0	1	0	0	0
1	1	1	1	0	0	1	1	1	0	0
1	1	1	1	0	0	0	1	1	1	0
1	1	1	0	0	0	0	1	1	1	0
1	1	0	0	0	0	0	0	1	0	0
1	0	1	1	0	0	1	0	1	0	0
1	1	0	1	0	0	0	1	1	1	1
1	1	1	0	0	0	0	1	1	1	0
1	1	1	1	0	0	0	1	1	0	1
1	0	0	1	0	0	0	1	1	0	0
1	0	0	0	0	0	0	0	1	1	0

Raw Data for Decrease Anticipated Rewards
Records 1 – 47

TR1	TR2	TR3	IP1	IP2	IP3	RT1	RT2	RT3	DB1	DB2	DB3
0	0	0	0	1	1	1	0	0	1	0	0
1	1	1	1	1	0	0	1	1	1	0	1
1	1	1	1	1	0	1	0	1	1	0	1
1	1	1	1	1	0	0	1	0	1	0	1
1	1	1	0	0	0	0	1	1	1	0	0
1	0	1	1	0	0	0	1	1	1	0	1
1	1	1	1	1	0	1	1	0	1	0	1
0	0	1	0	1	0	0	0	1	1	0	1
1	1	1	1	1	0	0	0	1	1	0	1
1	1	1	1	0	0	1	0	1	1	0	1
1	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	1	1	0	0
0	1	1	1	1	0	0	0	1	1	0	0
0	0	1	0	0	0	1	1	1	1	0	0
1	1	1	1	1	0	0	1	1	1	0	0
1	1	1	1	1	1	1	1	1	1	0	1
1	1	0	0	1	0	0	1	0	1	1	1
0	1	1	0	1	0	0	1	1	1	0	1
1	1	0	0	1	0	1	1	0	1	0	1
1	1	1	1	1	0	1	1	0	1	0	1
0	1	1	1	1	0	1	1	1	1	0	1
1	0	1	1	1	1	0	1	1	1	0	0
1	1	1	1	1	1	0	1	1	1	0	1
0	1	0	0	1	0	0	0	1	1	0	1
1	1	1	1	1	1	0	1	1	1	0	1
0	1	1	0	1	0	0	0	0	1	0	0
1	1	1	1	1	0	0	1	1	1	1	1
0	0	1	1	0	0	0	0	1	1	1	1
1	0	1	0	0	0	0	1	1	1	0	1
1	1	1	1	1	0	0	0	1	1	0	1
1	1	1	1	1	1	1	1	1	1	0	1
1	0	1	0	0	0	0	1	1	1	0	1
1	0	0	1	1	0	0	0	0	0	0	0
1	1	1	1	0	0	1	1	0	1	0	1
0	0	1	1	0	0	1	1	1	1	0	0
1	1	1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	0	1	1	1	1	0	0
0	0	1	0	0	0	0	1	0	1	0	0
1	1	1	1	1	0	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1	1	0	1
1	1	1	1	1	1	1	1	1	1	0	1
0	1	1	0	0	0	0	1	1	1	0	1
1	1	1	1	0	0	1	1	0	1	0	1
0	1	1	1	1	0	0	1	1	1	0	1
0	1	1	1	1	1	1	1	1	1	0	1

