CONTROL, PERCEIVED RISK AND INFORMATION SECURITY PRECAUTIONS: EXTERNAL AND INTERNAL MOTIVATIONS FOR SECURITY BEHAVIOR

by

Scott R. Boss

Bachelor of Science, Brigham Young University, 1994

Masters of Accountancy, Brigham Young University, 1994

Submitted to the Graduate Faculty of the

Joseph M. Katz Graduate School of Business

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2007

UNIVERSITY OF PITTSBURGH

Katz Graduate School of Business

This dissertation was presented

by

Scott R. Boss

It was defended on

July 11, 2007

and approved by

Laurie J. Kirsch, Ph.D., Chair
Professor of Business Administration
University of Pittsburgh

Jacob G. Birnberg, Ph.D.
Robert W. Murphy Jr. Professor of Control Systems
University of Pittsburgh

Brian S. Butler, Ph.D.
Associate Professor of Business Administration
University of Pittsburgh

Irene H. Frieze, Ph.D.
Professor of Psychology
University of Pittsburgh

Peter H. Gray, Ph.D
Assistant Professor of Management
University of Virginia

CONTROL, PERCEIVED RISK AND INFORMATION SECURITY PRECAUTIONS: EXTERNAL AND INTERNAL MOTIVATIONS FOR SECURITY BEHAVIOR

Scott R. Boss, Ph.D.

University of Pittsburgh, 2007

Computer security has become increasingly important to organizations as the number of security incidents skyrockets. While many technical means are used to secure corporate systems, individual employees remain the last line – and frequently the weakest link – in organizational defenses. When individuals choose to disregard security policies and procedures meant to protect the organization, they leave the organization at risk. How, then, can organizations motivate their employees to follow security guidelines? Using organizational control and the fear of crime as the lens, we build a model to examine this research question.

The research model examines the relationship between the elements of control (specification, evaluation, and reward), risk elements and risk antecedents (direct experience, indirect experience, and risk) and precautions that can be taken at the individual level which are typically motivated by organizational policies and procedures. The model also introduces the concept of "mandatoriness" which is generally not specifically highlighted in extant literature.

The specific hypotheses are developed and tested using a field survey. An organization was identified for data collection and 1,738 total responses were collected from a population of approximately 3,500. The model was tested using PLS analysis after examination of the data, scale reliability, and item validity.

The results from the analysis suggest that the acts of specifying a policy and evaluating behaviors are effective in convincing individuals that security policies and procedures are

mandatory. The perception of mandatoriness, in turn, is effective in motivating individuals to take security precautions. Likewise, both direct and indirect experience have a significant positive effect on perceptions of risk, but risk perceptions do not have any effect on the level of precautions taken by individuals.

The findings highlight the need for management to clearly specify computer security policies and procedures and to evaluate individual employee compliance with those policies. The findings also indicate that the perceived impact of specific scenarios is more likely to affect individual precaution taking behaviors than statistics indicating the likelihood that they will be affected. Additionally, managers need to address the problems of apathy as it relates to security and bolster individuals' efficacy as it relates to computers.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

Many people have played an important role not only in shaping this dissertation, but also in helping me through my entire doctoral program. I have been fortunate to work, study, and interact with many brilliant people who have never failed to challenge and inspire me. All of these people deserve much of the credit for any of my accomplishments, past or future.

I want to express my deep appreciation to Laurie Kirsch, my chair and advisor, for her direction and guidance over the past five years. Laurie has been and continues to be a role model for me and has shaped my views of academic life and research. Working with her has been an experience from which I will benefit throughout my academic career. She exemplifies what I hope to be as an academic and a researcher. Laurie has provided an excellent example of disciplined research that I hope to emulate.

I wish to thank Brian Butler for all that he has done for me during the last several years. He played an important role in crafting this research and also offered himself as a sounding board for ideas (some even relating to research) throughout my doctoral program. He has been a great friend and a fun colleague.

I want to express my gratitude to Peter Gray, Jake Birnberg and Irene Frieze for serving as members of my dissertation committee. These three helped me with various aspects of my dissertation and provided valuable feedback to help refine my ideas, improve my presentation,

and develop my research approach. They also provided much appreciated advice relating to not only research, but also to academic life and teaching that has made a difference to me.

I would also like to express my gratitude to Carrie Woods for her friendship and support throughout my experiences in the Katz School and to Jerry May and Dennis Galletta for advising me in an unofficial capacity and giving me opportunities to learn and grow. Thanks also to my friends and colleagues in the doctoral program (both students and teachers) who have helped me over the last six years. While there are too many people at school, in my professional community, and at church to thank individually, I owe a debt of gratitude to these people for helping me accomplish this goal.

I would particularly like to thank my parents for relating to me their experiences from their Ph.D. programs, facilitating completion of my research, and providing love, support, encouragement, faith, and advice throughout my time in graduate school. I would also like to thank all three of my parents for training me to think of obstacles as opportunities for growth and for providing me with the tools to excel at whatever I attempt. Likewise I'd like to thank my brothers and sister for their love, encouragement, support, and humor through the years.

Finally, my wife Libby and my daughters Beth and Sarah have given me the day-to-day support that was so necessary to complete this program. They have helped me cope with the stress and anxiety of graduate school as well as sharing with me the pleasures of accomplishment and unconditional love that at many times I did not deserve. Thank you three for being the most important part of my life and for hanging in with me throughout this program.

1.0 INTRODUCTION

The topic of computer security has received a great deal of attention in the popular media and in trade journals over the past ten years. For example, Ken Dunham, director of the Rapid Response Team at iDefense, is convinced that "There's a well-developed criminal underground market that's connected to the mafia in Russia and Web gangs and loosely affiliated mob groups around the world" (Naraine, 2006 p. 1). The risks of having poor security are generally well documented (Straub & Welke, 1998) and include identity theft, data loss, and appropriation of computer and telecommunications resources.

Alarmingly, the threat of attack is continuing to grow. A recent Internet study shows that there has been a marked increase in data theft and the creation of malicious code developed specifically to steal confidential information (Symantec Corporation, 2007). Cyber criminals are continuing to refine their attack methods to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity (Symantec Corporation, 2007). Accordingly, many companies view security as one of their top concerns (Dale & The Associated Press, 2006). There is evidence, however, that despite the efforts of organizations to secure their systems and data, they are still exposed to potential hackers in increasing numbers (Swartz, 2005) and individuals either do not view security as a top priority or do not realize that they are at risk (Frieze, Hymer, & Greenberg, 1987).

The CERT Coordination Center, a Pittsburgh, Pennsylvania-based center for security expertise, noted that the cost of electronic crimes to businesses exceeded $666 million in 2004 (CERT Coordination Center, 2004a) and it was estimated that U.S. organizations would spend in excess of $61 billion on Information Systems Security in 2006 (GRIDtoday, 2006). The number of security incidents reported by individuals and companies has increased steadily in the past, from approximately 21,000 in 2000 to more than 137,000 in 2003 (CERT Coordination Center, 2004b). Given the widespread use of automated attack tools, CERT (2004b) noted that attacks against Internet-connected systems are now so commonplace that the counts of incidents reported provide very little information to assess the scope and impact of attacks. CERT, in 2004, thus decided to discontinue reporting these statistics and to try to develop more appropriate measures of threat (CERT Coordination Center, 2004a).

Computer security refers to all necessary measures that assure that systems will behave as expected and produce reliable results (S. Garfinkel, Spafford, & Schwartz, 2003). Corporations typically address the issues of computer security through technical means, using centralized firewalls and other software to try to protect corporate data. However, to achieve secure systems and data requires more than a focus on the technical issues; it also requires attention from management (Dutta & McCrohan, 2002) to design effective computer security policies and to motivate individual behavior to follow those policies (National Cyber Security Alliance, 2005). Unfortunately, though extensive corporate measures are often put in place to protect data and systems, employees themselves often bypass extant computer security policies, exposing organizations to data loss and cybercrime (Dhillon & Backhouse, 2001). Jim Stickley, CEO of

Tracesecurity (a "white hat[1] hacking" security organization), notes that to illicitly obtain on-line access to corporate computer systems the easiest way to hack the system is to target the employees (Germain, 2007). Thus, organizations face a problem of how to promote security policies and procedures to individual employees in the most effective way.

Hardly a week goes by without some mention in the popular media regarding Internet (cyber) security threats to individuals. These notices usually take the form of a warning of either newly discovered weaknesses in extant operating systems or software (Associated Press, 2004) or new virus threats (Symantec Corporation, 2004). Hackers routinely scan groups of computer addresses looking for vulnerabilities, literally "testing the doorknobs" of computers linked to the Internet (Coren, 2005). Once a vulnerability has been found, hackers move to exploit that vulnerability. Many viruses perform similar functions, scanning for vulnerable machines and replicating through either scans or e-mails to other computers. This use of bandwidth is estimated to cost companies hundreds of millions of dollars every year (CERT Coordination Center, 2004a, 2004b; Chertoff, 2001; Coren, 2005). Further, the patterns of attack are accelerating as the financial payoff for compromising either individual or corporate data increases (Symantec Corporation, 2007).

Why are individuals targeted? At the organizational level networks are routinely protected by firewalls, corporate antivirus software, spam filters, etc. Additionally, organizations have the funds to hire security personnel who are dedicated entirely to the task of computer security within the firm as well as research security practices and possible future security threats.

---

[1] White hat hackers are individuals, typically consultants, who break into systems with the goal of helping the owners become aware of security flaws in their systems. These types of professionals differ from "black hat hackers" in that the black hats penetrate security without permission from the owners for their own purposes.

As noted earlier, in 2006 it was estimated that organizations would spend in excess of $61 billion on security with over half of that by the business service, financial service, and government sectors attempting to secure their computer systems (GRIDtoday, 2006). To bypass these controls, hackers target individuals because they can be used as a foothold to gain wider access within a larger organization (Germain, 2007) and can be reached through legitimate communications channels into the organization (i.e.: e-mail). Individuals are also targeted for a number of other reasons: to obtain financial information (credit card numbers, bank numbers, Social Security numbers, etc.), to co-opt computer resources (disk space, processor speed, Internet connection, etc.), and to advertise through e-mail and other cyber-media products (Rogers, 2002).

Effective security measures or cyber-precautions require effort at both the organizational and individual level. As noted above, corporations take extensive measures to protect corporate data assets and produce user policies to direct individual behavior. These efforts are typically reviewed by auditors for adequacy and to provide further guidance. At the individual level, widespread media publicity of both cyber-attacks and ways to combat them suggests that it is logical for individuals to put precautionary practices in place.

Yet many individuals do not take these cyber-precautions. Recent research shows that individuals do not consistently implement the most basic security measures. The National Cyber Security Alliance (NCSA), a not-for-profit, public-private partnership focused on driving awareness and promoting education of cyber security, recently performed a survey of 329 dial-up and broad-band computer users to examine their attitudes and views of computer security. Study participants were interviewed and then their computers were examined by computer specialists for common security issues (America Online & National Cyber Security Alliance, 2005). The

study revealed that approximately 75 percent of all respondents feel that their computer is very safe from online attack or from viruses. In keeping with these feelings of safety, 84 percent of respondents keep sensitive information on their computer and 72 percent use their computers for sensitive transactions such as banking or reviewing medical information. Unfortunately, the feelings of safety are not in line with the results of their actions. The NCSA study also found:

Regarding Virus Protection:

- 67 percent of total respondents do not have up-to-date anti-virus software (updated within the last week)
- 15 percent of the total do not have any anti-virus software
- 63 percent of the total have been victims of virus infection
- 19 percent of respondents had at least one virus currently on their computer

Regarding Spyware

- 80 percent of respondents had spyware or adware programs on their computer
- 89 percent of the respondents who had spyware/adware on their computer did not know the programs were on their computer
- 90 percent of respondents did not know what spyware/adware programs do

Regarding Firewalls

- 67 percent of respondents do not have any firewall protection
- 72 percent of those with firewall protection do not have a secure firewall

Further, the study found that there was a significant amount of confusion on the part of individuals regarding security steps they should take and the programs that will protect them. Fifty-eight percent did not know the difference between a firewall and anti-virus software and 53 percent did not know what a firewall was or how firewalls worked. If we extrapolate these percentages to the United States as a whole, this means that there are millions of individuals who are currently infected with viruses/adware/spyware and are unaware of how to protect their systems. Likewise almost 20 percent of the respondents stated that either a friend or family

member had already fallen victim to an online (phishing[2]) scam. Unfortunately, the survey revealed that only 42 percent were familiar with the term "phishing," and of those, just 57 percent could accurately define it (America Online & National Cyber Security Alliance, 2005). In the last six months of 2006, Symantec Corporation, a computer software infrastructure company, detected more than 166,000 unique phishing messages with the majority of them occurring during business hours (Symantec Corporation, 2007), a clear indication that individuals at organizations are the target of attacks to gain private and corporate information (Germain, 2007).

Underestimation of personal vulnerability and low risk perceptions are in keeping with crime research, which shows that individuals consistently underestimate their risk of becoming victims of crime (Frieze et al., 1987). Often individuals feel that they are either not at risk, as shown above, or that someone else is protecting them; thus their precaution-taking activities are a waste of time. Further, those who have not experienced an attack have their feelings of invulnerability reinforced, and even tend to relax any precaution-taking activity they do have as their (false) sense of confidence grows (Frieze et al., 1987). One area that has been neglected in

---

[2] Phishing is "…a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes" (Anti-Phishing Working Group, 2007) (page 1).

the IS research literature is this role of individuals, rather than management or IS security personnel, in preventing cyber-attacks. Specifically, how individuals take precautions, how they are motivated to take precautions, and the impact of corporate security policies on individual precaution-taking behavior is the focus of this research. The attention to these issues at the individual level will help organizations design better controls and understand better how to inspire individuals to enhance security beyond the technical protections that are commonplace within organizations.

Control theory is an appropriate tool to help us understand these issues and may be applied to the security environment to provide insight as to why individuals take cyber-precautions within the work environment. This literature also allows us to explore the impact of management policies and procedures on individual compliance. Organizations can focus their control efforts on measuring either individuals' behavior or the outcomes of those behaviors (Ouchi, 1977). In the case of security, the desired outcome – a secure system – is not always easy to measure. With the changing nature of security threats (America Online & National Cyber Security Alliance, 2004; American National Standards Institute, 2005; Associated Press, 2004; National Cyber Security Alliance, 2005; Symantec Corporation, 2007) organizations typically find that implementation of behavioral controls to prevent future outcomes is a more effective strategy (Straub, 1990; Straub & Nance, 1990; Straub & Welke, 1998). Additionally, prior research on risk perceptions suggests that individuals' action is influenced by individual perceptions of risk (Frieze et al., 1987). When individuals believe they are in a risky or hostile environment, they take precautions or enact personal rules to reduce their perceived vulnerability (Levi, 2001; McCoy, Wooldredge, Cullen, Dubeck, & Browning, 1996; Tyler, 1980; Walklate, 2001). This could be used to enhance the organizational security environment.

1.1 RESEARCH QUESTIONS

As noted above, organizations face a dilemma of how to promote security policies and procedures to individual employees in the most effective way. The purpose of this research is to examine this dilemma. Specifically, the following research questions will be addressed:

1. What effects do behavioral controls have on security precautions taken by individuals?
2. What role do individual perceptions of mandatoriness have on the level of precautions taken by individuals?
3. What effects do individual risk perceptions have on security precautions taken by individuals?

1.2 SUMMARY OF RESEARCH DESIGN

This research utilizes a field survey to test a theoretical model derived from the security, control, and fear of crime literatures. An organization was identified which had an interest in examining the behavioral aspects of information security at their organization. Based on the literature and general computer security practices a questionnaire was developed and administered on-line to the members of the organization. The individuals who took the survey were targeted as those who regularly worked with computers and had a great deal of exposure to computer systems.

1.3 SUMMARY OF THE RESULTS

Overall five of the seven proposed hypotheses were supported. The results of this study provide important contributions to both literature and practice. The results demonstrate that certain aspects of control are more effective than others in motivating individuals to view computer security policies and procedures as mandatory. Likewise, the results show that perceptions that a policy is mandatory significantly influence individuals' precaution taking behaviors; additionally, mandatoriness effectively mediates the relationship between control elements and precaution taking behaviors. Individual experience, either direct or indirect, significantly influences individuals' perceptions of the impact of cyber-crime and thus persuades them to take precautions. The results help us understand how to motivate individuals to protect their computer systems and help organizations design better controls, reducing their exposure to cyber-attacks.

1.4 OVERVIEW OF CHAPTERS

This dissertation is divided into six chapters. This introduction provides a general overview of the research topic, the research questions, and the document in general.

Chapter 2 provides the literature review. This chapter reviews the theoretical and empirical literature pertaining to security, control, risk, and the fear of crime.

Chapter 3 presents the theoretical model with specific hypotheses that will be tested in this research. The constructs used in the model and hypotheses are developed and defined. The constructs used in this research from the control literature include specification, evaluation,

reward, punishment, and mandatoriness. Those based on the risk and fear of crime literature include direct experience, indirect experience, risk likelihood, and risk impact. Finally, the dependent variable, precautions taken, is taken from the security literature and security practices.

Chapter 4 discusses the survey research methodology used in this study. The design of the research is described and the rationale for this approach is presented. The pretest and pilot tests along with the validation of the survey based on those tests are presented and the research constructs are designed and operationalized.

Chapter 5 describes the full data collection and survey procedures, the validation of the measurement instrument used, and the analysis and results of the study.

Chapter 6 discusses the results and implications of this research. The practical implications and lessons that organizations can take from these results are highlighted along with the implications for researchers. Potential future research building on the results and the limitations of this research are discussed and conclusions are presented.

2.0 LITERATURE REVIEW

This chapter presents a review of the literatures that form the underlying support for the theoretical model tested in this dissertation. The security, control, and fear of crime literatures provide a theoretical foundation for this study. The security literature provides an overview of what we know about the prevalence of cyber-attacks, the means to prevent them, and a starting point for our research. The control literature supplies a conceptualization of this phenomenon and offers a way to understand organizational policies and individual responses. Finally, the fear of crime literature focuses on individual precaution-taking behavior in a perceived hostile or risky environment.

2.1 SECURITY LITERATURE

Information security and how it relates with computers has been of concern for decades (Pearson & Weiner, 1985). With the increase in technological advances that allow companies to process, store and transmit digital data in a wide range of sectors (Dhillon & Backhouse, 2000, 2001), the problem of how to keep the organizations' and the individuals' information secure has become a problem that is often talked about, and often misunderstood (Whitman, 2003). The security literature falls into three broad categories: the ethics of computer abuse, the technical approach

to computer security and, often discussed as a subset of the technical approach, the behavioral aspects of computer security.

2.1.1 Ethics of Computer Abuse

The ethics of computer abuse approaches the topic of information security from a business ethics perspective (Gattiker & Kelley, 1999). Authors in this stream have found that when individuals use computers, they tend to depersonalize their potential victim, lower their ethical standards, and justify their actions beyond what most individuals would do if a computer were not used (Gattiker & Kelley, 1999). Harrington (1996) approached the ethics question from the standpoint of how company policies affect individuals when they are confronted with unethical opportunities. He found that company codes did not affect computer abuse judgments, but the existence of corporate policies did reduce justification that individuals tried to use to excuse their unethical acts (Harrington, 1996).

2.1.2 Technical Security

The technical aspects of information security have received the most attention in the academic literature. This literature focus emphasizes technical or programmed solutions that would prevent, stop, or contain cyber-attacks. For this research, ***cyber attacks are defined as any intentional act of sabotage or appropriation of individual or corporate systems or data***. These attacks typically take the form of virus infection, illicit installation of software, "hacking" a computer or server to gain access or gain remote use for other intentions, "phishing" for private information, etc. Extant academic security literature focuses primarily on programmed solutions

or tools to prevent crime. This literature draws from theories of physical security and crime which are based on general deterrence theory (Blumstein, 1978; Pearson & Weiner, 1985; Straub & Collins, 1990; Straub & Nance, 1990; Straub & Welke, 1998). General deterrence theory states that individuals with intent to commit anti-social acts (crimes) are best deterred by the implementation of strong disincentives and sanctions dealing with the anti-social act (Blumstein, 1978). In accordance with general deterrence theory, the majority of the existing literature emphasizes technical or programmed implementation of strong, centrally controlled solutions to protect computer systems (Dhillon & Backhouse, 2001). The reason for this approach is simple: a programmed approach involves fewer individuals who might not follow instructions (S. K. Chin, 1999; Ives, Walsh, & Schneider, 2004). Programs typically cost less than training and behave consistently if implemented correctly.

2.1.3 Behavioral Security

While technical solutions may be the easiest for firms to implement and centrally control, they are not always the most effective (Dhillon & Backhouse, 2000). For example, Straub (1990) argued that security deterrents are effective to reduce incidents of computer abuse. His survey of 1,211 organizations found, in rank order, the following to be most effective in reducing security incidents:

1. Number of hours/week dedicated to data security (by IS personnel)
2. Cumulative hours/week (by everyone involved) dedicated to security
3. Use of multiple methods to disseminate information regarding information security policies and procedures
4. Statements of penalties for violations

5. Use of security software (the technical solution)

Straub's (1990) research noted that the behavioral aspects of security and precaution-taking, such as dissemination of policies and procedures and information regarding penalties for violations, ranked higher in effectiveness across his respondents than did technical issues. Though many studies consider security policies and procedures (Dhillon & Backhouse, 2001; Straub, 1990; Straub & Collins, 1990; Straub & Nance, 1990; Straub & Welke, 1998), they are typically secondary to the technical discussion or to the discussion of technical ways to prevent cyber attacks (S. K. Chin, 1999; Ives et al., 2004; Mercuri, 2002). Some discuss the need to implement different security software to protect the company (Fernandes, 2001; Muralidhar, Batra, & Kirs, 1995; Muralidhar, Sarathy, & Parsa, 2001), others focus on specific database security measures (R. Garfinkel, Gopal, & Goes, 2002; Sarathy & Muralidhar, 2002), and still others emphasize the need to build trust through providing technical protections (Luo, 2002), but very few look directly at the role that behavioral policies and procedures play in the process of information security.

Of those researchers who do look at the behavioral aspects of information security, they tend to focus on either the organizational level or management level of effective control design (S. K. Chin, 1999; Rees, Bandyopadhyay, & Spafford, 2003) rather than the individual level. Whitman (2003) conducted a survey on information security of companies, found that the majority of companies do not have a systematic approach to information security and concluded that more work needs to be done at the management level to assess threats and build more effective security policies. Others have emphasized frameworks for policy development and implementation of controls to better protect the company (S. K. Chin, 1999; Rees et al., 2003). Dhillon and Backhouse (2000) note that often the rules and procedures relating to security are

generated by IS departments and seen as over-complicated and generally not applicable to ongoing business. This attitude often leads to "security blindness" on the part of the users and the general lack of awareness that the threat from computer security issues is a serious issue for businesses (Hughes & DeLone, 2007).

When individuals are not motivated to follow policies and procedures which are designed to protect both the individual and the organization, security fails (Campbell, 2000; CERT Coordination Center, 2004a; Coren, 2005; Dhillon & Backhouse, 2000). One area that has been neglected in the IS research literature is this role of individuals rather than management or IS security personnel in preventing cyber-attacks. Specifically, how individuals take precautions, how they are motivated to take precautions, and the impact of corporate security policies on individual precaution-taking behavior have not been extensively researched in the academic literature. The accounting literature recognizes IS security as a control system (Dopuch, Birnberg, & Demski, 1982), but the existing IS literature has underdeveloped conceptualizations of how these control systems work in the security realm. For more details we now turn to the control literature to explore the role of behavioral control in information security.

2.2 CONTROL

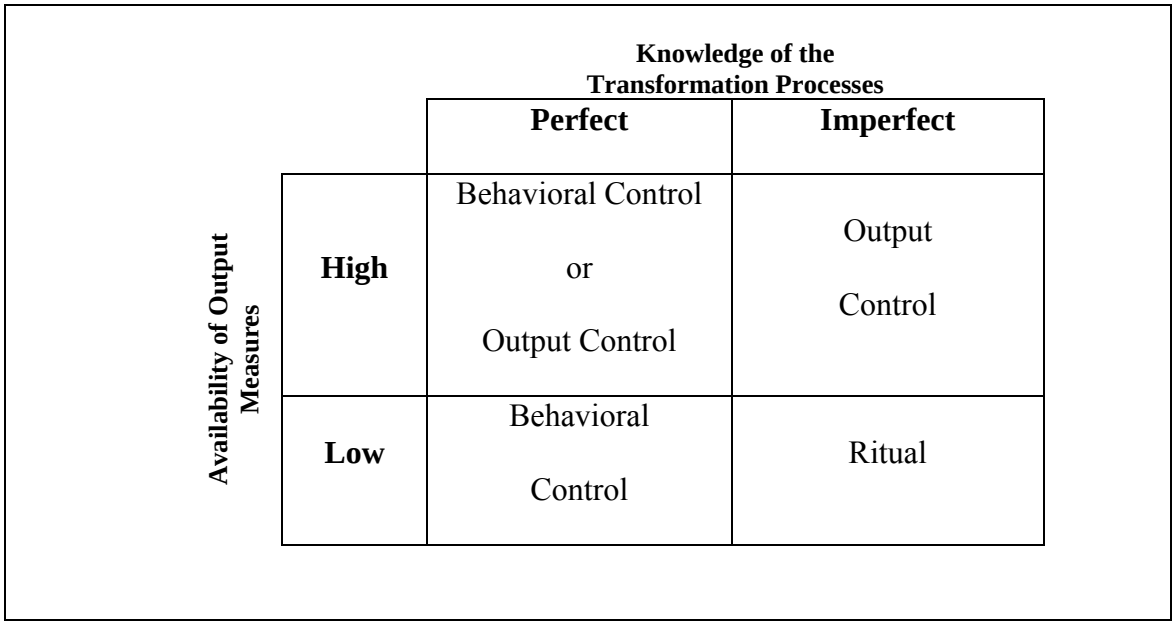
Control is defined as a process, system, or environment designed to provide motivation for organizational members to take actions and make decisions consistent with organizational objectives (Das & Teng, 1998; Jaworski, 1988; Kirsch, 2004; Kren, 1990; Ouchi & Maguire, 1975). Formal control is viewed in the organizational and IS literatures as a performance evaluation strategy where either outcomes or behaviors are specified, evaluated, and ultimately

rewarded or punished (Eisenhardt, 1985; Kirsch, 1996; Ouchi, 1978, 1979). IS scholarship has typically applied these concepts to the control of systems development (Kirsch, 2000; Kirsch, Sambamurthy, Ko, & Purvis, 2002), while others have used them in a general business context (Cardinal, 2001; Eisenhardt, 1985; Koberg, 1988; Rosenthal, 2004).

2.2.1 Historical Control Literature

Ouchi (1977) originally theorized that the organizational structure of a firm could be logically separated from the control system that the organization used where previously control had been very clearly linked to organizational structure in the literature. A control system consists primarily of the process that organizations use to monitor and evaluate behavioral performance of individuals against some standard and suggests a scheme where either the behaviors or the outputs resulting from individual behavior are measured (Ouchi, 1977, 1979). Early empirical studies demonstrated that the choice between measuring outputs versus behaviors depends on the availability of objective output measures and the knowledge that the controller had about the transformation process (Ouchi, 1977, 1979). Where the knowledge is perfect about the transformation process and there is a high level of output measurability, tasks are suited for either outcome or behavioral control. Where there is imperfect knowledge about the transformation process but an availability of objective output measures, tasks are suited for output control. Where there is a perfect knowledge of the transformation process but a low availability of objective output measures, tasks are suited for behavioral control. Where there is a low degree of both knowledge about the transformation process and availability of objective output measures, neither behavioral nor output control were is to control these tasks. These relationships are shown in Figure 1.

Figure 1 – Control Types and Its Antecedent Conditions (Source: Ouchi, 1977)



Since Ouchi's (1977; 1979) conceptualization, many researchers have applied these theories to their research. Eisenhardt (1985) incorporated an aspect of agency theory to Ouchi's (1977; 1979) model by adding "degree of behavior observability," or the extent to which the controller is able to access information that reveals the controllee's actions. This information can take the form of any system, automated or otherwise, that allows the controller to "observe" or monitor subordinates. Examples of these systems include system logs, accounting systems, other information systems, boards of directors oversight, individual observation, and evaluative meetings (Kirsch, 1996).

Eisenhardt (1985) found support for this model through her study of 95 specialty stores (small, product focused stores as opposed to large department stores) where the specific behaviors of employees were the focus of the organizational control. Kirsch (1996) extended Ouchi's and Eisenhardt's work by theorizing and finding support for an interaction effect

between behavior observation and knowledge of the controller: the more observable the controllee's behaviors and the more knowledgeable the controller is about the process, the more likely behavioral controls are used. Further application of this theory shows that the individual users in addition to IS managers play a critical role in systems development projects (Kendall, 1999; Kirsch, 1996; Kirsch et al., 2002). Other IS researchers have noted that formal controls often work together to achieve the desired objective (Nidumolu & Subramani, 2003) and that managers use "portfolios of control" to manage developers in both in-house and outsourced systems development projects (Choudhury & Sabherwal, 2003; Kirsch, 1997).

Control is, in essence, utilized primarily to achieve specific objectives within an organizational setting (Eisenhardt, 1985; Kirsch, 1996; Kirsch & Cummings, 1996; Ouchi, 1977). Formal controls are those that a company implements to achieve a certain outcome or to encourage specific behaviors. Application of the theory described above shows that scenarios where the desired outcome is easy to quantify and measure favor outcome controls, or controls where the outcome is judged (Eisenhardt, 1985; Kirsch, 1996, 1997; Ouchi, 1977). Researchers have noted that outcome measures are often used by managers to validate evidence of performance (Oreilly & Weitz, 1980; Ouchi & Maguire, 1975) and that formalization and enabling procedures help committed employees work more effectively (Adler & Borys, 1996). Ouchi & Maguire (1975) found that output measures were often inappropriately used by managers where the situation was highly complex and interdependent with other issues.

On the other hand, when the controller has a high degree of knowledge about a process or is able to exercise a high degree of oversight (behavior observability) of a process, management will implement controls that emphasize specific behaviors which will lead to a favorable (or at least predictable) outcome (Eisenhardt, 1985; Kirsch, 1996). Behavioral control has further been

conceptualized as "…attempts to ensure that individuals working on…projects act in conformity with pre-defined strategies" (Piccoli & Ives, 2003 pg 368).

A great deal of the extant literature conceptualizes modes of control, such as behavioral control, and measures it as a single construct. However, Kirsch (2004) notes that there are inconsistencies and overlaps in the definitions of behavioral controls in the literature. She argues that to address these inconsistencies and to further our understanding of control, additional research is needed that examines control at a more granular level: what she calls the elements of control. Drawing on the work of Eisenhardt (1985), Kirsch (2004) identifies three elements of control: *specification*, *evaluation*, and *reward.*

2.2.1.1 Elements of Control

As stated, controls are theorized to be comprised of three elements: specification, evaluation, and reward or penalty (Eisenhardt, 1985; Kirsch, 2004). *Specification* refers to the formalized statement of a required behavior or outcome and the provisions made to gather data related to compliance with the behavior or outcome. In the literature, specification, in terms of formal documentation, is usually the focus. An equally important aspect of this element, however, is the discussion of gathering data, by automated, observational, or surrogate means (Eisenhardt, 1985; Kirsch, 2004). This measurement allows the controller to align the desired behavior or outcome with organizational goals with the intent of achieving a specified objective (Kirsch, 2004; Lorange & Scott-Morton, 1974).

Evaluation is the sifting and organization of collected data with the intent of assessing individuals' compliance with specified behaviors or outcomes (Eisenhardt, 1985; Kirsch, 2004). Those involved in evaluation have the responsibility to determine whether the desired outcome has been achieved or whether the individual has followed the documented policies. With this

element, emphasis is placed on the use of formal documentation and information exchange to assess current status and make adjustments as necessary (Jaworski, 1988; Kirsch, 2004; Ouchi, 1980).

The final element of control is *reward or punishment*, where individuals are rewarded (or punished) based on following a prescribed behavior or meeting a target outcome (Kirsch, 2004). The control literature tends to emphasize the mechanisms of reward (Chow, Hirst, & Shields, 1995; Eisenhardt, 1985; Kirsch, 2004; Luft, 1994) which link adherence to behaviors or outcomes with the rewards themselves (Kirsch, 2004). Thus individuals would be rewarded based on following a required behavior or achieving the desired outcome. Eisenhardt (1985) notes that in the organizational literature, the reward for compliance with organizational control is often implicit in the evaluation phase. Agency theory, where contracting is specifically involved within the agency relationship, makes rewards explicit (Eisenhardt, 1985). The application of these elements of control has the potential to provide us with deeper understanding of the effectiveness of various aspects of control in different settings. Thus this research focuses on specification, evaluation, and reward.

2.3 CONTROL AND SECURITY

Control theory can be applied to the security environment to provide insight on why individuals take cyber-precautions within the work environment and the impact of management policies and procedures on individual compliance. It is logical to assume that observation of not only the mode of control (in this case behavioral controls) but also the different control elements will result in a richer understanding of how organizational policies impact individuals. Organizations

decide to measure either the behaviors or the outcomes of behaviors (Ouchi, 1977). With the changing nature of security threats (America Online & National Cyber Security Alliance, 2004; American National Standards Institute, 2005; Associated Press, 2004; National Cyber Security Alliance, 2005), it is next to impossible to say with any certainty that a system which is currently secure will be secure in the future without organizational encouragement of behaviors to achieve this goal. Thus organizations typically find that implementation of behavioral controls to prevent future outcomes is the most effective security strategy (Straub, 1990; Straub & Collins, 1990; Straub & Nance, 1990; Straub & Welke, 1998).

The examination of the elements of control directly applies to security for two reasons. First, security policies and procedures are often specified and administered by technical managers with no "line" responsibility for the individuals who must follow those policies. This means that specified controls, even if specified and evaluated, might be seen as optional as those enforcing compliance have no direct authority over those they seek to control. Second, security policies and procedures (measurements) are put in place to regulate the behaviors of individuals to achieve (or prevent) a particular outcome (Eisenhardt, 1985; Kirsch, 2004). These policies can be seen, collectively, as a recipe that will try to ensure a secure system not only at the present time, but also in the future. The result is that while policies are directed, in a general way, at the individual, how the individual follows those policies has implications for the entire organization. Thus how an organization coordinates specification, evaluation, and reward across business units has implications for the entire organization.

Security specifications are put in place primarily to encourage behaviors that will lead to a more secure computer environment within the organization. Thus an organization specifies rules (policies and procedures) to encourage the individual to behave in a way that will protect

corporate data assets and prevent a cyber-attack from being successful. Behavioral measurement is implemented to reduce system vulnerability to security threats by teaching the individual how to behave in security situations (Dutta & McCrohan, 2002; Hone & Eloff, 2002). Policies are specified and data are gathered through automated means, observational means, or examination of surrogate outcomes that are highly correlated with the desired behaviors. To monitor behavior, organizations have the option to physically monitor individuals with real-time observation (Ouchi, 1980; Ouchi & Maguire, 1975), or utilize surrogates for real-time monitoring by specifying indirect, but highly correlated indicators of the desired activity such as spot checks of individuals' computers to verify that anti-virus software is up to date or monitoring of logs to verify compliance with the policy. If an individual has connected to the anti-virus software vendor in the past week, or a spot check of an individual's computer is done to verify that vendor-issued security patches have been installed, these checks allow the controller to verify that the required behavior has been followed. The specification of policies and the measurement allow individuals to become aware of the desired behaviors and follow the stated policies.

Next, evaluation is required to validate compliance with the specified security measure. Managers analyze logs, integrate personal observation and spot check information, and come to a conclusion regarding individuals' compliance with security policies and procedures. Whether compliance with the policies was successful or not in preventing an attack is immaterial. The focus on the required behavior is integral to the evaluation of behavioral security controls.

Third, individuals are rewarded and/or punished based on the results of the evaluation. Compliance with required behaviors should result in the individual being rewarded, while noncompliance should result in punishment. Those who follow the documented policies and

procedures could be rewarded by either monetary or non-monetary means: a bonus could be paid or favorable mention made in the corporate newsletter. Penalties for non-compliance can be similarly applied: a reduction in pay, a poor performance evaluation, or formal letters of reprimand are punishments that negatively affect individuals' careers.

Regardless of the controls implemented at the organizational level, if those controls are not perceived by individuals to be mandatory, they will likely be ignored. Compliance with control requirements is expensive to the controller, in terms of both time and effort (Dopuch et al., 1982). Individuals are required to behave in ways that may be inconvenient and possibly take time away from primary work responsibilities. While there are a variety of different reasons why individuals do not follow defined policies and procedures, this research will examine whether individuals view organizational controls, specifically computer security controls, as mandatory.

2.3.1 Mandatory Controls

The concept of mandatory controls, where participation is not optional or where compliance is required by the company, is not typically discussed in the control or security literatures. The assumption, while not stated specifically, is that controls would not be specified if they were not important enough to be mandatory. Similarly, financial audit practices presume that the structured tasks of an audit plan will be followed as a matter of course because the required steps have evolved over time to arrive at the best way to complete the task in the shortest amount of time. There is little discussion in the literature about the choice of the individual and compliance with the management expectations. This research explicitly considers the role of mandatoriness in individual response to organizational controls. ***Mandatoriness is here defined as the degree***

to which individuals perceive that compliance with existing security policies and procedures is compulsory within the organization.

Some IS literature has discussed mandatory versus voluntary systems, but is not always consistent in the discussion or definition of a mandatory system. The IS literature classifies a mandatory system in terms of being declared mandatory by management (Karahanna & Straub, 1999), or non-mandatory because alternatives to the technology exist (S. Taylor & Todd, 1995). A stronger conceptualization of mandatory systems is used by Hartwick & Barki (1994) and Venkatesh & Davis (2000) who define mandatory as the individual's perceptions of "required use" by managers.

Approaching this from a control perspective, I use Kirsch's (2004) conceptualization of control elements discussed earlier. Control specification evokes a general level of obedience from individuals (Feldman, 1998; Milgram, 1974; Prakash & Rappaport, 1975). Further, the propensity of individuals to perceive that a policy or set of policies is mandatory depends on whether management evaluates the individual's compliance with the prescribed policy. Finally, a policy which has a specified reward or punishment affixed will also encourage compliance with the specified policy. Thus, security policies should not merely be specified, but also evaluated, and rewarded or punished (based on compliance) to communicate a level of "mandatoriness" regarding the policy itself.