Raw Data for Decrease Anticipated Rewards
Records 48 – 89

TR1	TR2	TR3	IP1	IP2	IP3	RT1	RT2	RT3	DB1	DB2	DB3
1	1	1	0	1	0	0	1	0	0	0	1
0	0	1	1	1	0	0	1	1	1	1	1
0	0	1	1	1	0	1	0	0	1	0	0
1	0	1	1	1	0	0	1	0	0	0	0
0	0	1	1	1	1	1	0	1	1	0	1
1	1	1	1	1	0	1	1	1	1	0	1
0	1	1	1	1	0	0	0	0	0	0	0
1	1	1	1	1	0	0	1	1	1	0	1
0	0	1	1	1	0	1	1	1	1	0	1
0	0	1	1	1	0	1	1	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	1	0	1
0	0	1	1	0	0	1	0	1	1	0	0
0	0	0	1	0	0	0	1	0	0	0	0
0	1	1	1	1	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0	1	1	0	1
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	1	0	0	0	0	1	0	1
0	0	1	1	1	0	0	1	1	1	0	0
1	1	1	0	0	0	0	0	1	0	0	1
1	1	1	0	0	0	0	1	0	1	0	0
0	0	1	1	1	0	0	1	1	1	0	1
1	1	1	0	1	0	1	1	1	1	0	1
1	1	1	1	1	0	0	0	1	1	0	1
1	1	1	0	0	0	0	0	0	1	0	1
1	1	1	1	0	0	1	1	1	0	0	0
1	1	1	0	1	1	0	1	1	0	1	0
0	1	1	0	0	0	0	1	1	1	0	1
1	0	1	1	1	0	0	0	1	1	0	0
0	1	1	0	1	0	0	1	0	1	0	1
1	1	1	1	1	1	0	0	1	1	0	1
1	1	1	1	1	1	0	1	1	1	0	1
1	1	1	0	0	0	0	0	0	1	0	1
1	1	1	1	1	1	0	1	1	1	1	1
1	1	1	1	1	0	1	1	1	1	0	1
1	1	1	1	1	0	0	0	1	1	0	0
0	0	1	0	0	0	0	1	1	1	0	1
1	0	1	0	1	0	1	1	1	1	1	1
1	1	1	1	1	0	0	1	1	1	1	1
1	1	1	1	0	0	1	1	1	1	0	1
0	1	1	0	1	0	0	1	1	0	0	1
1	1	1	1	1	0	0	1	1	1	0	1
1	0	1	0	0	0	0	1	1	1	0	0

Raw Data for Remove Excuses
Records 1 – 47

RSC1	RSC2	RSC3	SC1	SC2	CD1	CD2	CD3	FC1	FC2
0	1	1	0	1	0	0	0	0	0
1	0	1	1	0	0	0	0	1	0
1	1	1	0	0	0	0	0	1	1
1	1	1	0	0	0	0	0	1	0
1	0	1	0	0	0	1	0	0	0
1	1	1	1	1	0	0	0	0	0
1	1	0	0	1	1	0	0	0	0
1	0	0	0	0	0	0	0	0	0
1	1	1	1	1	0	0	0	1	1
1	1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	1	0	1	0
1	0	1	1	0	0	1	0	1	1
1	0	0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	1	0	0
1	1	1	1	1	0	0	0	0	0
1	1	1	1	1	1	1	0	1	1
1	0	1	1	1	0	0	1	1	0
1	0	1	0	0	0	0	0	0	0
1	0	1	1	1	0	0	0	1	1
1	1	0	0	0	0	0	0	0	0
1	1	1	1	0	1	0	0	1	1
1	0	0	0	0	0	0	0	1	0
1	1	1	1	1	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	0
1	1	0	0	0	0	0	0	1	1
1	1	1	1	1	1	1	0	1	1
1	0	1	1	0	1	0	0	1	0
1	0	0	1	1	1	0	1	1	0
0	0	0	0	0	0	0	0	1	0
1	0	0	1	1	0	0	0	1	1
1	1	0	0	0	0	0	0	0	0
1	1	1	1	1	0	0	1	1	1
1	1	1	1	1	1	0	0	1	0
1	0	0	0	0	0	0	0	1	1
1	1	1	1	1	1	0	0	1	1
1	1	1	1	1	1	0	0	1	0
1	1	1	1	1	1	1	0	1	1
1	1	0	0	1	0	0	0	0	0
1	1	1	1	1	0	0	0	1	1
1	1	1	1	1	1	0	0	1	1
1	0	1	1	0	0	1	0	1	1

Raw Data for Remove Excuses
Records 48 – 89

RSC1	RSC2	RSC3	SC1	SC2	CD1	CD2	CD3	FC1	FC2
1	1	1	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0	1	0
1	1	0	0	0	0	0	0	1	0
1	0	1	0	0	0	0	0	1	1
1	0	1	0	1	0	0	0	1	0
1	1	1	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	1	1
1	1	1	1	1	1	0	0	1	1
1	1	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	1	0	0
1	0	1	0	0	0	0	0	1	0
1	1	1	1	1	1	0	0	1	1
1	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	1	0
1	1	0	0	0	0	0	0	1	0
1	1	0	0	0	0	1	0	1	0
1	0	0	0	1	0	0	0	1	0
1	1	1	0	1	0	0	0	1	1
1	0	0	1	1	1	0	0	1	1
1	1	1	0	0	1	0	0	1	1
1	1	1	0	0	0	0	0	1	0
1	0	1	0	0	1	0	0	0	0
1	0	1	1	1	1	0	0	1	0
1	1	1	0	0	0	0	0	1	1
1	1	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	0	0	0
1	1	1	1	1	0	0	0	1	0
1	1	1	0	1	0	0	0	1	0
1	1	1	1	1	0	0	1	0	1
1	1	1	1	0	0	0	0	1	1
1	1	1	0	0	0	0	0	1	1
1	0	0	0	0	0	0	0	1	0
1	0	1	0	1	0	0	0	1	0
1	0	1	1	0	0	0	0	1	1
1	0	0	0	1	0	0	0	1	1
1	0	1	0	0	0	0	0	0	0
1	1	1	0	1	0	0	0	1	0
1	0	0	0	0	0	0	0	1	0

Appendix F

PLS-Graph Licensing Agreement

PLS-Graph User's Guide, Version 3.0, February, 2001 edition Wynne W. Chin (author)
Copyright Notice

SOFT MODELING SOFTWARE LICENSE AGREEMENT
The following constitutes the terms of the License Agreement between a single user (User) of this software package, and the producer of the package, Soft Modeling, Inc. (called Soft Modeling hereafter). By opening the package, you (the User) are agreeing to become bound by the terms of this agreement.

If you do not agree to the terms of this agreement do not open the package, and contact the Soft Modeling Customer Service Department at a local Soft Modeling office (or an authorized Soft Modeling reseller) in order to obtain an authorization number for the return of the package. This License Agreement pertains also to all third party software included in or distributed with Soft Modeling products.

License
Unless explicitly stated on the program media (CD or disks), the enclosed software package are sold to be used on one computer system by one user at a time. This License Agreement explicitly excludes renting or loaning the package. Unless explicitly stated on the program media, this License Agreement explicitly excludes the use of this package on multi-user systems, networks, or any time-sharing systems. (Contact Soft Modeling concerning Multi-user License Programs.) The user is allowed to install the software package on a hard disk and make a backup copy for archival purposes. However, the software will never be installed on more than one hard disk at a time. The documentation accompanying this software package (or any of its parts) shall not be copied or reproduced in any form.

Disclaimer of Warranty
Although producing error free software is obviously a goal of every software manufacturer, it can never be guaranteed that a software program is actually free of errors. Business and scientific application software is inherently complex (and it can be used with virtually unlimited numbers of data and command settings, producing idiosyncratic operational environments for the software); therefore, the User is cautioned to verify the results of his or her work. This software package is provided "as is" without warranty of any kind. Soft Modeling and distributors of Soft Modeling software products make no representation or warranties with respect to the contents of this software package and specifically disclaim any implied warranties or merchantability or fitness for any particular purpose.

In no event shall Soft Modeling be liable for any damages whatsoever arising out of the use of, inability to use, or malfunctioning of this software package. Soft Modeling does not warrant that this software package will meet the User's requirements or that the operation of the software package will be uninterrupted or error free.

Limited Warranty

If within 30 days from the date when the software package was purchased (i.e., invoice date), the program media (CD or disks) are found to be defective (i.e., they are found to be unreadable by the properly aligned media drive of the computer system on which the package is intended to run), Soft Modeling will replace the media free of charge. After 30 days, the User will be charged for the replacement a nominal disk replacement fee.

If within 30 days from the date when the software package was purchased (i.e., invoice date), the software package was found by the User not capable of performing any of its main (i.e., basic) functions described explicitly in promotional materials published by Soft Modeling, Soft Modeling will provide the User with replacement media free of defects (or a replacement component downloadable from the Soft Modeling WEB site), or if the replacement cannot be provided within 90 days from the date when Soft Modeling was notified by the User about the defect, the User will receive a refund of the purchasing price of the software package.

Updates, Corrections, Improvements

The User has a right to purchase all subsequent updates, new releases, new versions, and modifications of the software package introduced by Soft Modeling for an update fee or for a reduced price (depending on the scope of the modification); however, purchasing an update or upgrade (for a reduced price) constitutes a replacement of an existing license and not acquisition of a new license.