Looking at how controls are applied, including how each of the components of behavioral controls is applied, will help us understand the impact of the security controls and why individuals follow those controls. Additionally, examination of the perceptions of individuals regarding control measurement and evaluation and whether controls are perceived as mandatory will help us deepen our understanding of why individuals take precautions.

2.4 RISK PERCEPTIONS

Finally, there is a large body of evidence that suggests that the decision to take precautions stems from individual perceptions of risk (Finne, 1998, 2000; Frieze et al., 1987) rather than (or perhaps in addition to) the existence of company policy. Indeed, the accounting literature bases the need for control on risk assessment (Dopuch et al., 1982; Waller, 1988) and the information systems literature often references the need to model systems risk (Barki, Rivard, & Talbot, 1992, 2001). Many of the studies that examine perceived risk view risk as a rational decision involving the individual's assessment of both the probability of something occurring and the severity of the experience (Han, 2004). However, this view excludes the emotions that have a strong impact on individuals while assessing their current level of risk. These emotions typically cause individuals to feel more at risk for things that probably will never occur (e.g.: terrorist attack, shark attack, etc.) and less at risk for things that will (clogged arteries, skin cancer, automobile accident, etc.) (Sturrock, 2005). Likewise some research indicates that much of the information that individuals receive regarding computer security threats focuses on the emotional impact of cybercrime (Hughes & DeLone, 2007).

In the management literature, there are numerous studies that examine risk perceptions at the organizational or departmental level (Clarke, 1993; Straub & Welke, 1998), and this risk is the basis for much of the technically focused security literature discussed earlier. There are also many management studies investigating individual risk perceptions. This body of literature tends to focus on risk perceptions relating to financial or investment decisions (Ahlbrecht & Weber, 1997; Jia & Dyer, 1996; Jia, Dyer, & Butler, 1999; J. W. Taylor, 2005). The IS literature pertaining to risk and risk management is rooted in the management literature and focuses on risk at the departmental or project level (Barki et al., 2001).

Alternatively, the crime literature (specifically the fear of crime literature) also focuses on risk perceptions at the individual level (Pain, 2000, 2001; Walklate, 2001), but focuses directly on individual decisions to take precautions as the consequence of perceived risk (Hastings & Dean, 2003). To better understand individual motivation to assess risk, and thus take precautions, we will draw on such factors from the fear of crime literature as direct experience and indirect experience with cyber-crimes.

Fear of crime has long been identified as central to the understanding of individuals' responses to crime and its consequences (Parker, McMorris, Smith, & Murty, 1993; Walklate, 2001). At the same time, because of its role in individuals' perceptions and choices, fear of crime is a significant factor in its own right (Pain, 2000, 2001). While there is debate regarding the full nature of fear of crime (Rountree & Land, 1996), it can generally be characterized in terms of individuals' perceptions of risk and the degree to which they are worried about the possibility of becoming victims (Levi, 2001; Rountree & Land, 1996). For this research, ***perceived risk***, as a component of fear of crime, is ***defined as the degree to which an individual perceives that it is probable that they will become a victim of a cyber-attack*** (Frieze et al., 1987). The perception of risk is typically related to the experiences that the individual has had regarding security incidents or direct experience (Skogan & Maxfield, 1981; Stinchcombe et al., 1980; S. Taylor & Todd, 1995). Individuals do many things using computers that could be construed as risky; however, unless they have had direct experience, they will not take precautions as a result of the "security blindness" discussed earlier (Dhillon & Backhouse, 2000). In addition to direct experience, stories told by others or indirect experience have an equivalent or greater effect on individual risk perceptions (Hanson, Smith, Kilpatrick, & Freedy, 2000; Tyler, 1980). Hearing about a virus infection, learning of a friend's identity being stolen,

or hearing that your father found 200 instances of spyware on his computer contributes to individual experience. These experiences have the effect of causing individuals to perceive risk and thus take precautions (Frieze et al., 1987).

While the IS literature is not as helpful at defining the phenomenon of individual risk and why individuals take precautions, it is helpful in defining the aspects of risk that should be addressed. Barki et al. (2001) proposed a contingency model of software project risk based on extant systems risk literature (Barki et al., 1992; Deephouse, Mukhopadhyay, Goldenson, & Kellner, 1995; Kappelman & McLean, 1994) that identify key aspects of risk that are appropriate to address in this research. Risk exposure, or the probability of an unfavorable outcome, is captured through the fear of crime literature components of direct and indirect experience as antecedents to the individual assessment of risk. The actual probability assessment at the individual level is composed of individual judgments regarding the likelihood that the unfavorable experience will happen, and the impact of that experience were it to happen (Barki et al., 2001; Frieze et al., 1987; Rountree & Land, 1996).

2.5 CHAPTER SUMMARY

This chapter has summarized the various literatures that form the basis of this study and provide a foundation for the development of the theoretical model. The security literature provided a foundation for the study and an explanation of the problem businesses face as a result of computer security issues. The control literature provided us with a specific lens to examine the problem of computer security control compliance and identified five aspects of control to be tested as they relate to precaution-taking behaviors: specification, evaluation, reward,

punishment, and mandatoriness. While the control literature addresses the managerial aspects of directing individuals how to take computer security precautions, it is insufficient to explain all of the individual responses to these requirements. The risk and fear of crime literatures address the individual reaction to the fear of becoming a victim to cybercrime and also address the aspects missing in the control literature. In the next chapter, a research model based on this foundation is introduced and hypotheses are developed.

3.0 RESEARCH MODEL AND HYPOTHESES

The following sections deal with presenting the research model and proposing hypotheses to test this model. The effects of the control elements on perceived mandatoriness are examined first. Next, perceived mandatoriness effects on precautions taken are discussed. Third, the effects of perceived risk on precautions taken are examined and we conclude with the effects of personal and indirect experience on perceived risk.

3.1 CONTROL ELEMENTS AND PRECAUTION TAKING

Behavioral controls are often implemented within organizations for security purposes (American National Standards Institute, 2005) with the goal of motivating individuals to comply with the desired behavior. A good behavioral security policy might state that "Employees are to log off their computers when not at their desks." This policy does two things: it addresses the issue of accountability in that someone might use the "available" computer and thus not be held accountable for their actions, and it limits the amount of time a hacker has to attack a specific system. Behavioral control research suggests that establishing uniform performance criteria throughout the company enhances performance (Nidumolu & Subramani, 2003). The literature emphasizes the use of formal, documented procedures to communicate the desired behavior along with provisions to collect data regarding that behavior. The classic, if somewhat

disturbing, obedience studies done by Milgram (1974) found that directives from a perceived authority resulted in the majority of individuals complying with those directives, and subsequent research has supported these findings over the past 30 years (Feldman, 1998; Schneider, Gruman, & Coutts, 2005). This leads us to deduce that behavioral controls that pertain to security will follow a similar course. The specification of rules, policies, and procedures (by an authority) will result in individuals' perceptions of required obedience or a perception of urgency. Therefore we predict that:

H_1 Specification will be positively associated with the individual's perceived mandatoriness of the established set of security policies.

According to the old business adage "That which is measured improves," the simple act of formulating and communicating policy to an organization is rarely enough to motivate action (Lim, Teo, & Loo, 2002; Luft, 1994). Individuals need to perceive that compliance with extant policies is important to management and that management views compliance with the policy as mandatory. One way management signals the importance of a policy is by assessing whether it is being followed. Evaluation is an essential part of control and can be characterized as the analysis of collected data that allows management to determine individual compliance (Kirsch, 2004). If management either never or only infrequently evaluates compliance, those policies will most likely be disregarded by employees. Evaluation of individual compliance thus results in the perception that a policy is mandatory, suggesting that:

H_2 Evaluation of compliance with security policies will be positively associated with the individual's perceived mandatoriness of the established set of security policies.

Reward and punishment are the final factors that signal to the individual that a control is mandatory. Effective behavioral control rewards individuals based on their compliance with specified behaviors (Das & Teng, 1998; Eisenhardt, 1985; Kirsch, 2004). If policies are stated, data gathered, individuals evaluated, but there is no consequence for either compliance or non-compliance, individuals will soon decide that the control is not important to management and thus not mandatory, regardless of management declarations (Straub & Welke, 1998). When compliance with a control is rewarded, the individual is more likely to perceive the control as mandatory which leads us to conclude that:

H_{3A} Reward for compliance with security policies and procedures will be positively associated with the individual's perceived mandatoriness of the established set of security policies.

Research shows that individuals view punishment and reward differently in different contexts (Frederickson & Waller, 2005; Luft, 1994). Punishment is often seen as the opposite of reward, and therefore should be explicitly examined, thus:

H_{3B} Punishment for non-compliance with security policies and procedures will be positively associated with the individual's perceived mandatoriness of the established set of security policies.

The additional costs of time and effort required to comply with security policies and procedures make it easy to ignore requirements that are not considered to be mandatory. Lim et al. (2002) found that only 60 percent of employees accept Internet usage policies at face value, suggesting that there are doubts at the individual level regarding how they view extant policies. Specifying a policy with subsequent evaluation and reward is not enough to motivate individuals to follow policy. On the other hand, management expectations have a strong effect on individual

behavior (D'Aquila, 2001): the compliance expectations of managers will influence the behavior of their employees. This suggests that if individuals perceive security policies to be mandatory, they are more likely to adhere to those policies. We therefore predict that:

H_4 Perceived mandatoriness of control measurements will be associated with an increased likelihood that the individual will take cyber-precautions.

3.2 RISK PERCEPTIONS AND PRECAUTION-TAKING

There is a great deal of evidence that the decision to take precautions stems from individual perceptions of risk (Finne, 1998, 2000; Frieze et al., 1987) rather than the existence of company policy. Key antecedents to perceived risk are a function of the degree to which an individual has been previously exposed to crime through either direct experience (Skogan & Maxfield, 1981) or through indirect experiences (Skogan & Maxfield, 1981; Stinchcombe et al., 1980). Prior victimization is defined as individuals' direct experiences that make it easier for them to visualize themselves as victims in the future. Existing empirical studies suggest that individuals who have been victims of crimes are more likely to perceive themselves as victims in the future (Skogan & Maxfield, 1981; Smith & Hill, 1991; Stinchcombe et al., 1980; Tyler, 1980; Weinrath & Gartrell, 1996). Therefore, individuals who have been victims of cybercrime or cyber-security incidents (hacking, virus infection, lost data, inaccessible system, etc.) should follow a similar pattern. It is therefore reasonable to predict that:

H_5 Direct experience with cyber-security incidents will be positively associated with the individuals' perception of risk.

Direct experience is not the only way that individuals are exposed to crime. Exposure to others' experiences in the form of anecdotes by colleagues, corporate training, or reports through media outlets increases the awareness of individuals' vulnerability (Hughes & DeLone, 2007). Just as personal experience can make it easier to imagine oneself being a future victim, learning of others' victimization has been found to cause individuals to feel more at risk regarding the specified activity (Hanson et al., 2000; Skogan & Maxfield, 1981; Tyler, 1980). This suggests that:

H_6 Indirect experience (through media, collegial anecdotes, or other sources) with cyber-security incidents will be positively associated with the individuals' perception of risk.

Perceived risk, as a component of fear of crime, has been shown to influence individual behaviors (Levi, 2001; Rountree & Land, 1996). Individuals who perceive their behaviors to be risky are more likely to take precautions in order to reduce their vulnerability (Frieze et al., 1987) in many different contexts such as personal safety, securing valuables and other belongings, etc. When individuals perceive that their actions with computers have potential risk, they are more likely to take cyber-precautions. We therefore predict that:

H_7 Perceived risk of cyber-vulnerability will be associated with an increased likelihood that the individual will take precautions.

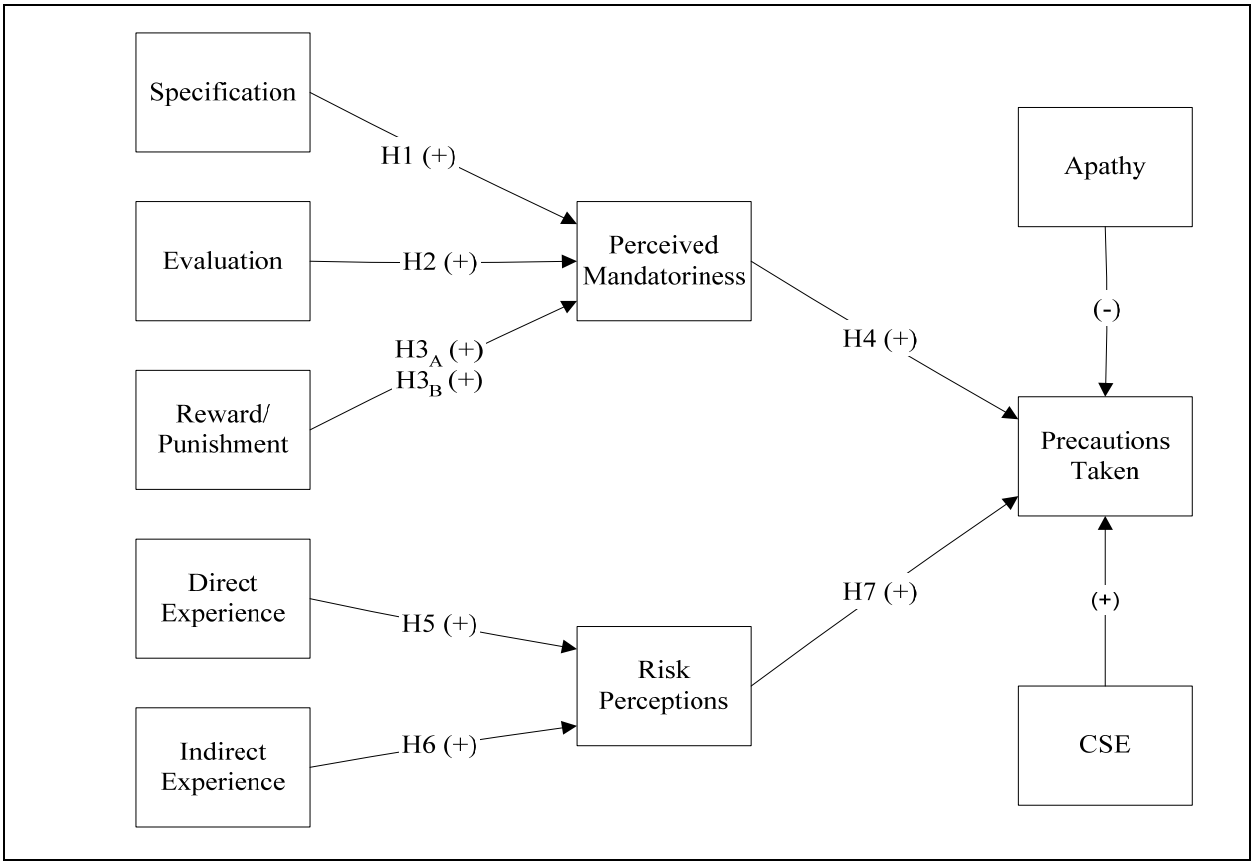
Apathy, or the lack of motivation or enthusiasm, was added as a possible covariant to capture information relating to individuals who disregard policies and procedures because they are too busy or just don't consider computer security to be important. Apathy is predicted to have a negative affect on individual precaution taking. Additionally, Computer Self-Efficacy (CSE) (Compeau & Higgins, 1995), or the individual's estimate or personal judgment of his or

her own ability to succeed with computers, was also added as a potential covariant as individuals who have high levels of CSE would more likely be interested in computer security. CSE is predicted to have a positive affect on individual precaution taking.

3.3 THEORETICAL MODEL

The theoretical model representing these assertions and their relationships is shown below in Figure 2.

Figure 2 – Theoretical Model



3.4 CHAPTER SUMMARY

This chapter has presented the hypotheses and the research model. The objective of this stage in the research was to introduce the central constructs and to develop a theoretically grounded model of the relationships between these constructs based on prior work. The constructs were based in the literature and affect the dependent variable. The control elements of *specification*, *evaluation*, and *reward/punishment* are theorized to have a positive effect on individual perceptions of the mandatoriness of a control implemented at the organizational level applying to

individual behaviors. The degree to which individuals perceive that control to be mandatory influences the degree to which they are likely to take precautions. *Mandatoriness* itself mediates the relationship between the control elements and the dependent variable *precautions taken*. The effects of *direct and indirect experience* are theorized to have a positive impact on individual *perceptions of risk*. The degree to which individuals perceive themselves to be at risk influences the degree to which they are likely to take precautions. The individual perceptions of risk mediate the relationship between experience and precautions taken. The following chapter discusses the methodology that will be used to test these hypotheses.

4.0 METHODOLOGY

This chapter discusses the details of the research design used for this study. The main topics presented in this section include: description of the research design, pretesting the instruments, the pilot test for this study, the operationalization of the constructs, the final data collection, and a description of the sample. This chapter also discusses the treatment of invalid cases and the procedures for identifying those data.

4.1 RESEARCH DESIGN

There are a number of potential research designs that can be used to collect data and test theory. The choices of methodology include case studies, field experiments, lab experiments, participatory research, and field surveys (Cryer & Miller, 1991). Each methodology has certain strengths and weaknesses and the choice of research methodology must reflect the overall objectives of the study and the nature of the research questions being addressed.

The goal of this research is to examine the effects of external influences (security controls) mediated by mandatoriness and internal pressures (perceived risk) on the precaution taking behaviors of individuals. Do these conditions motivate individuals to make changes? The primary purpose of this research is to test the model described above. The ability to test the hypotheses and achieve the stated objectives requires selecting a research design that allows the

input of individuals who experience these differing influences. It is also important to choose a design that allows the results to be generalized across organizations. For these reasons a field survey was considered the most appropriate approach.

Using this methodology, where a single individual assesses both the independent and the dependent variables, raises the possibility of single source or method bias within the study (Crampton & Wagner, 1994). I address this by rigorously validating the variables at every stage of data collection to reduce the possibility of common method bias (Nidumolu, 1995). I also followed the recommendations of Podsakoff and Organ (1986) during the pretest and pilot test and measured and performed Harman's one-factor statistical test where all of the scale items are entered into a factor analysis to see if either a single factor emerges or any one factor accounts for the majority of the variance between the variables. Podsakoff et. al (2003) recommends additional tests which will be described in the results chapter and applied to the final dataset.

As a side note, even without the measure validation, there is evidence to show that single source bias may not be as strong as previously thought. Research by Crampton & Wagner (1994), which examined over 11,000 correlations from published literature, suggests that method bias is likely in some areas of research, but is more the exception than the rule. While some existence of method bias exists in extant literature, it does not support the general assertion that all self-reported surveys are fundamentally flawed. Specifically, the areas that were shown to be susceptible to method bias were those that deal with job satisfaction, turnover and turnover intentions, personality, individual ability, role characteristics, job performance appraisals, and leader initiation of structure (Crampton & Wagner, 1994). The only area where this research may have problems is with the self-reporting of precaution-taking behavior. This area will be rigorously tested in the analysis of the final data.

4.2 TESTING

Validation of instruments is an important part of the research process (Straub, 1989). Instrument validation requires that individual instruments must have content validity, construct validity, reliability, internal validity, and statistical conclusion validity (Straub, 1989). As discussed below, these issues are addressed through a pretest and pilot test of the survey items. Further, the pretest and pilot test provide assurance that the instruments are understandable, and also provide a "run-through" to allow the researcher to experience some of the issues that may occur during the main data collection. Finally, these steps help ensure that no important elements related to the study have been omitted.

4.2.1 Pretest

A pretest is conducted primarily to provide qualitative assurance about a measure's content validity, construct validity, and reliability. This phase is designed to facilitate revision of the instrument to allow it to be statistically validated (Straub, 1989). Important criteria to be evaluated in the pretest include: meaning of items, flow of items and sections in the survey, and how long it takes to complete the survey (Fowler, 2002). The overall goal is to include only items that will be readily understood by the participants (Fowler, 2002).

The instruments were drafted based on the sources discussed in the literature review and reviewed by the author and other individuals familiar with control, security, and fear of crime literatures. Further, the author interviewed a number of the faculty at the University of Pittsburgh to determine the face validity of the survey (Boss, Butler, & Frieze, 2005). The pretest instruments are shown in Appendix A.

4.2.1.1 Pretest Subjects

The pretest was administered to 32 MBA students at the University of Pittsburgh. The sample consisted of 24 males and 8 females, all of whom had either previous work experience or were currently employed. Participants ranged in ages from 24 to 50 with an average age of 30. The participants were instructed to fill out the survey as if they were taking it in their own organization. Participants were asked to indicate any unclear or ambiguous wording or instructions and were also asked to note any issues with the flow of the survey. The respondents were timed to determine the length of the survey. All participants completed the survey within 15 minutes. All respondents were given extra credit for participation.

Participants identified questions that were either confusing or ambiguous. One area in particular about which respondents expressed concern related to the measures of direct and indirect experience. The original measure asked respondents to indicate their "…level of experience with each of the following scenarios" and listed a number of scenarios. This was revised to ask respondents to indicate the "…number of times they had experienced the following scenarios" on a 5-point scale with the following anchors:

- Never
- Once
- 2-3 Times
- Several Times
- More Than 5 Times.

The changed portion of the questionnaire was re-administered to the original respondents who responded positively to the change.

4.2.1.2 Pretest Analysis and Validation

The technical validation of the questionnaire looked first at the reliability of each of the constructs in the form of Chronbach's Alpha to test for internal consistency. As noted below in Table 1, all of the independent variable alphas, with the exception of the Direct Experience ("revised" 5-item version), have values above .70 in accordance with the convention for acceptable reliability (Nunnally, 1978; Nunnally & Bernstein, 1994). What was surprising was that the Direct Experience measure failed to meet this test. This may indicate that the construct is a formative rather than a reflective construct as noted in Chin (1998b).

Table 1 – Pretest Scales and Reliabilities

Scale	# of Items	N	Alpha	Mean	Std Dev	Range
Measurement	7	29	.93	3.51	1.48	1.00 - 6.29
Evaluation	6	30	.97	2.12	1.24	1.00 – 5.67
Reward	6	30	.80	2.17	1.00	1.00 - 4.17
Perceived Mandatoriness	5	31	.92	3.44	1.93	1.00 - 7.00
Direct Experience	13	25	.78	1.75	0.57	1.00 - 3.35
Direct Experience (revised 5-point scale)	13	26	.64	1.58	0.31	1.00 - 2.23
Indirect Experience	13	30	.92	3.24	1.31	1.15 - 6.54
Indirect Experience (revised 5-point scale)	13	26	.94	2.97	1.08	1.00 - 7.00
Perceived Risk	13	32	.92	3.05	1.11	1.23 - 5.38
Precautions Taken	14	21	.73	4.85	0.85	3.50 - 6.50

Correlation data show that there is a high degree of association between measurement, evaluation, reward, and mandatoriness, so much so that multicollinearity issues make it difficult to distinguish between constructs. As shown below in Table 2, the correlation scores constructs for the measurement, evaluation, reward, and perceived mandatoriness indicate that the

relationships between constructs are both significant and the correlation coefficients are very high.

Table 2 – Pretest Correlations

	Measure-ment	Eval-uation	Reward	Manda-toriness	Direct Experience (7 pt scale)	Direct Experience (5 pt scale)	Indirect Experience (7 pt scale)	Indirect Experience (5 pt scale)	Risk	Precautions Taken
Measurement	1									
Evaluation	0.73**	1								
Reward	0.52**	0.63**	1							
Mandatoriness	0.82**	0.73**	0.55**	1						
Direct Experience (7 pt scale)	0.09	0.23	0.17	0.17	1					
Direct Experience (5 pt scale)	-0.11	-0.02	0.04	0.03	.59**	1				
Indirect Experience (7 pt scale)	0.21	0.36*	0.25	0.27	.56**	0.38	1			
Indirect Experience (5 pt scale)	-0.24	-0.17	-0.20	-0.10	0.20	0.29	0.51**	1		
Risk	0.17	0.17	0.03	0.01	0.44*	0.38	0.33	0.01	1	
Precautions Taken	0.1872	0.03	0.22	0.34	-0.16	-0.20	0.07	0.42*	-0.49**	1

** p<.01 * p<.05

A factor analysis of the measurement, evaluation, reward, and mandatoriness constructs, shown below in Table 3, shows high loading score across constructs. While these issues may be an artifact of the small sample size, a number of steps were taken to correct the issues identified as noted in the next section.

Table 3 – Pretest Factor Loadings

Factor Loadings*					
	1	2	3	4	5
Meas01		0.811			
Meas02		0.706			
Meas03		0.846			
Meas04			0.462	0.620	
Meas05		0.846			
Meas06		0.711			
Meas07		0.733			
Eval01	0.767				
Eval02	0.831				
Eval03	0.827				
Eval04	0.553			0.547	
Eval05	0.843				
Eval06	0.821				
Rew01	0.546		0.528		
Rew02					0.763
Rew03				0.825	
Rew04			0.763		
Rew05			0.884		
Rew06			0.789		
Mand01		0.770			
Mand02					0.711
Mand03	0.493	0.568			0.546
Mand04	0.787				
Mand05	0.475	0.605			0.503

*Loadings <.45 removed for readability

4.2.1.3 Actions Based on the Pretest

All of the items, with the exception of the direct and indirect experience constructs, were standardized to rating questions on a standard Likert-type 7-point scale asking the "…degree to which you agree or disagree with the following statements" with possible answers ranging from Strongly Disagree to Strongly Agree as suggested by Mangione (1995). Likewise, the questions were rewritten to be unidimensional (Mangione, 1995). Each scale was trimmed to include only the most relevant questions relating to the study with those that the respondents indicated were confusing being removed. This resulted in four items for each of the control variables (measurement, evaluation, reward, punishment, and perceived mandatoriness) and nine items for each of the risk-related variables (direct experience, indirect experience, and perceived risk). Finally, the items were examined for ambiguous wording and changed as deemed necessary.

On the construct level, the measurement construct was re-named specification.[3] The reward measure was additionally split into two constructs, reward and punishment, based on discussions with respondents who indicated that they felt that the concepts were separate regarding computer security. Mandatoriness was also re-examined and the wording was changed to more accurately reflect the concept of a mandate, and to separate it conceptually from the specification described earlier (Chae & Poole, 2005). All of these changes are reflected in the pilot test instrument shown in Appendix B.

[3] Following Eisenhardt (1985), Kirsch (2004) used "measurement" instead of "specification." However, the term "specification" better captures the meaning of this element since it emphasizes "… articulating specific behaviors and outcomes … common norms and values" (Kirsch 2004, p. 377).

4.2.2 Pilot Test

The pilot study is used to identify potential problems before starting a major data collection. In many ways the objectives are similar to those of the pretest except that it extends to the target population. The pilot study allows researchers to understand how data collection procedures and instruments work under realistic conditions. In this research the pilot served several purposes. First, the pilot study helped identify what would be encountered during the main data collection. Second, the pilot allowed us to identify and further refine our instruments in terms of reliability and validity. Several changes were made after the pretest and this gave us an opportunity to test those changes. Third, the pilot provided additional feedback about the reactions of individuals to the instruments including potential issues regarding sensitive subjects such as reward and punishment. Finally, the pilot study allowed testing of the on-line data collection mechanisms prior to the main data collection.

4.2.2.1 Pilot Test Subjects

The pilot study was conducted as a field survey at a large public institution on a population of approximately 180 individuals within the Information Systems Department (ISD). ISD had recently implemented security policies and procedures and declared them "mandatory" for all employees, similar to the theory discussion above; thus the responses from this department were deemed appropriate to use to answer the questions of validity and reliability. The instrument administered as part of the pilot study can be viewed in Appendix B.

The survey was electronically administered from November 1, 2005 to November 14, 2005. Potential respondents received an e-mail soliciting their participation by their managers prior to data collection on November 1, 2005. An invitation to participate e-mail was sent to the

population on November 1, 2005 and one reminder e-mail was sent seven days later. The full text of the e-mail messages sent to the potential respondents can be seen in Appendix D, Section D.1.

To provide valid responses, individuals were assigned an ID number by the third party who collected the data. Individuals were required to submit this ID number in order to fill out the survey. The ID number was used for three purposes:

1. To link the individual with an e-mail so the respondent could be invited to participate.
2. To prevent unauthorized respondents from answering the questionnaire, thus invalidating the collected data.
3. The ID was used to allow us to identify the individual who was to receive the prize from a random drawing for filling out the survey.

The ID list was maintained by the third party and was/is available on request from that party.

Of the 180 potential participants 70 individuals (approximately 39 percent) participated in the study. On examination of the data, one response was dropped because of spurious data (all questions were answered "1") leaving a valid sample of 69 or 38 percent. The sample consisted of 14 males, 34 females, and 21 individuals who chose not to disclose their gender. The respondents' education ranged from some high school to graduate degrees, with over 80 percent having at least an associates degree or higher (2% High School, 18% Some College, 40% Associates Degree, 9% Bachelors Degree, 31% Graduate Degree). Participants covered a wide range of positions, from help desk operators to network administrators to managers. Other descriptive statistics for the sample are shown below in Table 4.

Table 4 – Pilot Test Subject Characteristics

Characteristic*	Mean	Min	Max	n
Job Tenure (in Years)	6.76	0	30	66
Computer Expertise (in Years)	16.96	3	39	66
Age (in Years)	38.05	22	53	40

*Note: All characteristics are self reported

4.2.2.2 Common Method Bias Tests

With 69 data points it is possible to assess the likelihood of common method bias, or the extent to which the use of a single individual to measure both the independent and dependent variables, introduces bias within the study. Determination of common method bias is done by testing if a portion of the method influences the responses to the survey. Following Podsakoff and Organ (1986), a factor analysis of all scale response items shows 19 components explaining 88 percent of the variance, with no single factor accounting for variance across items. Lindell & Whitney (2001) note that a method bias would appear as an inflated level of bivariate correlations amongst all representative items, thus a correlation matrix with at least one non-significant correlation can be taken as absence of method bias. Examination of this matrix showed many items that were correlated, but many that were not correlated with each other. A similar examination of correlations among construct scores shows a lack of correlation as well. Together these tests suggest that common method bias is unlikely in the collected data.

4.2.2.3 Pilot Test Validation

The constructs measured in the pilot study included those from the pretest as well as three new constructs: punishment, apathy, and computer self-efficacy. Punishment, as noted earlier, is related to reward, but measures different aspects relating to penalties. Punishment is defined as

the perception that individuals will be sanctioned in some way for failure to follow required policies and procedures. Apathy and computer self-efficacy (CSE) were discussed as part of the description of the theoretical model. The items used in the apathy and CSE constructs are shown in Appendix E Sections E.1 and E.2.

A reliability analysis of the scales was performed and is summarized below in Table 5. Unlike the pretest, all of the main independent variables have a general reliability score (Chronbach Alpha) well above the generally accepted minimum of .70 (Nunnally, 1978; Nunnally & Bernstein, 1994). The co-variants also did well with CSE having a Chronbach's Alpha of .95 and apathy having a score of .79.

Table 5 – Pilot Test Scales and Reliabilities

Scale	# of Items	n	Alpha	Mean	Std Dev	Range
Specification	4	69	.84	5.50	1.03	3.00 – 7.00
Evaluation	4	69	.94	3.94	1.40	1.00 – 7.00
Reward	4	69	.89	3.00	1.44	1.00 – 7.00
Punishment	4	69	.80	4.95	1.20	1.75 – 7.00
Mandatoriness	4	69	.84	5.82	1.08	3.25 – 7.00
Direct Experience	9	69	.80	1.41	0.48	1.00 – 4.56
Indirect Experience	9	69	.92	3.64	1.09	1.00 – 5.00
Perceived Risk	9	69	.94	2.80	1.22	1.00 – 5.67
Precautions Taken	16	69	.83	6.03	0.67	4.13 – 7.00
Computer Self-Efficacy	10	69	.96	5.71	1.13	1.30 – 7.00
Apathy	6	69	.79	2.27	0.98	1.00 – 4.75

Examination of the statistics on a construct by construct basis showed that the direct experience construct has an unusually low mean (1.41 of 5). This could be due to several factors. First, our sample from ISD may be unusually vigilant, thus have very few computer security incidents which is supported by the high mean (6.03) in precaution taking. Other issues

may be that the small number of participants (69) may not give us enough variability to truly measure the population. A final reason may be, as noted in the description of the pretest, that this construct is formative rather than reflective (W. W. Chin, 1998b).

Factor analysis was performed in three separate analyses due to the low number of responses to the survey. The first analysis examined the control element variables and mandatoriness. The second grouping examined the risk and experience variables. The final analysis examined mandatoriness, risk, and precautions taken.

Factor analysis of the control literature variables showed a good separation of items along construct lines. Mandatoriness item 4 was dropped

Mand04 Regulatory compliance requirements (FERPA, HIPAA, etc.) emphasize the need for me to follow the University's IT security policies, procedures, and guidelines to the best of my ability.

because this aspect of mandatoriness is externally or legislatively imposed as opposed to the other items which are imposed or generated from within the organization. A factor analysis of the specification, evaluation, reward, punishment, and mandatoriness constructs showed all the items loading on their relative constructs with at least a 0.40 factor value as shown below in Table 6.

Table 6 – Control Element Factor Analysis

Factor Loadings*					
	1	**2**	**3**	**4**	**5**
Spec01			0.738		
Spec02			0.687		
Spec03			0.789		
Spec04			0.681		
Eval01	0.893				
Eval02	0.894				
Eval03	0.897				
Eval04	0.785				
Rew01		0.650			
Rew02		0.743			
Rew03		0.865			
Rew04		0.918			
Punish01					0.701
Punish02					0.805
Punish03					0.728
Punish04					0.589
Mand01				0.813	
Mand02				0.843	
Mand03				0.773	

*Loadings <.45 removed for readability

Analysis of the risk/experience items do not indicate cross loadings, as shown in Table 7, but item Dir04 has no value because it does not load strongly (more than 0.40) on any of the factors.[4]

[4] While Dir04 does not load strongly on any of the factors, since this is exploratory research, it was retained for the analysis. The discussion of items to retain or drop is in dialog following these results.

Table 7 – Risk Element Factor Analysis

Factor Loadings*			
	1	**2**	**3**
Risk01	0.858		
Risk02	0.899		
Risk03	0.910		
Risk04	0.801		
Risk05	0.918		
Risk06	0.796		
Risk07	0.766		
Risk08	0.762		
Risk09	0.779		
Indr01		0.824	
Indr02		0.772	
Indr03		0.741	
Indr04		0.580	
Indr05		0.829	
Indr06		0.820	
Indr07		0.860	
Indr08		0.890	
Indr09		0.709	
Dir01			0.650
Dir02			0.824
Dir03			0.781
Dir04			
Dir05			0.771
Dir06			0.580
Dir07			0.565
Dir08			0.672
Dir09			0.744

*Loadings <.45 removed for readability

When a factor analysis is performed on the mandatoriness, risk, and precautions taken items, some cross-loading does occur between mandatoriness and precautions taken as shown in Table 8. As with the analysis of risk elements, item Prec16 does not load because it does not load strongly (more than .30) on any of the factors:

Table 8 – Risk, Mandatoriness, and Precautions Taken Factor Analysis

Factor Loadings*			
	1	**2**	**3**
Risk01	0.841		
Risk02	0.854		
Risk03	0.88		
Risk04	0.738		
Risk05	0.900		
Risk06	0.787		
Risk07	0.748		
Risk08	0.725		
Risk09	0.764		
Mand01			0.704
Mand02		0.459	0.525
Mand03		0.342	0.639
Mand04			0.619
Prec01		0.503	0.522
Prec02		0.686	0.405
Prec03		0.732	
Prec04		0.767	
Prec05	-0.302	0.628	
Prec06		0.8	
Prec07		0.514	
Prec08		0.424	0.437
Prec09		0.452	
Prec10			0.322
Prec11		0.347	
Prec12			0.73
Prec13			0.743
Prec14			0.618
Prec15		0.492	
Prec16			

*Loadings <.30 removed for readability

This cross-loading may be due more to the placement of the questions in the questionnaire (mandatoriness is placed immediately before precautions taken and only the first two items of precautions taken load with mandatoriness).

Further analysis, both theoretical and statistical, of the dependent variable show that there are a number of theoretical sub-constructs within the main construct: *General Precautions* (item

1 to item 3) show the general precaution-taking awareness of individuals and comprise a reflective construct. *Task Specific* precautions individuals can take (items 4 to 8, and item 16), *Interactive* precautions (items 9 to 11, and item 15), or how individuals interact with others to take precautions, and *Reporting* precautions (items12 to 14), or how individuals report issues to superiors. The general precautions measure is clearly reflective where a change in the underlying construct will result in a change of all of the variables. The other sub-constructs, however, do not meet this criterion and appear to be formative. Each of the items of the other precautions taking constructs (task specific, interactive, or reporting) would be caused by the indicators and do not necessarily change or covary in conjunction with the other indicators (W. W. Chin, 1998b). To simplify the subsequent analysis of the pilot test, I intend to use only the reflective construct "general precautions" to analyze these results. Discussion regarding the multi-dimensionality of the dependent variable can be found below in Section 4.2.2.7.

The multicollinearity issue noted in the pretest has been reduced to a manageable level with more data points. As shown below in Table 9, the constructs are still significantly correlated with each other, but the coefficients are not as high as they were in the pretest. Additionally, a regression analysis of the variables result in a variable inflation factor (VIF) score of no higher than 1.5, while the maximum cutoff VIF score is generally considered to be 10 where multicollinearity makes the model un-testable (Neter, Wasserman, & Kutner, 1990).

Table 9 – Pilot Test Correlation Matrix

	Specification	Evaluation	Rewards	Punishment	Mandatoriness	Direct Experience	Indirect Experience	Risk	Precautions
Specification	1.00								
Evaluation	0.43**	1.00							
Rewards	0.40**	0.47**	1.00						
Punishment	0.43**	0.36**	0.44**	1.00					
Mandatoriness	0.58**	0.36**	0.23	0.59**	1.00				
Direct Experience	0.04	-0.04	0.07	0.06	-0.03	1.00			
Indirect Experience	0.31**	-0.02	-0.05	-0.08	0.25*	0.13	1.00		
Risk	-0.31*	-0.08	0.10	-0.12	-0.17	0.04	-0.23	1.00	
Precautions	0.46**	0.25*	0.24	0.37**	0.37**	-0.06	0.03	-0.17	1.00

** p<.01 * p<.05

4.2.2.4 Pilot Test Results – Regression Analysis

Regression analysis is performed as outlined in Baron & Kinney (1986) to test for mediated effects on our outcome variable. In order to do this, however, the data have to conform to the assumptions of normality required by traditional regression analysis. Further, to show mediated effects of the independent variables on the dependent variable, the following steps need to be taken:

1. Regress the mediator on the independent variables
2. Regress the dependent variable on the independent variables
3. Regress the dependent variable on both the independent variables and the mediator variable

To show mediation, the following conditions need to hold: First, the independent variable must show a significant effect on the mediator variable in Step 1. Second, the independent variable must likewise significantly affect the dependent variable in Step 2. Third, the mediator must significantly affect the dependent variable in Step 3. Finally, if all of these relationships hold in the predicted direction, then the effects of the independent variable in Step 3 must be less than the effects shown in Step 2.