Soft Modeling is not obligated to inform the User about new updates, improvements, modifications, and/or corrections of errors introduced to its software packages. In no event shall Soft Modeling be liable for any damages whatsoever arising out of the failure to notify the User about a known defect of the software package.

Appendix G

Bootstrap Data Output

Output results with Construct Level sign change preprocessing:

Bootstrap raw data generated for Julie Santiago

Number of cases in full model: 89

Number of cases per sample: 89

Number of samples generated: 200

Number of good samples: 200

Outer Model Weights:

	Original sample estimate	Mean of subsamples	Standard error	T-Statistic
Incident:				
Incident	1.0000	1.0000	0.0000	0.0000
IPE :				
TH1	0.2392	0.2088	0.3046	0.7852
TH3	0.4385	0.3473	0.2277	1.9256
AC1	0.3821	0.3178	0.2144	1.7819
DO1	0.0824	0.0654	0.2327	0.3541
DO2	0.1629	0.1293	0.2102	0.7751
CF1	0.2343	0.1842	0.1884	1.2434
IPR :				
EES1	0.5342	0.4627	0.2299	2.3232
EES2	0.2439	0.2359	0.2389	1.0211
FS1	0.3243	0.2790	0.2189	1.4818
NS2	0.4111	0.3830	0.2482	1.6564
DAR :				
TR1	0.1870	0.1623	0.2277	0.8211
TR3	0.4948	0.3966	0.1797	2.7532
RT2	0.3003	0.2359	0.2730	1.1001
RT3	0.0940	0.0206	0.2698	0.3484
DB1	0.3446	0.2938	0.1615	2.1340
DB2	0.3850	0.3794	0.1941	1.9835
RE :				
SC1	0.0901	0.0891	0.2151	0.4190
CD1	0.5920	0.4807	0.2168	2.7310
CD2	0.1388	0.1197	0.2304	0.6024
CD3	-0.3554	-0.2859	0.2546	1.3960
FC1	0.4298	0.3517	0.2227	1.9298

FC2	0.1440	0.1137	0.2031	0.7089

Outer Model Loadings:

	Original sample estimate	Mean of subsamples	Standard error	T-Statistic
Incident:				
(Composite Reliability =	1.000 , AVE =	1.000)		
Incident	1.0000	1.0000	0.0000	0.0000
IPE :				
(Composite Reliability =	0.770 , AVE =	0.377)		
TH1	0.3629	0.3255	0.3318	1.0938
TH3	0.8153	0.6703	0.2669	3.0552
AC1	0.7811	0.6534	0.2572	3.0369
DO1	0.5518	0.4518	0.2864	1.9266
DO2	0.4012	0.3156	0.2680	1.4970
CF1	0.6250	0.5113	0.2414	2.5890
IPR :				
(Composite Reliability =	0.743 , AVE =	0.421)		
EES1	0.7129	0.6223	0.2612	2.7291
EES2	0.5729	0.5342	0.2195	2.6096
FS1	0.6427	0.5700	0.2295	2.8008
NS2	0.6591	0.6098	0.2058	3.2020
DAR :				
(Composite Reliability =	0.695 , AVE =	0.281)		
TR1	0.3780	0.3327	0.2601	1.4535
TR3	0.6803	0.5601	0.2348	2.8978
RT2	0.5284	0.4472	0.2737	1.9304
RT3	0.4837	0.3608	0.2949	1.6404
DB1	0.5433	0.4320	0.2421	2.2437
DB2	0.5230	0.5021	0.1925	2.7168
RE :				
(Composite Reliability =	0.679 , AVE =	0.277)		
SC1	0.4847	0.4254	0.2605	1.8604
CD1	0.7529	0.6430	0.2134	3.5275
CD2	0.3574	0.3048	0.2913	1.2269
CD3	-0.3378	-0.2846	0.2752	1.2273
FC1	0.6412	0.5416	0.2305	2.7819
FC2	0.4537	0.3867	0.2585	1.7549

Path Coefficients Table (Original Sample Estimate):

	Incident	IPE	IPR	DAR	RE
Incident	0.0000	-0.1210	-0.1930	-0.2030	0.3920
IPE	0.0000	0.0000	0.0000	0.0000	0.0000
IPR	0.0000	0.0000	0.0000	0.0000	0.0000
DAR	0.0000	0.0000	0.0000	0.0000	0.0000
RE	0.0000	0.0000	0.0000	0.0000	0.0000