The specification, evaluation, reward, punishment, and mandatoriness constructs approximately conformed to the assumptions of normality so were left unchanged. General precautions taken, however, is negatively skewed and thus non-normal as required to perform regression analysis. Recoding to a thermometer measure of Low, Moderate, and High was done based on data quartiles using the top 25 percent of responses as high, the lower 25 percent as low, and the middle 50 percent of responses as medium. General precautions were used instead

of the overall measure of precautions taken based on the results of the previously described factor analysis.

Each of the steps to test for mediation for the control aspects of the hypothesized model is detailed below in Table 10:

Table 10 – Control Variable – Regression Beta Coefficients

	Step 1 DV=Mandatoriness	**Step 2 DV=General Precautions**	**Step 3 DV=General Precautions**
(Constant)	1.55	0.11	-0.19
Specification of Polices	0.55***	0.32***	0.21*
Evaluation Performed	0.05	-0.02	-0.03
Rewards Given	-0.14	-0.07	0.02
Punishment Given	0.31**	0.08	-0.020
Mandatoriness			0.20*
Adjusted R^2	0.42***	0.16**	0.20**

*** p>.001 ** p>.01 * p>.05 † p>.10

Step 1 regresses the mediator (mandatoriness) on the independent variables (specification, evaluation, reward, and punishment) and is shown in the second column of Table 10. This analysis shows that only the effects of specification (Hypothesis 1) with a β of 0.55 ($p<0.001$) and punishment (Hypothesis 3_B) with a β of 0.31 ($p<0.01$), have any effect on mandatoriness. Step 2 regresses the dependent variable (general precautions) on the independent variables (specification, evaluation, reward, and punishment) and is shown in the third column of Table 10. Specification (Hypothesis 1) is the only independent variable that has any effect on general precautions ($\beta=0.21$ ($p<0.05$). Finally Step 3 regresses the dependent variable (general precautions) on both the independent variables and the mediator (mandatoriness) where both specification (Hypothesis 1) and mandatoriness (Hypothesis 4) affect general precautions. Since specification's effects on the independent variable are lower in Step 3 (0.21) than in Step 2

(0.32), mandatoriness fully mediates the effects of specification on precautions taken, while it is not a mediator for the other three variables.

The risk aspects of the model present more of a problem. The data for direct experience and risk perceptions are highly positively skewed while the data for indirect experience are highly negatively skewed. To proceed with a regression-based analysis requires that we recode the data to an approximate normal distribution. The data for all three constructs were recoded to a thermometer measure of Low, Moderate, and High, again using the highest and lowest quartile of responses as high and low, and the remaining responses coded as moderate. Again, the dependent variable for this portion of the analysis is general precautions, a subset of precautions taken.

As with the control portion of the model, the risk hypotheses of the model must be tested in the same way (Baron & Kenny, 1986). Each of the steps of the risk aspects of the hypothesized model is detailed below in Table 11:

Table 11 – Risk Variables – Regression Beta Coefficients

	Step 1 DV=Risk Perceptions	**Step 2 DV=General Precautions**	**Step 3 DV=General Precautions**
(Constant)	2.08	1.64	2.15
Direct Experience	0.23*	-0.06	-0.00
Indirect Experience	-0.34*	0.22†	0.14
Risk Perceptions			-0.25*
Adjusted R^2	0.13**	0.02	0.06†

*** p>.001 ** p>.01 * p>.05 † p>.10

Similar to the regression analysis above, we can see that Hypothesis 5 (direct experience on risk) is supported (β=0.23, $p<0.05$) as shown in column two above while Hypothesis 6 (Indirect

experience on risk) is not supported but is significant in the opposite direction with an adjusted R^2 of 0.13. Further, risk perceptions do not mediate the relationship between precautions taken and either direct or indirect experience.

Finally, we regress general precautions taken on mandatoriness and risk perceptions, and get the following results (Table 12):

Table 12 – Mandatoriness and Risk Regression Coefficients

	DV=Precautions
(Constant)	0.78
Perceived Mandatoriness	0.26***
Risk	-0.18†
Adjusted R^2	0.23***

*** p>.001 ** p>.01
* p>.05 † p>.10

Hypothesis 4 (mandatoriness on precautions taken) is supported with an adjusted R^2 of 0.23, while Hypothesis 7 (risk perceptions on precautions taken) is not supported and further shows a significant negative relationship opposite to the predicted relationship.

4.2.2.5 Pilot Test Results – Partial Least Squares (PLS) Analysis

In order to more fully test the hypothesis using the pilot test data, I decided to do an additional analysis using standard PLS analysis techniques. This structural equation modeling technique will do principal component analysis, path analysis, and regression to simultaneously evaluate both theory and data (Wold, 1982). PLS is further useful in exploratory research which focuses on prediction rather than covariance structure replication (Jèoreskog & Wold, 1982). Finally, this methodology is also particularly well suited to complex models, where the importance shifts from individual paths to groups of variables (Anderson & Gerbing, 1988).

While some of this analysis has already been done in the regression analysis above, it is worth repeating to determine the most effective way of analyzing the results of this study and will provide direction for the main data collection. There are three standard processes for assessing reliability of scales. Chronbach's coefficient alpha (Nunnally, 1978) where alpha scores exceed 0.70 are considered reliable. A second process is the measure of internal consistency developed by Fornell & Larcker (1981) and preferred in PLS analysis (W. W. Chin, 1998b). The goal of this analysis, similar to Chronbach's alpha, is to achieve a score greater than 0.70. A final test of scale reliability involves examining whether items have item loadings of at least 0.70 from PLS which demonstrates that the items share more variance with the construct than error variance (Carmines & Zeller, 1979).

Table 13 provides the relevant statistics for each item (the loadings and residual variance) and for each scale (internal consistency and Chronbach's alpha) for the variables that are theoretically reflective in nature. The variables that were determined to be formative in nature (direct experience, indirect experience, and risk) are shown to give the Chronbach's alpha only as it theoretically does not make sense to calculate the other reliability measures for formative constructs[5].

[5] The differences between the reflective and formative constructs are elaborated on at the end of this chapter and the results of this discussion and are implemented in the final data collection.

Table 13 – Pilot Test Reliability and Validity Measures

Variable	Loading /Weight	Residual Variance	Internal Consistency	Chronbach's Alpha	Average Variance Extracted	Square Root of AVE
Spec01	0.81	0.34				
Spec02	0.76	0.42				
Spec03	0.85	0.27				
Spec04	0.85	0.27				
Specification			0.89	0.84	0.67	0.82
Eval01	0.92	0.15				
Eval02	0.94	0.12				
Eval03	0.91	0.17				
Eval04	0.89	0.21				
Evaluation			0.95	0.94	0.84	0.91
Rew01	0.91	0.17				
Rew02	0.90	0.19				
Rew03	0.82	0.33				
Rew04	0.77	0.41				
Reward			0.92	0.89	0.73	0.85
Punish01	0.79	0.38				
Punish02	0.80	0.36				
Punish03	0.72	0.48				
Punish04	0.83	0.31				
Punishment			0.86	0.80	0.62	0.78
Mand01	0.90	0.19				
Mand02	0.89	0.21				
Mand03	0.89	0.21				
Mandatoriness			0.92	0.84	0.80	0.89
Prec01	0.91	0.17				
Prec02	0.96	0.08				
Prec03	0.80	0.36				
General Precautions			0.92	0.83	0.80	0.89
Direct Experience				0.80		
Indirect Experience				0.92		
Risk				0.94		

All scales demonstrated an internal consistency and alpha scores above 0.70, so all are acceptable from a reliability perspective.

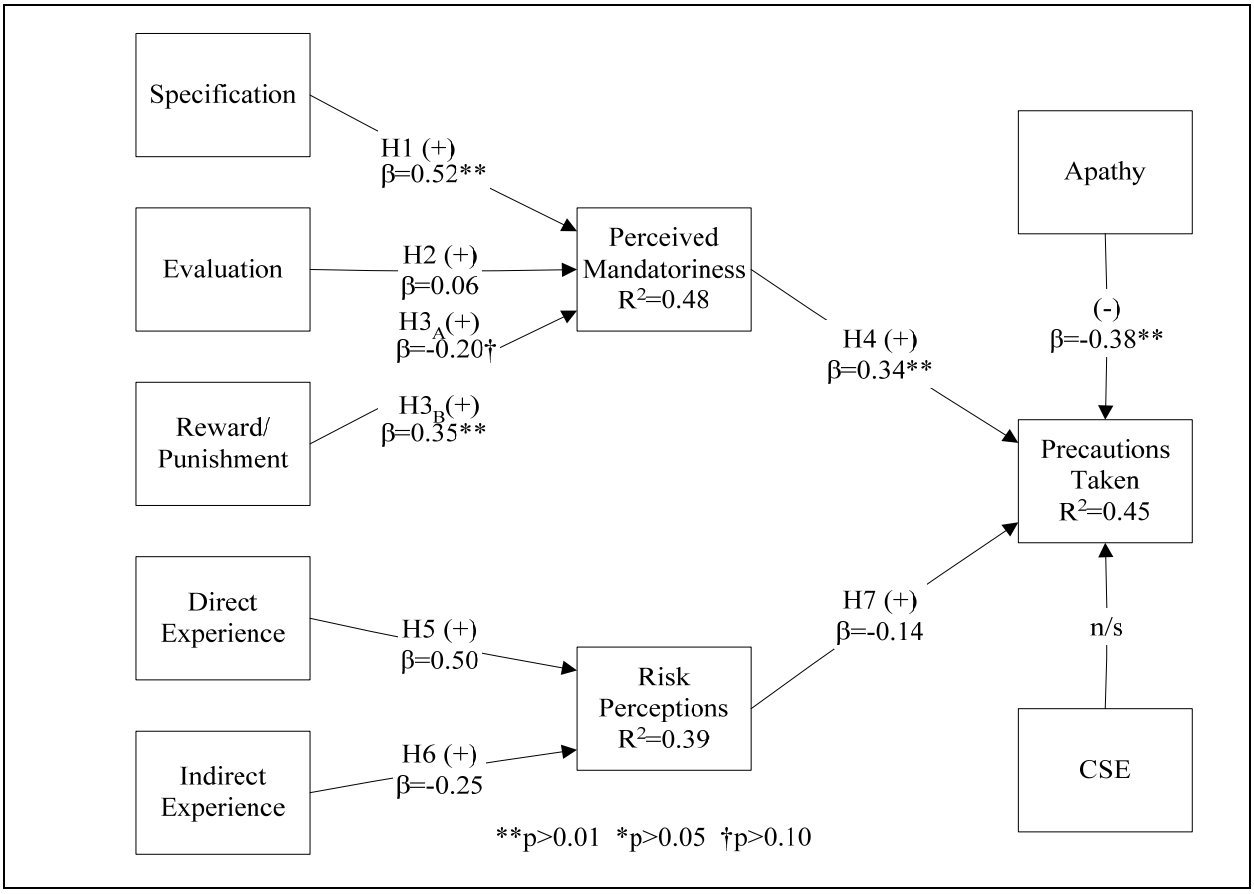
Initial assessment of convergent and discriminant validity were conducted using factor analysis with Varimax rotation and are shown above in the regression analysis in Table 7, Table 8, and Table 9. Convergent validity is demonstrated when the average variance extracted (AVE) by a construct's items is at least 0.50 (W. W. Chin & Gopal, 1995). AVE greater than 0.50 shows that the variance explained by the construct is greater than the variance explained by measurement error. An examination of Table 13 above shows that all constructs meet this criterion. Discriminant validity is assessed by comparing the correlations between two constructs with the square root of AVE of each construct. Correlations between two constructs that are greater than the square root of AVE are indicative of poor discriminant validity between the constructs involved. Examination of Table 13 and Table 14 shows that this model exhibits both convergent validity (all AVE scores are at least 0.50 or higher) and discriminant validity (the square root of AVE scores (in bold along the diagonal) is larger than the correlations between any two constructs) and we can thus conclude that the constructs are valid.

Table 14 – Construct Discriminant Validity Results

	Specification	Evaluation	Rewards	Punishment	Mandatoriness	General Precautions
Spec	**0.82**					
Eval	0.43	**0.91**				
Rew	0.40	0.47	**0.85**			
Pun	0.43	0.36	0.44	**0.78**		
Mand	0.60	0.31	0.20	0.49	**0.89**	
General Prec	0.53	0.24	0.21	0.32	0.54	**0.89**

The research hypotheses were tested by examining the size and significance of structural paths in the PLS analysis. The percentage of variance is shown below in Figure 3, with 48 percent of the variance being explained in the relationships between the control elements and mandatoriness and 39 percent of the variance being explained between experience and risk perceptions. Finally, 45 percent of the variance is explained between mandatoriness and risk perceptions and precautions taken.

Figure 3 – Pretest Path Coefficients Between Constructs



Through this analysis, similar to the regression analysis, we see support for Hypothesis 1 (specification on mandatoriness) and Hypothesis 3_B (punishment on mandatoriness) at the $p<0.001$ level with 48 percent of the variance (R^2) being explained by these variables. Likewise

we see that mandatoriness has a significant effect on general precautions taken ($p<0.001$) with an R^2 of 0.45. Again, similar to the regression analysis, evaluation does not significantly affect mandatoriness and reward has a significant negative effect ($p<0.10$) on mandatoriness. None of the risk hypotheses (Hypothesis 5 to Hypothesis 7) were supported in the PLS analysis. The control variable apathy has a significant negative affect on general precautions taken ($p<0.001$), but CSE did not have a significant affect in this analysis.

A comparison of hypotheses based on the different analysis methods are shown below in Table 15.

Table 15 – Hypotheses Results Summary

Hypothesis	**Regression**	**PLS**
H_1 (Specification → Mandatoriness)	Supported	Supported
H_2 (Evaluation → Mandatoriness)	Not Supported	Not Supported
H_{3A} (Reward → Mandatoriness)	Not Supported	Not Supported Significant in the opposite direction
H_{3B} (Punishment → Mandatoriness)	Supported	Supported
H_4 (Mandatoriness → Gen. Precautions)	Supported	Supported
H_5 (Direct Experience → Risk)	Supported	Not Supported
H_6 (Indirect Experience → Risk)	Not Supported Significant in the opposite direction	Not Supported
H_7 (Risk → Gen. Precautions)	Not Supported	Not Supported

4.2.2.6 Pilot Test Discussion

First, regarding the control aspects of the model, as predicted, Hypothesis 1 was supported across both types of analysis: specification of a policy or procedure does significantly predict precaution-taking behavior. Further specification of a policy or procedure is fully mediated by an individual perception of mandatoriness using regression. Second, the perception of punishments being affixed to failure to follow policies and procedures significantly contributed

to the level of perceived mandatoriness (Hypothesis 3B) using both regression and PLS. Surprising results were that neither evaluation of a control nor reward for following a control (Hypothesis 2 and Hypothesis 3A) contributed significantly to mandatoriness. Further regression analysis shows that evaluation and control also do not contribute toward precautions being taken without the mediating factor of mandatory perceptions. This may be an artifact of the surveyed population: an IS department may view security policies and procedures in a different way than other populations. A better reason for this may be that this population is only provided with specification of the policy or procedure and then only punished for failure to conform to those directives. Speculatively, evaluation is probably implied, but rarely performed within IS organizations until there is a need to make an example of someone. Anecdotally, rewards are rarely given to individuals for adherence to policies and procedures; rather, adherence is an expectation (as shown by the perceptions of mandatoriness – Hypothesis 4), and thus individuals would only be punished for non-compliance.

The risk aspects of the model, examined using PLS, and with regression after normalizing the variables have the following results: Risk perceptions are driven by direct experience (Hypothesis 5) in regression, but are reduced by indirect experience (negative significant effect of Hypothesis 6). On the other hand, individuals do take precautions based on indirect experience, but do not take precautions based on direct experience. Finally, perceptions of risk significantly reduce the amount of precautions taken by individuals. The adjusted R^2 results of these sections of the model are relatively low providing little explanatory power for this section of the model. The reasons for this low explanatory power and results that contradict extant literature may be that I am missing a critical aspect of risk and risk perceptions: impact.

The failure to find support for the risk hypotheses (Hypothesis 5 to Hypothesis 7) using PLS may support this explanation.

Individuals can perceive that they are at risk, but if the impact is low, they will neglect to take precautions. This means that an impact component will need to be added to the risk aspects of the model. Additionally, there is a decided lack of variance in the experience measures which may be masking the true effects of experience on risk perceptions. The main data collection will have more variability as it will comprise more departments than our pilot study included. Further, it may be that the risk aspects of the model are best measured as formative constructs rather than reflective constructs. The variety of facets of direct and indirect experience as well as the multidimensionality of risk perceptions and precautions taken means that the measure will not necessarily covary. This suggests that a tool such as PLS, which allows formative constructs, may be appropriate for this research.

4.2.2.7 Actions Based on the Pilot Test

Methodologically, the changes that need to be made prior to the main data collection are as follows: First, the risk aspect of the model (direct experience, indirect experience, and risk perceptions) should be measured formatively and integrated into the full model. Second, the multidimensionality of the dependent variable (general, task specific, interactive, and reporting precautions) should be explored, but the overall analysis should probably focus on the more generalizable "general" precautions taken as this sub-construct is more generalizable to an entire group and addresses the "general" issues regarding computer security. I will collect data on all of the items during the full data collection, but will then evaluate the dependent variable prior to final analysis. Finally, an "impact" construct will be incorporated into the risk aspects of the

model. This will help us provide more meaningful results in our analysis of risk. These impacts would then be multiplied by the analogous risk perceptions or used as an additional construct to provide a more comprehensive measure of risk to compare against precautions taken (Barki et al., 1992, 2001). These results will be more reflective of the actual state of mind of the participants.

Analytically, due to the formative nature of the risk constructs described above, as well as the need to evaluate the overall model, I have decided that the testing of the main data collection will be done using Partial Least Squares (PLS) instead of using regression analysis.

Operationally, there were a number of things learned from the pilot study that will be applied to the main data collection. First, the need to have upper level management support from the beginning: At the request of the security officer at the data collection site, all communications with the director of ISD were handled by the security officer. This resulted in delay and confusion throughout the data collection process. In future data collections, I will meet personally with the head of the organization being surveyed to obtain their support and for collaboration. Second, one of the issues that respondents had with the study was the inclusion of questions regarding punishment. This led to the data collection itself being suspended one week into the collection. To mitigate this, future data collections will place the reward and punishment questions alongside each other to show parallel questions to try not to alarm respondents.

4.3 OPERATIONALIZATION OF THE RESEARCH CONSTRUCTS

It is important to consider the way that the constructs included in the research model are operationalized, as this has an impact on the ability of the model to test the hypothesized

relationships (Straub, 1989). Several steps have been taken to help ensure that the measures are both valid and reliable: First, each of the constructs is measured using multiple items and, when possible, the items have been adapted from previously developed instruments. Second, for constructs where no previously developed instruments exist, new measures were created based on the appropriate literature. Third, each of the constructs was statistically evaluated for validity and reliability.