Path Coefficients Table (Mean of Subsamples):

	Incident	IPE	IPR	DAR	RE
Incident	0.0000	-0.1787	-0.1678	-0.2037	0.3680
IPE	0.0000	0.0000	0.0000	0.0000	0.0000
IPR	0.0000	0.0000	0.0000	0.0000	0.0000
DAR	0.0000	0.0000	0.0000	0.0000	0.0000
RE	0.0000	0.0000	0.0000	0.0000	0.0000

Path Coefficients Table (Standard Error):

	Incident	IPE	IPR	DAR	RE
Incident	0.0000	0.1187	0.1191	0.1058	0.1453
IPE	0.0000	0.0000	0.0000	0.0000	0.0000
IPR	0.0000	0.0000	0.0000	0.0000	0.0000
DAR	0.0000	0.0000	0.0000	0.0000	0.0000
RE	0.0000	0.0000	0.0000	0.0000	0.0000

Path Coefficients Table (T-Statistic)

	Incident	IPE	IPR	DAR	RE
Incident	0.0000	1.0190	1.6208	1.9191	2.6970
IPE	0.0000	0.0000	0.0000	0.0000	0.0000
IPR	0.0000	0.0000	0.0000	0.0000	0.0000
DAR	0.0000	0.0000	0.0000	0.0000	0.0000
RE	0.0000	0.0000	0.0000	0.0000	0.0000

Appendix H

Partial-Least Squares Analysis

```
        P   L   S   G R A P H
                  for
       Partial Least Squares Analysis
             (2004 Feb 27)

     YEAR-MONTH-DAY: 2010-10-31
      HOUR:MIN:SECS: 19:39:23.

   (HOWDY PARDNER!!  HOW Y'ALL  DOING, EH?)
0    600000 = Available Field Length.
     600000 = Requested Field Length.

0CPU-Time =   0 min  0.00 sec
 Total =      0 min  0.00 sec

0     Comments..
 COMM
 PLS Deck generated for Julie Santiago
0JBL                                1.8
 ====================================
0--      P    L    S    X           --
0-- LATENT VARIABLES PATH ANALYSIS --
 - PARTIAL LEAST-SQUARES ESTIMATION -
0

0====================================
0Number of Blocks       NBLOCS =    5
 Number of Cases        NCASES =   89
 Number of Dimensions     NDIM =    1
0Output Quantity           OUT = 2255
 Inner Weighting Scheme  IWGHT =    1
 Number of Iterations    NITER =  100
 Estimation Accuracy       EPS =    5
 Analysed Data Metric   METRIC =    1
0====================================
 Block   N-MV Deflate LV-Mode   Model
 ------------------------------------
 Incident   1   yes   outward Endogen
 IPE        6   yes   outward  Exogen
 IPR        4   yes   outward  Exogen
 DAR        6   yes   outward  Exogen
 RE         6   yes   outward  Exogen
 ------------------------------------
          23               .
 ====================================

0Real words needed    3803 from 600000
0Char words needed     235 from  40000
1
0Dimension No.  1
0Partial Least-Squares Parameter Estimation
0Change of Stop Criteria during Iteration
0Cycle No.    CR1          CR2          CR3          CR4          CR5

    1  0.1355E+01  0.3912E-01  0.3558E+00  0.3290E+00  0.5296E+00
    2  0.5551E-15  0.1276E-01  0.1110E-15  0.1110E-15  0.2220E-15
0Convergence at Iteration Cycle No.   2
```

0B .. Path coefficients

	Incident	IPE	IPR	DAR	RE
Incident	0.000	-0.121	-0.193	-0.203	0.392
IPE	0.000	0.000	0.000	0.000	0.000
IPR	0.000	0.000	0.000	0.000	0.000
DAR	0.000	0.000	0.000	0.000	0.000
RE	0.000	0.000	0.000	0.000	0.000

0R .. Correlations of latent variables

	Incident	IPE	IPR	DAR	RE
Incident	1.000				
IPE	-0.244	1.000			
IPR	-0.299	0.520	1.000		
DAR	-0.286	0.544	0.516	1.000	
RE	0.292	0.223	0.156	0.211	1.000

0Inner Model

Block	Mean	Location	Mult.RSq	AvResVar	AvCommun	AvRedund
Incident	0.0000	0.0000	0.2594	0.0000	1.0000	0.2594
IPE	0.0000	0.0000	0.0000	0.6229	0.3771	0.0000
IPR	0.0000	0.0000	0.0000	0.5790	0.4210	0.0000
DAR	0.0000	0.0000	0.0000	0.7187	0.2813	0.0000
RE	0.0000	0.0000	0.0000	0.7232	0.2768	0.0000
Average			0.0519	0.6394	0.3606	0.0113

0Outer Model

Variable	Weight	Loading	Location	ResidVar	Communal	Redundan
Incident	outward					
Incident	1.0000	1.0000	0.0000	0.0000	1.0000	0.2594
IPE	outward					
TH1	0.2392	0.3629	0.0000	0.8683	0.1317	0.0000
TH3	0.4385	0.8153	0.0000	0.3353	0.6647	0.0000
AC1	0.3821	0.7811	0.0000	0.3899	0.6101	0.0000
DO1	0.0824	0.5518	0.0000	0.6955	0.3045	0.0000
DO2	0.1629	0.4012	0.0000	0.8391	0.1609	0.0000
CF1	0.2343	0.6250	0.0000	0.6094	0.3906	0.0000
IPR	outward					
EES1	0.5342	0.7129	0.0000	0.4917	0.5083	0.0000

EES2	0.2439	0.5729	0.0000	0.6718	0.3282	0.0000
FS1	0.3243	0.6427	0.0000	0.5869	0.4131	0.0000
NS2	0.4111	0.6591	0.0000	0.5656	0.4344	0.0000
DAR	outward					
TR1	0.1870	0.3780	0.0000	0.8571	0.1429	0.0000
TR3	0.4948	0.6803	0.0000	0.5372	0.4628	0.0000
RT2	0.3003	0.5284	0.0000	0.7208	0.2792	0.0000
RT3	0.0940	0.4837	0.0000	0.7660	0.2340	0.0000
DB1	0.3446	0.5433	0.0000	0.7048	0.2952	0.0000
DB2	0.3850	0.5230	0.0000	0.7265	0.2735	0.0000
RE	outward					
SC1	0.0901	0.4847	0.0000	0.7651	0.2349	0.0000
CD1	0.5920	0.7529	0.0000	0.4331	0.5669	0.0000
CD2	0.1388	0.3574	0.0000	0.8723	0.1277	0.0000
CD3	-0.3554	-0.3378	0.0000	0.8859	0.1141	0.0000
FC1	0.4298	0.6412	0.0000	0.5888	0.4112	0.0000
FC2	0.1440	0.4537	0.0000	0.7941	0.2059	0.0000

0Theta .. Outer residual covariance

	Incident	TH1	TH3	AC1	DO1	DO2	CF1
Incident	0.000						
TH1	0.000	0.868					
TH3	0.000	-0.210	0.335				
AC1	0.000	-0.175	-0.080	0.390			
DO1	0.000	-0.141	-0.044	-0.047	0.696		
DO2	0.000	0.013	-0.099	-0.270	-0.127	0.839	
CF1	0.000	-0.168	-0.198	-0.104	0.146	0.073	0.609
EES1	0.000	-0.037	-0.044	0.188	-0.104	-0.158	-0.040
EES2	0.000	-0.058	0.084	-0.078	0.131	-0.044	0.013
FS1	0.000	0.032	-0.008	-0.169	0.099	0.152	0.118
NS2	0.000	0.057	0.014	-0.065	-0.021	0.111	-0.048
TR1	0.000	0.001	0.003	-0.067	0.016	0.055	0.059
TR3	0.000	-0.122	0.064	0.142	-0.080	-0.115	-0.120
RT2	0.000	0.104	-0.136	-0.037	0.094	0.069	0.128
RT3	0.000	0.103	0.015	-0.024	0.078	-0.083	-0.065
DB1	0.000	-0.014	-0.029	-0.016	-0.071	0.058	0.080