Following is a description of the operationalization of each of the research constructs as they were administered in the final data collection. This section reflects the changes made based on the pretest and pilot test. The descriptions focus on how the constructs are measured including the items and the source of the items. Tables provide the complete set of items included on the surveys for each construct. The items themselves are generalized, but were adapted to the specific organization during the testing phase by providing relevant terminology and department-specific references. Versions of the survey used for the pretest, pilot test, and main data collection are located in Appendix C with the final wording of the items for the main data collection shown in the tables below.

4.3.1 Specification

This construct measures the individual perceptions of the existence of corporate policies and/or procedures dealing with computer security. This construct includes four items measured on a 7-point Likert scale. These items are shown below in Table 16. Items were adapted from elements of control specification identified in Kirsch's (1996) Behavioral Control Composite Measure (adapted from Daft & Macintosh (1981)) and the Cardinal (2001) Formalization Measure (adapted from Aiken & Hage (1968), Dewar & Werbel (1979), and Hall (1968)). These items

assess the level of awareness individuals have about the existing policies and procedures in their organization.

Table 16 – Survey Items: Specification

Item	Question
Please indicate the degree to which you agree or disagree with the following statements.	
Spec01	I am familiar with the organization's IT security policies, procedures, and guidelines.
Spec02	I am required to know a lot of existing written procedures and general practices to secure my computer system.
Spec03	There are written rules regarding security policies and procedures at the organization.
Spec04	The organization's existing policies and guidelines cover how to protect my computer system.

4.3.2 Evaluation

This construct measures the individual perceptions that managers sift through, organize, and analyze collected data to reach a conclusion regarding individual compliance with the specified policies and procedures. This construct includes four items measured on a 7-point Likert scale and shown below in Table 17. Items were adapted from the Cardinal (2001) Frequency of Performance Appraisal measure (adapted from Abbey (1982)) and general control literature (Eisenhardt, 1985). These items assess the level of awareness an individual has about the actions of management to measure compliance with specified policies and procedures in their organization.

Table 17 – Survey Items: Evaluation

Item	Question
Please indicate the degree to which you agree or disagree with the following statements.	
Eval01	Managers in my department frequently evaluate my security behaviors.
Eval02	Managers regularly examine data relating to how well I follow security policies and procedures.
Eval03	Managers formally evaluate me and my colleagues regarding compliance with security policies.
Eval04	Managers assess whether I follow organizational security procedures and guidelines.

4.3.3 Reward

This construct measures the degree to which individuals feel that they are rewarded for compliance with required security policies and procedures. This construct includes four items measured on a 7-point Likert scale. These items are shown below in Table 18. Items were adapted from the Kirsch (1996) Behavioral-Reward Link Measure (adapted from Lawler (1981)) and the Cardinal (2001) Rewards and Recognition Measure (adapted from Abbey (1982), Ivancevich (1983), and Kopelman (1976)). These items assess the perceptions that rewards exist and are awarded either formally or informally based on individual precaution-taking behavior relating to security in the organization.

Table 18 – Survey Items: Reward

Item	Question
Organizations use different approaches to reward and sanction employees. Please indicate the degree to which you agree or disagree with the following statements.	
Rew01	My pay raises and/or promotions depend on whether I follow documented security policies and procedures.
Rew02	I will receive personal mention in oral or written reports if I comply with security policies and procedures at this organization.
Rew03	I will be given monetary or non-monetary rewards for following security policies and procedures.
Rew04	Tangible rewards are tied to whether I follow the organization's IT security policies, procedures, and guidelines.

4.3.4 Punishment

The punishment construct is similar to the reward construct, but instead measures the negative aspects of control enforcement rather than the positive "reward" aspects. This dimension was included based on anecdotal evidence from corporate practice as well as feedback from pretest that individuals are not rewarded for security behaviors, rather they are punished for failing to adequately follow security polices and procedures. This construct includes four items measured on a 7-point Likert scale and shown below in Table 19. These items were adapted from the Kirsch (1996) Behavioral-Reward Link Measure (adapted from Lawler (1981)) and the Cardinal (2001) Rewards and Recognition Measure (adapted from Abbey (1982), Ivancevich (1983) and Kopelman (1976)).

Table 19 – Survey Items: Punishment

Item	Question
Organizations use different approaches to reward and sanction employees. Please indicate the degree to which you agree or disagree with the following statements.	
Pun01	I will be sanctioned for not complying with documented security policies and procedures.
Pun02	Senior management will be notified if I do not follow the organization's IT security policies, procedures, and guidelines.
Pun03	There are specific punishments tied to whether I follow security policies and procedures.
Pun04	Failure to secure my system by following the organization's IT security policies, procedures, and guidelines can have repercussions on my career.

4.3.5 Direct Experience

This construct measures the degree to which individuals have been previously personally been exposed to crime (Skogan & Maxfield, 1981). These items were adapted from a section of the U.S. Department of Justice (USDOJ) National Crime Victimization Survey specific to computer fraud, virus exposure, physical threat/obscene e-mail reception, and software copyright violation (USDOJ, 2001). The construct includes nine items measured on a "yes/no" basis relating to their personal experience. If respondents answered "yes" they were asked to indicate the impact of that experience on them measured on a 7-pont Likert scale. The direct experience items are shown below in Table 20.

Table 20 – Survey Items: Direct Experience

Item	Question
Please indicate whether or not you have ever experienced any of the following situations. If **YES**, please indicate the degree to which that experience impacted you (in terms of time lost, data lost, monetary losses, etc.).	
Dir01	My computer system corrupted by a virus or worm.
Dir02	My computer system taken over by a hacker.
Dir03	My current work data corrupted by a virus or cyber-attack.
Dir04	My identity stolen (credit card number, Social Security Number, Bank account information, etc.).
Dir05	My work lost due to a virus or worm on my computer.
Dir06	Computer resources (internal network, the Internet) inaccessible because of computer security problems.
Dir07	Downloading a file that is infected with a virus from the internet.
Dir08	Downloading a file that is infected with a virus through my e-mail.
Dir09	Any of my accounts being used by someone else without my knowledge.

4.3.6 Indirect Experience

Similar to the direct experience construct, this construct measures the degree to which an individual has been previously exposed to crime through other people's experiences (Skogan & Maxfield, 1981). These items were also adapted from a section of the USDOJ National Crime Victimization Survey specific to computer fraud, virus exposure, physical threat/obscene e-mail reception, and software copyright violation (USDOJ, 2001) and include the same nine items used in the direct experience measure to provide parallel information. Similar to direct experience, the construct is measured on a "yes/no" basis relating to personal experience. If respondents answered "yes" they were asked to indicate the impact of that experience on them measured on a 7-pont Likert scale. These items are shown below in Table 21.

Table 21 – Survey Items: Indirect Experience

Item	Question
Please indicate the number of times in the last year you have heard of others (**NOT YOU**) having the following experiences (e.g.: from friends, in discussions at work, in the media, etc.). If you have heard of others having these experiences, in general, to what degree do you think it impacted those people (in terms of time lost, data lost, monetary losses, etc.)?	
Indr01	Their computer system corrupted by a virus or worm.
Indr02	Someone's computer system taken over by a hacker.
Indr03	Someone's work data corrupted by a virus or cyber-attack.
Indr04	Identity stolen (credit card number, Social Security Number, Bank account information, etc.).
Indr05	Work lost due to a virus or worm on their computer.
Indr06	Computer resources (internal network, the Internet) inaccessible because of computer security problems.
Indr07	Other people downloading a file that is infected with a virus from the internet.
Indr08	Others downloading a file that is infected with a virus through my e-mail.
Indr09	Someone else's accounts being used by someone else without their knowledge.

4.3.7 Mandatoriness

This construct measures individuals' perceptions that that compliance with existing security policies and procedures is compulsory within the organization. This construct includes four items measured on a 7-point Likert scale that were adapted from the conceptualization of mandates discussed in Chae & Pool (2005) and explicitly stated in Hartwick & Barki (Hartwick & Barki, 1994) regarding the compulsory use of a system. Mandatoriness items are shown below in Table 22.

Table 22 – Survey Items: Mandatoriness

Item	Question
Please indicate the degree to which you agree or disagree with the following statements regarding this organization.	
Mand01	I am required to secure my system according to the organization's documented policies and procedures.
Mand02	It is expected that I will take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.).
Mand03	There is an understanding that I will comply with organization security policies and procedures.
Mand04	Regulatory compliance requirements (FERPA, HIPAA, Sarbanes-Oxley etc.) emphasize the need for me to follow the organization's IT security policies, procedures and guidelines to the best of my ability.

4.3.8 Perceived Risk

This construct measures two aspects of risk: The degree to which an individual feels that he is likely to experiencing a cyber-attack and the impact to him were it to happen (Frieze et al., 1987; Rountree & Land, 1996). The items were adapted from a section of the USDOJ National Crime Victimization Survey specific to computer fraud, virus exposure, physical threat/obscene e-mail reception, and software copyright violation (USDOJ, 2001) and include the same nine items used in both the direct experience and the indirect experience measures. Instead of asking whether respondents had experienced a specific scenario, the item assesses the degree to which individuals feel that it is likely they will experience the scenario, and assesses the impact to them were it to happen. The items are measured on a 7-point Likert scale and are shown below in Table 23 with likelihood (L) and impact (IM) captured in using two scales, respectively.[6]

[6] To see how this was operationalized, see Appendix C

Following Barki et al. (2001) an overall risk item will be constructed by multiplying the likelihood and impact scores together.

Table 23 – Survey Items: Perceived Risk

Item	Question
Please indicate the degree to which you believe that one of the following scenarios is likely to happen **TO YOU** at some point in the future**.** Additionally, please indicate the impact that it would have on you if it were to occur (in terms of time lost, data lost, monetary losses, etc.).	
Risk01 (L & IM)	A computer system corrupted by a virus or worm.
Risk02 (L & IM)	A computer system taken over by a hacker.
Risk03 (L & IM)	My work data corrupted by a virus or cyber-attack.
Risk04 (L & IM)	My identity stolen (credit card number, Social Security Number, Bank account information, etc.).
Risk05 (L & IM)	Work lost due to a virus or worm on my computer.
Risk06 (L & IM)	Computer resources (internal network, the Internet) inaccessible because of computer security problems.
Risk07 (L & IM)	Downloading a file that is infected with a virus from the internet.
Risk08 (L & IM)	Downloading a file that is infected with a virus through my e-mail.
Risk09 (L & IM)	Account being used by someone else without their knowledge.

4.3.9 Precautions Taken

Precautions taken is the dependent variable in this study. This construct measures the degree to which individuals feel that they are taking precautions to protect their computers. This construct was developed from professional standards and from general computer security best practices published by the National Cyber Security Alliance (2005) and are designed to capture many of the ways that individuals can take security precautions in dealing with a computer. This construct is comprised of 16 items measured on a 7-point Likert scale. These items are shown below in Table 24.

Table 24 – Survey Items: Precautions Taken

Item	Question
Please indicate the degree to which you agree or disagree with the following statements about how you take precautions to protect your computer system.	
Prec01	I pay attention to computer security during my daily routine.
Prec02	I keep aware of the latest security threats so I can protect my system.
Prec03	My system is as secure as I can make it.
Prec04	I regularly download security patches for my operating system/computer programs.
Prec05	I regularly download virus protection software updates.
Prec06	I regularly update the anti-spyware software on my computer.
Prec07	I update my e-mail spam filter on a regular basis.
Prec08	I take precautions with my passwords (Protect them, regularly change them, use multiple passwords, etc.).
Prec09*	I share my passwords with other people.
Prec10*	I allow non-employees access to my computer.
Prec11*	I allow other employees access to my computer.
Prec12	I notify a manager or IS personnel if I suspect that my system has been infected by a virus.
Prec13	I notify a manager if the system slows down to an unreasonable level.
Prec14	I report suspicious e-mails to a supervisor or security personnel in the Information Systems department.
Prec15*	I open attached executables from friends even if the message doesn't make particular sense.
Prec16*	I regularly download "unauthorized" software to install on my computer.

* Reverse Coded Items

4.4 CHAPTER SUMMARY

This chapter described the methodology used in this study, in terms of the research design, the measures used for the constructs in the research model, and the pretest, technical validation, and pilot test phases of validation (Straub, 1989). Whenever possible, items from previous instruments were adapted for this research. The survey instruments were pretested by MBA students for readability and to test the model. Likewise, the survey instruments were pilot tested

to provide technical validation and to refine the instruments. The data collection was performed and the data were examined for completeness and problem cases were removed. The respondents came from all areas of the targeted population and comprised approximately 49 percent of that population. In the next chapter the data are used to validate the instruments and test the hypotheses.

5.0 DATA COLLECTION, ANALYSIS, AND RESULTS

The primary objective of this research is to explore the effects that external controls and internal risk assessment have on individuals' precaution taking behavior. The previous chapter described the creation of items to support this research. This chapter describes the use of those items to collect cross-sectional data, analyze the data, and test the research hypotheses. The chapter is divided into the following sections: data collection and survey procedures, preliminary analysis, construct reliability and validity testing, hypothesis testing, and discussion of common method bias and the effects on this study.

5.1 DATA COLLECTION AND SURVEY PROCEDURES

Data collection for the main study took place in May 2006 at a large medical center located in the southeastern United States (SEMC). The organization employs approximately 4,750 people, of whom approximately 3,900 are female and 850 are male. Those targeted for participation were individuals who use computers on a daily basis as these employees are most likely to encounter computer security issues. The target group includes clerical support staff, professional services, technical services, nurses and nursing services, physicians, and management. The organization has historically been technologically oriented and has recently integrated their information systems with their medical records, resulting in almost all employees having to

utilize a computer on a daily basis. Additionally, HIPAA regulations require computer security training for hospital employees, which made this site a good choice for data collection.

The data were gathered through a web-based survey which was available to employees for a period of approximately three weeks. Individuals were contacted initially by e-mail informing them that SEMC was conducting a security study and would like their participation. User names and a link to the questionnaire URL were provided in the initial e-mail. Reminder e-mails were sent to individuals who had not yet filled out the survey throughout the collection period. Once the survey was complete, incentive awards for participation were distributed through a random drawing. The e-mails sent to the participants for both this data collection and the pilot test can be viewed below in Appendix D Section D.2.

The initial e-mail was sent by the organization's CEO on Tuesday, May 9, 2006. Follow up e-mails were sent on Friday, May 12, 2006; Friday, May 19, 2006 and Monday, May 22, 2006. On May 22, 2006, the organization's administration decided to extend the data collection period for one week and the organization sent a global e-mail reminding people to take the survey if they hadn't already participated. Additional reminder e-mails were sent out on Friday, May 26, 2006 and on Tuesday, May 30, 2006. The data collection officially finished at midnight on May 30, 2006, but the survey remained active until June 1, 2006. Nine respondents completed the survey on May 31 and June 1, 2006 and were subsequently included in the data set.

5.1.1 Respondent Demographics

The sample included personnel from all areas of the organization with staff nurses and office/clerical personnel having the highest number of responses. The full breakdown of the sample by organizational area is detailed in Table 25.

Table 25 – Respondent Position Descriptions and Frequencies

Position	Description (if necessary)	n	%
Office and Clerical	Secretary, Legal Assistant, Transcriptionist, Registrar, Clerk, etc.	381	22.7%
Support Services	Maintenance, Environmental Service, Facilities, Security, Nutrition Services, Materials Management/Purchasing, etc.	53	3.2%
Professional Services	Non-Managerial Positions Such as Pharmacist, PT, OT, Speech Therapist, Accountant, Auditor, Dietitian, COTA, CPTA, etc.	161	9.6%
Technical Services	Non-Managerial Positions Such as Medical Lab Tech, Cyto-Tech, Radiology Tech, Rehab Tech, Respiratory Therapist, CRTT, etc.	194	11.5%
Staff RN		476	28.3%
Other Nursing Services	LPN, Nurse Tech, PCA, etc.	126	7.5%
Physician		37	2.2%
Coordinator		81	4.8%
Team Leader, PDS		10	0.6%
Manager		112	6.7%
Director		40	2.4%
Administration	Executive Director, Vice President, CEO	11	0.7%
	Total*	1682	100.0%

*Note: 15 respondents (0.9% of the total data set) did not indicate their position when completing the survey.

Respondents' education ranged from some high school to graduate degrees, with 93 percent having at least some college education. The sample consisted of 1471 females (87 percent) and 226 males (13 percent) which generally reflects the population of SEMC, which is 85 percent female and 15 percent male overall. Descriptive statistics for the sample are shown

below in Table 26 along with total organizational means for tenure and age which were obtained from SEMC records.

Table 26 – Respondent Demographic Characteristics

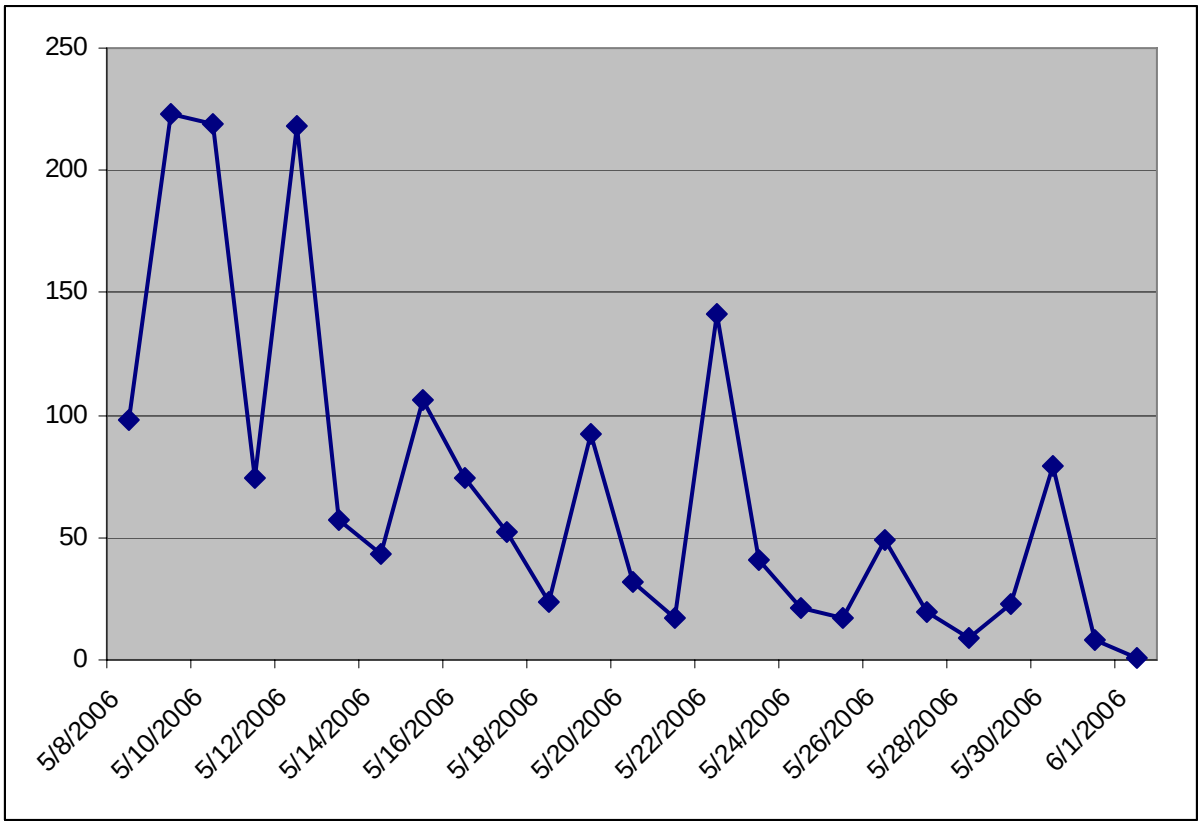
Characteristic	Mean	SD	Org Mean	Min	Max	n
Job Tenure (Years)	8.29	8.18	8.42	0.2	47	1696
Computer Expertise (Self Reported, In Years)	13.34	6.55	--	1.0	40	1660
Age (Years)	41.82	10.87	42.68	21.0	78	1696

Additional analysis of the response patterns indicate that the respondents are distributed throughout the organization in approximately the same proportions as the general organizational population.