DB2	0.000	0.062	0.045	-0.101	0.065	0.036	-0.031
SC1	0.000	0.054	-0.095	-0.095	0.061	0.194	0.122
CD1	0.000	0.070	0.016	-0.002	-0.030	-0.029	-0.068
CD2	0.000	0.043	-0.085	0.009	0.007	-0.021	0.111
CD3	0.000	0.042	0.029	-0.035	0.006	-0.032	-0.021
FC1	0.000	-0.131	0.059	0.000	0.000	0.003	0.022
FC2	0.000	0.131	-0.030	-0.026	0.091	-0.068	-0.019
Inc	0.000	-0.032	-0.022	-0.002	0.093	0.016	0.034
IPE	0.000	0.000	0.000	0.000	0.000	0.000	0.000
IPR	0.000	-0.049	-0.039	0.170	0.085	-0.163	-0.070
DAR	0.000	-0.081	-0.036	0.135	-0.041	-0.034	-0.032
RE	0.000	-0.109	0.040	-0.032	0.075	0.062	0.018

0Theta .. Outer residual covariance

	EES1	EES2	FS1	NS2	TR1	TR3	RT2
EES1	0.492						
EES2	0.159	0.672					
FS1	0.228	-0.163	0.587				
NS2	-0.364	-0.063	-0.069	0.566			
TR1	-0.179	0.102	0.118	0.080	0.857		
TR3	0.187	-0.026	-0.079	-0.166	-0.181	0.537	
RT2	-0.094	0.008	0.031	0.093	0.007	-0.216	0.721
RT3	-0.055	-0.070	0.016	0.100	-0.057	-0.001	-0.107
DB1	0.105	-0.044	-0.027	-0.089	-0.192	-0.108	-0.203
DB2	-0.161	0.034	0.040	0.157	-0.003	-0.337	-0.081
SC1	-0.134	0.034	0.197	-0.002	0.084	-0.191	0.098
CD1	-0.063	0.016	0.015	0.061	-0.021	-0.073	0.036
CD2	-0.071	-0.125	0.112	0.078	-0.023	-0.014	-0.001
CD3	-0.083	-0.018	0.088	0.049	0.062	-0.194	0.055
FC1	0.074	-0.020	-0.032	-0.059	0.036	-0.005	-0.013
FC2	-0.014	0.047	0.022	-0.027	0.100	-0.031	-0.033
Incident	-0.045	0.053	0.036	-0.001	0.025	-0.025	0.018
IPE	0.273	-0.109	-0.068	-0.236	-0.045	0.091	0.041
IPR	0.000	0.000	0.000	0.000	0.033	-0.072	0.085
DAR	0.143	-0.087	-0.075	-0.075	0.000	0.000	0.000
RE	-0.019	-0.014	0.012	0.023	0.248	0.010	-0.061

0Theta .. Outer residual covariance

	RT3	DB1	DB2	SC1	CD1	CD2	CD3
RT3	0.766						
DB1	-0.010	0.705					
DB2	-0.065	-0.238	0.726				
SC1	0.014	0.131	0.008	0.765			
CD1	0.032	-0.006	0.074	0.044	0.433		
CD2	0.020	0.030	-0.001	0.041	-0.020	0.872	
CD3	-0.071	-0.012	0.205	0.263	0.306	0.149	0.886
FC1	-0.092	-0.031	0.049	-0.048	-0.307	-0.141	0.145
FC2	-0.061	-0.021	0.050	0.095	-0.117	0.007	0.188
Incident	0.097	0.003	-0.021	-0.104	0.024	-0.047	-0.048
IPE	-0.111	0.052	-0.146	0.230	-0.011	0.008	0.176
IPR	0.071	0.062	-0.061	0.300	0.102	0.129	0.222
DAR	0.000	0.000	0.000	0.199	0.038	0.105	0.283
RE	0.102	-0.003	-0.108	0.000	0.000	0.000	0.000

```
0Theta  .. Outer residual covariance

================================================================================
====
             FC1       FC2       Incident  IPE       IPR       DAR
RE
 ------------------------------------------------------------------------------
-----
 FC1       0.589
 FC2       0.029     0.794
 Incident -0.010    -0.073     1.000
 IPE       0.065     0.134    -0.244     1.000
 IPR      -0.102     0.124    -0.299     0.520     1.000
 DAR       0.047     0.178    -0.286     0.544     0.516     1.000
 RE        0.000     0.000     0.292     0.223     0.156     0.211
1.000

================================================================================
===0        ==PLSW no prob, eh?
0CPU-Time =   0 min  0.01 sec
 Total =      0 min  0.01 sec
0        No errors reported.
```