5.1.2 Response Rate and Non-response Bias

With the electronic responses it is possible to track responses precisely. As shown below in Figure 4, the response rates dropped off after the first week with a spike in response to the May 12th e-mail reminder. There were smaller spikes in responses corresponding to the other reminder e-mails. A larger than normal spike occurred on May 22 when the data collection was extended by the hospital administration and again on the last day of the survey, May 30. One survey was filled out the day after the survey ended and was included in the total dataset. The population of potential respondents, described above, was approximately 3,500 people. A total of 1738 responses were collected, of which 41 were duplicates, leaving 1697 valid responses, or a 49 percent response rate.

Figure 4 – Daily Response Rates



To assess the possibility of non-response bias, the extrapolation method described by Armstrong and Overton (1977) was used to examine "waves" of respondents. The last "wave" of 184 respondents (those who responded after the May 26th e-mail was sent) were compared with the first 184 responders of the survey, the rationale being that the last wave (approximately 11 percent of responders) would not have participated at all without the additional stimulus of reminders, e-mails, and extensions. These responders would then be the most similar to non-respondents if non-response bias exists and they are significantly different from the first group of

responders.[7] The extrapolation was done by performing t-tests comparing the first wave respondents' construct scores with the last wave respondents' scores. All construct differences were insignificant with the exception of Risk-Impact ($p>0.05$) and Computer Self Efficacy ($p<0.01$), showing that those who responded later felt that they believed that the impact of cyber-incidents was lower, on average, than the earlier group, and had less confidence in their abilities to use computers to accomplish tasks. This is to be expected, as those who put off taking a mandatory on-line survey would be those with the least confidence in their abilities in working with a computer. Likewise, these individuals would be expected to have lower assessment of the impact of computer security because of their low computer self efficacy. I do not feel that these issues will have any effects on our results.

5.2 PRELIMINARY DATA ANALYSIS

In order to create viable results, it is necessary to validate the data to ensure that they are suitable for detailed analysis and inclusion in the research model. This includes re-coding reverse coded items, re-coding inconsistent responses, testing for and removing inconsistent and missing cases that could affect the results, and calculating descriptive statistics on responses.

[7] The first "wave" of responders totaled 629 participants over the first three days of the survey. The total to compare to the final "wave" was cut down to provide a parallel sample. Thus, the first 184 respondents were compared to the final 184 respondents rather than comparing unequally sized waves.

5.2.1 Recoding

There are two types of recoding that I performed on the data set. The first was the rather routine task of coding reverse coded items so they can be included in the larger scales. The following items were reverse coded in the survey and were subsequently recoded for analysis:

- Prec09
- Prec10
- Prec11
- Prec15
- Prec16
- Apathy04

5.2.1.1 Inconsistent Responses Requiring Recoding

The second recoding dealt with inconsistent responses to questions within the survey itself. Additional examination of the data showed that a number of people answered questions that were conditional on the "yes" answer in the previous question. (For example, if you answered "no" to the question "Has your system ever been infected with a virus?" then the question "If yes, to what degree did it impact you?" has no meaning.) These items were intended to show the actual experience of the individual (whether direct or indirect) and the impact on that individual if the person had the experience. To clean the data of these errors, items were recoded in the following way:

1. If the answer to the experience question was answered "no" then the impact question was recoded to show a "0" value.
2. If the answer to the experience question was answered "yes" then the impact question was left "as is" including those who left the question blank.
3. If the answer to the experience question was blank, then the impact question was re-coded to be blank if the answer was not already missing.

The following "impact" items required recoding in this dataset:

- Dir01IM
- Dir02IM
- Dir03IM
- Dir04IM
- Dir05IM
- Dir06IM
- Dir07IM
- Dir08IM
- Dir09IM
- Indr01IM
- Indr02IM
- Indr03IM
- Indr04IM
- Indr05IM
- Indr06IM
- Indr07IM
- Indr08IM
- Indr09IM

The statistics showing response frequencies for these items and the experience items are shown in Appendix F. Overall 21,776 responses were recoded as detailed below in Table 27.

Table 27 – Responses Recoded by Survey Item

Item	Number of Responses Recoded
Dir01IM	1,274
Dir02IM	1,627
Dir03IM	1,531
Dir04IM	1,548
Dir05IM	1,457
Dir06IM	1,380
Dir07IM	1,456
Dir08IM	1,429
Dir09IM	1,571
Indr01IM	704
Indr02IM	1,315
Indr03IM	1,045
Indr04IM	813
Indr05IM	908
Indr06IM	1,012
Indr07IM	826
Indr08IM	798
Indr09IM	1,082
Total	21,776

5.2.2 Inconsistent Respondents Requiring Dropping the Case

I used three procedures to identify subjects whose responses indicated "deviance" and were thus unsuitable for inclusion in our survey. Deviance was identified as either participants who failed to respond to a large number of questions, or those who did not provide consistent responses given the reverse coded items in the survey. Respondents who exhibited either of these characteristics were, likely, not paying complete attention when completing the survey, thus their responses are suspect and were removed from the response data.

The first step was to examine the data for cases with large amounts of missing data. The data set consisted of 1,697 individuals responding to 116 questions resulting in 196,852 total responses. Of these responses, 6,327 responses (3.2 percent) were missing. Missing demographic data (Computer Expertise, Shift, Employee Status, Education, Position, Ethnicity, Participation in the RNPride Program, or Participation in PMIs) comprised 141 (2 percent of the total missing) of those values. The majority of the remaining missing variables were distributed equally across the data; however, several cases had a disproportionate percentage of missing values. The mean number of missing responses per case was 3.74, or about 3 percent of the survey. A number of cases had many times in excess of that amount, with 20 cases having in approximately 40 percent or more missing, accounting for 1,259 instances of missing data or approximately 20 percent of the total missing data. These cases, shown below in Table 28, were clearly anomalous and were removed from the data set.

Table 28 – Deleted Cases Due to Missing Data

Case	# Missing	% Missing
116	116	100.00
954	103	88.79
320	102	87.93
41	78	67.24
86	68	58.62
373	64	55.17
416	55	47.41
1024	55	47.41
1127	55	47.41
199	54	46.55
266	54	46.55
533	54	46.55
1056	54	46.55
1694	53	45.69
31	52	44.83
935	50	43.10
1440	50	43.10
1213	49	42.24
42	47	40.52
162	46	39.66

Additional analysis of the missing data showed that some of those missing data points were likely due to questionnaire design. The risk variables were asked in a two-column format as shown in the sample below in Figure 5.

Figure 5 – Risk Variable Questionnaire Sample

	How Likely? *(answer below)*							**Impact to you if this occurred** *(answer below)*						
	Low Likelihood		Moderate Likelihood				High Likelihood	Low Impact		Moderate Impact				High Impact
A computer system corrupted by a virus or worm.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
A computer system taken over by a hacker.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
Account being used by someone else without their knowledge.	1	2	3	4	5	6	7	1	2	3	4	5	6	7

Of those who answered in the "How Likely" column on the left, 1,742 (28 percent of the total missing) responses were not answered in the "Impact" column. The cases with these missing values will not be removed form the dataset, but will not be included in the calculation for risk-impact.

Deviant cases are easily identifiable through the use of reverse coded items in the scales. By assessing the extent to which an individual scored reverse coded items in the same direction as those that were not, we are able to detect individuals who should be removed from the dataset. To identify individuals who may not have been taking the survey seriously, I identified those respondents who responded with the same answer throughout the survey (for example a respondent who answered "5" to all questions) for Likert-type questions and removed them from the data set. The logic behind this approach is that that even a minimal amount of attention to the survey would have resulted in at least one different answer. There were 25 cases which met these criteria:

- 55
- 174
- 276
- 331
- 344
- 397
- 523
- 598
- 599
- 716
- 835
- 846
- 900
- 967
- 974
- 979
- 988
- 1013
- 1028
- 1031
- 1067
- 1204
- 1263
- 1386
- 1536

These subjects answered all of questions with the same answer and have been removed from the dataset. With the removal of the 25 inconsistent cases along with the 20 cases for which there is insufficient data, 45 cases have been removed from the dataset.

5.2.3 Descriptive Statistics

Following the removal of the cases described above, descriptive statistics were calculated on the remaining 1,652 remaining data points. Table 29 provides descriptive statistics for each item on the final questionnaire shown in Appendix C.

Table 29 – Item Descriptive Statistics

Variable	Item	n	Minimum	Maximum	Mean	Standard Deviation	Skewness	Std. Error	Kurtosis	Std. Error	Survey Question #
Specifi-cation	Spec01	1648	1	7	5.19	1.46	-0.75	0.06	0.25	0.12	1
	Spec02	1643	1	7	4.70	1.55	-0.36	0.06	-0.45	0.12	2
	Spec03	1648	1	7	5.67	1.44	-1.16	0.06	1.03	0.12	3
	Spec04	1645	1	7	5.24	1.45	-0.70	0.06	0.03	0.12	4
Evaluation	Eval01	1645	1	7	4.27	1.61	-0.20	0.06	-0.50	0.12	5
	Eval02	1643	1	7	4.31	1.57	-0.25	0.06	-0.39	0.12	6
	Eval03	1646	1	7	4.36	1.64	-0.27	0.06	-0.58	0.12	7
	Eval04	1637	1	7	4.49	1.61	-0.35	0.06	-0.47	0.12	8
Reward	Rew01	1646	1	7	4.34	1.65	-0.34	0.06	-0.44	0.12	9
	Rew02	1644	1	7	3.73	1.62	0.00	0.06	-0.55	0.12	10
	Rew03	1639	1	7	2.92	1.69	0.45	0.06	-0.68	0.12	11
	Rew04	1640	1	7	3.26	1.68	0.16	0.06	-0.80	0.12	12
Punishment	Punish01	1641	1	7	5.24	1.46	-0.78	0.06	0.34	0.12	13
	Punish02	1643	1	7	5.05	1.46	-0.51	0.06	-0.09	0.12	14
	Punish03	1644	1	7	5.06	1.50	-0.60	0.06	-0.05	0.12	15
	Punish04	1640	1	7	5.24	1.50	-0.75	0.06	0.19	0.12	16
Mandatori ness	Mand01	1645	1	7	5.70	1.36	-1.14	0.06	1.21	0.12	17
	Mand02	1644	1	7	5.27	1.63	-0.84	0.06	0.07	0.12	18
	Mand03	1636	1	7	5.96	1.27	-1.56	0.06	2.81	0.12	19
	Mand04	1640	1	7	5.84	1.34	-1.28	0.06	1.48	0.12	20
Computer Self Efficacy	CSE1	1643	1	7	3.99	1.61	-0.09	0.06	-0.54	0.12	21
	CSE2	1648	1	7	3.51	1.56	0.10	0.06	-0.57	0.12	22
	CSE3	1646	1	7	4.18	1.59	-0.15	0.06	-0.55	0.12	23
	CSE4	1645	1	7	4.66	1.45	-0.33	0.06	-0.33	0.12	24
	CSE5	1647	1	7	5.36	1.37	-0.62	0.06	-0.11	0.12	25
	CSE6	1641	1	7	5.34	1.33	-0.61	0.06	0.00	0.12	26
	CSE7	1646	1	7	5.07	1.41	-0.50	0.06	-0.09	0.12	27
	CSE8	1641	1	7	4.60	1.53	-0.26	0.06	-0.48	0.12	28
	CSE9	1645	1	7	5.68	1.26	-0.81	0.06	0.19	0.12	29
	CSE10	1639	1	7	5.52	1.27	-0.81	0.06	0.44	0.12	30
Precautions Taken	Prec01	1649	1	7	5.80	1.20	-1.11	0.06	1.45	0.12	31
	Prec02	1645	1	7	5.07	1.45	-0.56	0.06	-0.02	0.12	32
	Prec03	1643	1	7	5.49	1.34	-0.70	0.06	0.03	0.12	33
	Prec04	1641	1	7	2.98	1.85	0.51	0.06	-0.81	0.12	34

Variable	Item	n	Minimum	Maximum	Mean	Standard Deviation	Skewness	Std. Error	Kurtosis	Std. Error	Survey Question #
	Prec05	1645	1	7	2.88	1.87	0.59	0.06	-0.76	0.12	35
	Prec06	1641	1	7	2.86	1.84	0.59	0.06	-0.73	0.12	36
	Prec07	1631	1	7	3.05	1.87	0.44	0.06	-0.89	0.12	37
	Prec08	1638	1	7	5.81	1.46	-1.41	0.06	1.59	0.12	38
	Prec09R	1651	1	7	6.75	0.92	-4.52	0.06	21.21	0.12	39
	Prec10R	1644	1	7	6.83	0.85	-5.59	0.06	31.90	0.12	40
	Prec11R	1643	1	7	6.05	1.60	-1.55	0.06	1.28	0.12	41
	Prec12	1642	1	7	5.80	1.62	-1.46	0.06	1.51	0.12	42
	Prec13	1644	1	7	5.64	1.54	-1.29	0.06	1.27	0.12	43
	Prec14	1639	1	7	5.37	1.62	-0.94	0.06	0.30	0.12	44
	Prec15R	1647	1	7	6.01	1.47	-1.49	0.06	1.54	0.12	45
	Prec16R	1647	1	7	6.62	1.11	-3.61	0.06	13.25	0.12	46
Risk – Likelihood	Risk01L	1616	1	7	3.31	1.76	0.38	0.06	-0.66	0.12	47a
	Risk02L	1617	1	7	2.84	1.67	0.71	0.06	-0.24	0.12	48a
	Risk03L	1612	1	7	3.08	1.71	0.52	0.06	-0.57	0.12	49a
	Risk04L	1612	1	7	3.50	1.85	0.28	0.06	-0.89	0.12	50a
	Risk05L	1616	1	7	3.35	1.81	0.40	0.06	-0.75	0.12	51a
	Risk06L	1605	1	7	3.64	1.75	0.14	0.06	-0.82	0.12	52a
	Risk07L	1606	1	7	2.95	1.86	0.65	0.06	-0.68	0.12	53a
	Risk08L	1606	1	7	3.16	1.85	0.51	0.06	-0.80	0.12	54a
	Risk09L	1602	1	7	2.69	1.80	0.89	0.06	-0.26	0.12	55a
Risk – Impact	Risk01IM	1442	1	7	5.70	1.61	-1.29	0.06	1.02	0.13	47b
	Risk02IM	1436	1	7	5.81	1.66	-1.53	0.07	1.56	0.13	48b
	Risk03IM	1427	1	7	5.81	1.65	-1.51	0.07	1.52	0.13	49b
	Risk04IM	1429	1	7	6.42	1.38	-2.78	0.07	7.22	0.13	50b
	Risk05IM	1433	1	7	5.95	1.61	-1.71	0.07	2.15	0.13	51b
	Risk06IM	1426	1	7	5.51	1.71	-1.06	0.07	0.30	0.13	52b
	Risk07IM	1416	1	7	5.59	1.79	-1.30	0.07	0.76	0.13	53b
	Risk08IM	1411	1	7	5.65	1.72	-1.34	0.07	0.96	0.13	54b
	Risk09IM	1406	1	7	5.90	1.65	-1.65	0.07	1.95	0.13	55b
Indirect Experience – Actual	Indr01L	1597	0	1	0.56	0.50	-0.26	0.06	-1.93	0.12	57a
	Indr02L	1595	0	1	0.19	0.39	1.59	0.06	0.52	0.12	58a
	Indr03L	1594	0	1	0.35	0.48	0.61	0.06	-1.63	0.12	59a
	Indr04L	1599	0	1	0.50	0.50	0.00	0.06	-2.00	0.12	60a
	Indr05L	1588	0	1	0.44	0.50	0.25	0.06	-1.94	0.12	61a
	Indr06L	1594	0	1	0.37	0.48	0.52	0.06	-1.73	0.12	62a
	Indr07L	1590	0	1	0.49	0.50	0.06	0.06	-2.00	0.12	63a

Variable	Item	n	Minimum	Maximum	Mean	Standard Deviation	Skewness	Std. Error	Kurtosis	Std. Error	Survey Question #
	Indr08L	1580	0	1	0.50	0.50	-0.01	0.06	-2.00	0.12	64a
	Indr09L	1590	0	1	0.33	0.47	0.71	0.06	-1.49	0.12	65a
Indirect Experience – Impact	Indr01IM	1578	0	7	3.26	3.06	0.02	0.06	-1.80	0.12	57b
	Indr02IM	1586	0	7	1.16	2.49	1.75	0.06	1.17	0.12	58b
	Indr03IM	1579	0	7	2.12	3.00	0.78	0.06	-1.29	0.12	59b
	Indr04IM	1574	0	7	3.20	3.35	0.14	0.06	-1.93	0.12	60b
	Indr05IM	1563	0	7	2.61	3.13	0.45	0.06	-1.69	0.12	61b
	Indr06IM	1574	0	7	2.13	2.93	0.75	0.06	-1.29	0.12	62b
	Indr07IM	1567	0	7	2.84	3.10	0.28	0.06	-1.78	0.12	63b
	Indr08IM	1555	0	7	2.95	3.13	0.22	0.06	-1.81	0.12	64b
	Indr09IM	1556	0	7	1.94	2.95	0.95	0.06	-1.00	0.12	65b
Direct Experience – Actual	Dir01L	1632	0	1	0.23	0.42	1.28	0.06	-0.36	0.12	66a
	Dir02L	1629	0	1	0.02	0.13	7.30	0.06	51.35	0.12	67a
	Dir03L	1625	0	1	0.07	0.26	3.28	0.06	8.77	0.12	68a
	Dir04L	1630	0	1	0.07	0.25	3.47	0.06	10.06	0.12	69a
	Dir05L	1623	0	1	0.12	0.32	2.38	0.06	3.65	0.12	70a
	Dir06L	1628	0	1	0.17	0.37	1.80	0.06	1.26	0.12	71a
	Dir07L	1619	0	1	0.11	0.32	2.42	0.06	3.85	0.12	72a
	Dir08L	1608	0	1	0.13	0.33	2.26	0.06	3.12	0.12	73a
	Dir09L	1614	0	1	0.04	0.20	4.64	0.06	19.56	0.12	74a
Direct Experience – Impact	Dir01IM	1620	0	7	1.28	2.49	1.56	0.06	0.64	0.12	66b
	Dir02IM	1622	0	7	0.07	0.66	9.38	0.06	89.58	0.12	67b
	Dir03IM	1618	0	7	0.41	1.53	3.66	0.06	11.79	0.12	68b
	Dir04IM	1623	0	7	0.39	1.54	3.83	0.06	12.94	0.12	69b
	Dir05IM	1607	0	7	0.65	1.93	2.72	0.06	5.61	0.12	70b
	Dir06IM	1614	0	7	0.86	2.09	2.17	0.06	3.02	0.12	71b
	Dir07IM	1606	0	7	0.60	1.81	2.85	0.06	6.51	0.12	72b
	Dir08IM	1596	0	7	0.67	1.91	2.66	0.06	5.39	0.12	73b
	Dir09IM	1603	0	7	0.21	1.17	5.40	0.06	27.50	0.12	74b
Apathy	Apathy01	1648	1	7	2.68	1.94	0.83	0.06	-0.55	0.12	78
	Apathy02	1649	1	7	1.76	1.60	2.31	0.06	4.25	0.12	79
	Apathy03	1649	1	7	4.45	1.71	-0.34	0.06	-0.51	0.12	80
	Apathy04R	1645	1	7	2.51	1.54	1.08	0.06	0.75	0.12	81
	Apathy05	1643	1	7	1.94	1.34	1.55	0.06	2.02	0.12	82
	Apathy06	1640	1	7	1.87	1.37	1.78	0.06	2.77	0.12	83

These results show that in every instance, the full range of possible response was recorded. Skewness ranged from -5.589 to 9.384, and kurtosis ranged from -2.003 to 89.576 showing definite non-normality in the results. Further examination shows that the severely non-normal data are some of the direct and indirect experience variables and the precautions variables which were expected to be non-normal as discussed in the results of the pilot data.

5.2.4 Dependent Variable

As discussed following the pilot test, the dependent variable "precautions taken" was deemed to be a multidimensional construct in the pilot study. Exploratory factor analysis using a minimum Eigenvalue of 1 with loadings less than 0.40 suppressed are shown in Table 30 below. These results confirm findings of multidimensionality as discussed above in the pilot study. The results show that there are five separate factors (named below) in the overall "precautions taken" construct:

- *General Precautions* (Prec01, Prec02, Prec03, Prec08). These items reflect general attitudes toward computer security and actions to protect individuals' systems.
- *System Updates* (Prec04, Prec05, Prec06, Prec07). These items address specific actions that can be taken to be sure that individuals' systems have the most up-to-date operating system software, virus software, etc. These items do not necessarily covary with each other.
- *Interactions-Others* (Prec09R, Prec10R, Prec11R). These items address specific behaviors by individuals that are not in keeping with good computer security policies. These behaviors do not necessarily covary with each other.

- *Interactions-Management* (Prec12, Prec13, Prec14). These items address specific actions that individuals should take when confronted with a security incident. These individual actions do not necessarily covary with each other.
- *Risky Behavior* (Prec15R, Prec16R). These items address potential individual behaviors that are considered risky by computer security standards (America Online & National Cyber Security Alliance, 2005; Boss et al., 2005; CERT Coordination Center, 2004a; National Cyber Security Alliance, 2005). These behaviors are not expected to covary with each other.

Table 30 – Dependent Variable Factors

		Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
Prec01	I pay attention to computer security during my daily routine.		0.835			
Prec02	I keep aware of the latest security threats so I can protect my system.		0.772			
Prec03	My system is as secure as I can make it.		0.818			
Prec04	I regularly download security patches for my operating system/computer programs.	0.917				
Prec05	I regularly download virus protection software updates.	0.963				
Prec06	I regularly update the anti-spyware software on my computer.	0.962				
Prec07	I update my e-mail spam filter on a regular basis.	0.873				
Prec08	I take precautions with my passwords (Protect them, regularly change them, use multiple passwords, etc.).		0.639			
Prec09R	I share my passwords with other people.				0.834	
Prec10R	I allow non-employees access to my computer.				0.816	
Prec11R	I allow other employees access to my computer.				0.678	
Prec12	I notify a manager or IS personnel if I suspect that my system has been infected by a virus.			0.846		
Prec13	I notify a manager if the system slows down to an unreasonable level.			0.865		
Prec14	I report suspicious e-mails to a supervisor or security personnel in the Information Systems department.			0.826		
Prec15R	I open attached executables from friends even if the message doesn't make particular sense.					0.841
Prec16R	I regularly download "unauthorized" software to install on my computer.					0.797

Analysis of the dependent variable can also theoretically be broken down into specific actions individuals can take (Items 4 to 16), and general, overall perceptions that individuals are protecting their systems (Items 1 to 3). While we could examine each of these dimensions within the context of this research, it is likely that individuals who consider any subset of the actions denoted above (items 4 to 16) as important – whether they covary or not – would tend to score responses to the "general" items similarly. Thus, individuals who take actions to update their systems, refrain from risky behaviors, and limit access to their systems to authorized individuals would likely score their answers to items 1 to 3 higher than those who do not. Additionally, given the potential complexity of the interrelationships between each of the sub-constructs, including them individually in the current model would produce a less than parsimonious model from which to draw conclusions. As a result, I have chosen to focus the remainder of this study using only the "general" precautions as the dependent variable (Prec01, Prec02, Prec03, and Prec08) and plan to address the interrelationships in further research. This construct is reflective and shows a general awareness of security and the intention to take precautions.[8]

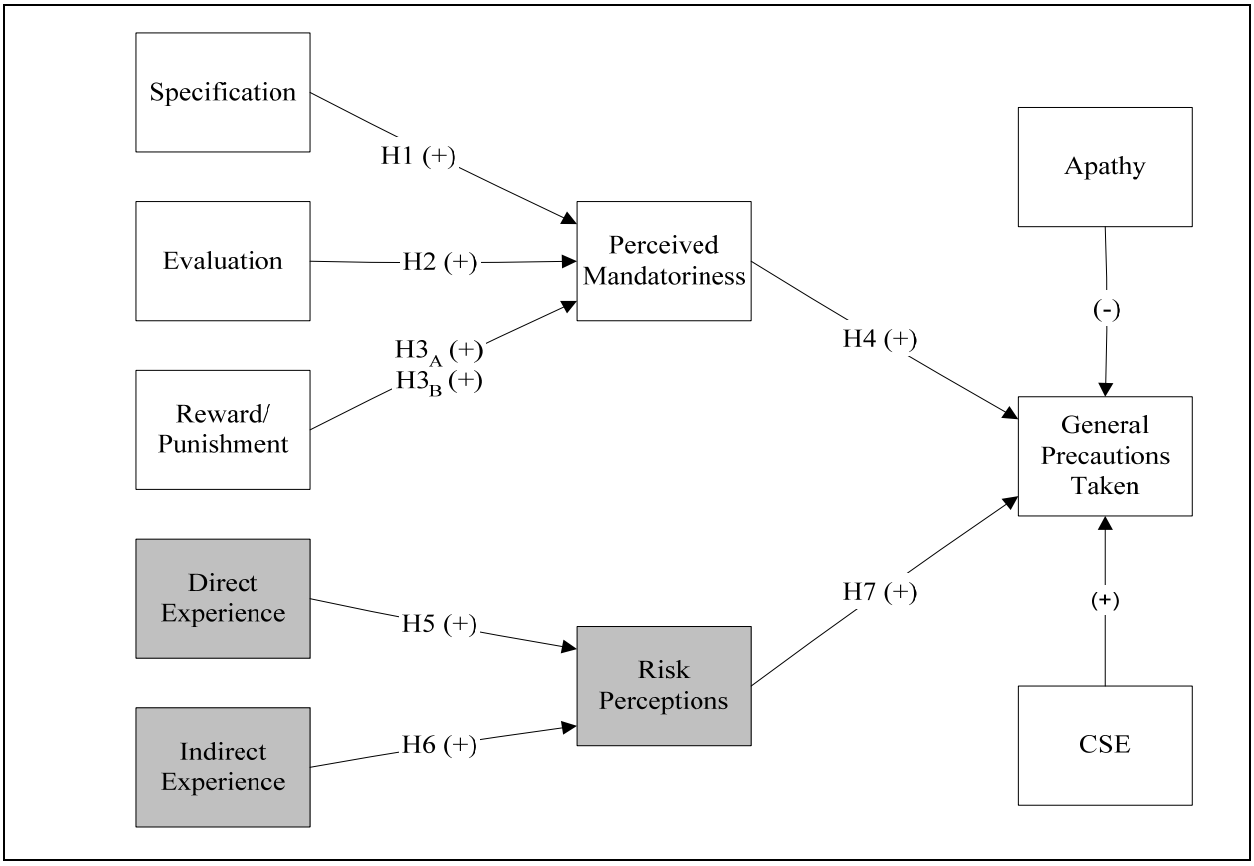
[8] While it could be argued that precautions regarding passwords (Prec08) are markedly different from the other items in the construct, public and private cautions regarding passwords and the prevalence of media regarding this topic (a Google search produced 34.3 million hits on "password") shows that password security is viewed as a "general" precaution and is appropriately included in the General Precautions construct in this study.

5.3 CONSTRUCT RELIABILITY AND VALIDITY

The following section discusses the results of the analysis to determine the adequacy of the measurement model. Specifically, it reports on the tests for internal consistency, item loadings, convergent validity, and discriminant validity. I use analytical techniques similar to those used in testing the pilot data with additional tests taken from existing literature. Upon demonstration of the adequacy of the measurement model, the data will be ready to test the hypotheses.

The measurement model is composed of eight independent variables, two control variables, and one dependent variable. As discussed in the results from the pilot test, the independent variables are comprised of five reflective constructs (specification, evaluation, reward, punishment, and mandatoriness) and three formative constructs (direct experience, indirect experience, and risk.). The dependent variable, general precautions taken, is a reflective construct. The control variables, CSE and apathy, are also reflective constructs. Since items in formative constructs are not expected to covary with other items (Loch, Straub, & Kamel, 2003), the reflective and formative reliability and validity will be presented separately using different methods recommend in extant literature (W. W. Chin, 1998a, 1998b; Gray & Meister, 2004; Hulland, 1999). The reflective portion of the model to be tested is shown below in Figure 6 with the formative constructs grayed out.

Figure 6 – Reflective Portion of the Research Model



5.3.1 Reflective Construct Reliability

The reliability tests used in the PLS analysis of the pilot test will also be performed here with a few additions. Specifically, Chronbach's Alpha (Nunnally, 1978; Nunnally & Bernstein, 1994) and Internal Consistency (Fornell & Larcker, 1981), and examination of item loadings (Carmines & Zeller, 1979). The results for the reflective measures are shown below in Table 31. Items with potential issues (low Chronbach's Alpha, low internal consistency score, or loadings lower than 0.70) are candidates for deletion and are indicated in bold-face type.

Table 31 – Reliability Analysis

Variable	Loading	Residual Variance	Internal Consistency	Chronbach's Alpha
Spec01	0.83	0.31		
Spec02	0.75	0.44		
Spec03	0.88	0.23		
Spec04	0.89	0.21		
Specification			0.90	0.86
Eval01	0.93	0.13		
Eval02	0.95	0.10		
Eval03	0.95	0.10		
Eval04	0.95	0.10		
Evaluation			0.97	0.96
Rew01	0.93	0.14		
Rew02	0.71	0.50		
Rew03	**0.53**	0.71		
Rew04	**0.56**	0.69		
Reward			0.79	0.78
Pun01	0.86	0.26		
Pun02	0.84	0.29		
Pun04	0.85	0.28		
Pun03	0.86	0.26		
Punishment			0.91	0.88
Mand01	0.90	0.19		
Mand02	0.82	0.34		
Mand03	0.90	0.19		
Mand04	0.88	0.23		
Mandatoriness			0.93	0.89
Prec01	0.87	0.24		
Prec02	0.82	0.33		
Prec03	0.84	0.30		
Prec06	**0.65**	0.58		
General Precautions			0.87	0.80
Apathy01	**0.36**	0.87		
Apathy02	**0.36**	0.87		
Apathy03	**-0.02**	1.00		

Variable	Loading	Residual Variance	Internal Consistency	Chronbach's Alpha
Apathy04R	**0.70**	0.51		
Apathy05	0.81	0.34		
Apathy06	0.80	0.36		
Apathy			**0.70**	**0.53**
CSE01	0.71	0.50		
CSE02	0.71	0.49		
CSE03	0.79	0.38		
CSE04	0.84	0.30		
CSE05	0.84	0.29		
CSE06	0.86	0.26		
CSE07	0.82	0.33		
CSE08	0.79	0.38		
CSE09	0.77	0.41		
CSE10	0.80	0.36		
CSE			0.94	0.93

All scales, with one exception, demonstrated an internal consistency and alpha scores above 0.70, so all are acceptable from a reliability perspective. The exception, apathy, with an internal consistency of 0.70 and a Chronbach's Alpha of 0.53, is below the generally accepted level so items were dropped to improve its reliability. Through dropping the lowest loading items in the Apathy construct and re-running the analysis iteratively, Apathy items 1, 2, and 3 were dropped, which improved the internal consistency score from 0.70 to 0.83 and the Chronbach's Alpha from 0.53 to 0.697. Likewise, the loading for Apathy04R increased from 0.70 to 0.75. The revised apathy scale is shown below in Table 32. While the Chronbach's Alpha score is technically a little below the recommended cutoff, I will hold off on making additional changes until after doing a factor analysis in the validity section below.

Table 32 – Revised Apathy Reliability Measure

Variable	Loading	Residual Variance	Internal Consistency	Chronbach's Alpha
Apathy04R	0.75	0.44		
Apathy05	0.82	0.33		
Apathy06	0.81	0.35		
Apathy			0.83	0.70

Additionally, three items have item loadings from PLS below the 0.70 cutoff established in the literature:

- Rew03 (0.53)
- Rew04 (0.56)
- Prec06 (0.65)

These items can either be deleted or we can accept that the constructs have internal consistencies that are good enough to continue. There are arguments that items with internal consistencies as low as 0.50 are acceptable in the early stages of scale development (W. W. Chin, 1998a), but there are also strong arguments for having the cleanest scales possible, especially the dependent variable in the study. Consequently, I will retain all of the items as they all meet the 0.50 guideline, and pending the results of the validity tests below.

As a final measure of construct reliability, I tested the significance of the remaining reflective items on their respective constructs using a bootstrap analysis with 500 sub-samples (W. W. Chin, 1998b). The results from this analysis are shown below in Table 33, which confirms that all items load significantly at the $p<0.01$ level or below on their intended constructs.

Table 33 – Significance of Reflective Item Loadings

Construct	Item	Entire Sample Estimate	Mean of Subsamples	Standard Error	t-Statistic
Specification	Spec01	0.83	0.83	0.01	73.75**
	Spec02	0.75	0.75	0.02	47.21**
	Spec03	0.88	0.88	0.01	108.43**
	Spec04	0.89	0.89	0.01	124.39**
Evaluation	Eval01	0.93	0.93	0.01	152.08**
	Eval02	0.95	0.95	0.01	181.63**
	Eval03	0.95	0.95	0.00	221.75**
	Eval04	0.95	0.95	0.00	265.75**
Reward	Rew01	0.93	0.93	0.02	46.85**
	Rew02	0.71	0.70	0.04	18.31**
	Rew03	0.53	0.52	0.07	7.61**
	Rew04	0.56	0.55	0.07	8.50**
Punishment	Punish01	0.86	0.86	0.01	98.19**
	Punish02	0.84	0.84	0.01	79.16**
	Punish03	0.85	0.85	0.01	75.87**
	Punish04	0.86	0.86	0.01	77.76**
Mandatoriness	Mand01	0.90	0.90	0.01	122.40**
	Mand02	0.82	0.82	0.01	63.55**
	Mand03	0.90	0.90	0.01	125.55**
	Mand04	0.88	0.88	0.01	103.22**
General Precautions	Prec01	0.87	0.87	0.01	118.66**
	Prec02	0.82	0.82	0.01	71.18**
	Prec03	0.84	0.84	0.01	74.80**
	Prec08	0.65	0.65	0.02	31.26**
CSE	CSE1	0.71	0.71	0.02	40.18**
	CSE2	0.71	0.71	0.02	39.41**
	CSE3	0.79	0.78	0.01	58.72**
	CSE4	0.84	0.84	0.01	78.47**
	CSE5	0.84	0.84	0.01	86.40**
	CSE6	0.86	0.86	0.01	94.18**
	CSE7	0.82	0.82	0.01	78.65**
	CSE8	0.79	0.79	0.01	67.81**
	CSE9	0.77	0.77	0.01	52.40**
	CSE10	0.78	0.80	0.01	63.52**
Apathy	Apathy04R	0.75	0.75	0.02	32.99**
	Apathy05	0.82	0.82	0.02	47.46**
	Apathy06	0.81	0.81	0.02	45.97**

** $p < 0.01$

5.3.2 Reflective Item Construct Validity

Initial assessment of convergent and discriminant item validity were conducted using factor analysis with Varimax rotation. This test ensures that items load cleanly on the constructs to which they are intended to load and do not cross load to other constructs providing an initial level of item discriminant validity (Straub, Boudreau, & Gefen, 2004). The results of the initial factor analysis using Varimax rotation with Kaiser Normalization using Eigenvalues greater than 1 are shown below in Table 34 (loadings less than 0.40 suppressed).

Table 34– Initial Reflective Construct Factor Loadings

	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8
Spec01					0.75			
Spec02					0.65			
Spec03					0.76			
Spec04					0.75			
Eval01			0.84					
Eval02			0.87					
Eval03			0.87					
Eval04			0.85					
Rew01		0.52						
Rew02							0.68	
Rew03							0.89	
Rew04							0.88	
Punish01		0.76						
Punish02		0.75						
Punish03		0.75						
Punish04		0.78						
Mand01		0.61		0.44				
Mand02		0.47		0.51				
Mand03		0.63						
Mand04		0.58		0.41				
Prec01				0.75				
Prec02				0.73				
Prec03				0.75				
Prec08				0.57				
CSE1						0.81		
CSE2						0.84		
CSE3	0.52					0.69		
CSE4	0.67					0.53		
CSE5	0.80							
CSE6	0.89							
CSE7	0.81							
CSE8	0.69							
CSE9	0.88							
CSE10	0.84							
Apathy04R								0.52
Apathy05								0.87
Apathy06								0.85

The analysis shows that items from the mandatoriness, punishment, reward, and general precautions are cross loading on several of the factors identified. Additionally, CSE is loading on two different factors.

To address these issues, I reviewed the questions relating to the central portion of my model (the non-control items) for theoretical reasons for the poor loadings. Item Rew01, which loads with the mandatoriness and punishment items, states the following:

> Rew01 My pay raises and/or promotions depend on whether I follow documented security policies and procedures.

Theoretically, this could be viewed as a "punishment" in that it relates to individuals receiving (or implicitly not receiving) promotions or raises based on the level of compliance. Due to the ambiguity of the item, it should be dropped. Additionally, item Mand02, loads with the precautions taken items. The text of the item is as follows:

> Mand02 It is expected that I will take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.).

While this question does address things that are "expected," it also addresses precaution taking activities. As with the Rew01 question, due to its ambiguity, the question it will be dropped from the remaining analysis.

To address the remaining cross-loading issues in the control variable (CSE), items were dropped one at a time and the factor analysis was re-run and examined for additional cross-loading items.[9] As a result of this iterative analysis, the following items were dropped:

- CSE1 (loaded on 2 factors)
- CSE2 (loaded on 2 factors)
- CSE3 (loaded on 2 factors)

---

[9] Since CSE is not one of the main "theory" component variables in my model but is a control variable, no effort was made to examine theoretical reasons for dropping items.

This coupled with dropping Rew01 and Mand02, results in the items loading cleanly over seven constructs as shown in Table 35.

Table 35 – Final Reflective Construct Factor Loadings

	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
Spec01					0.75		
Spec02					0.67		
Spec03					0.75		
Spec04					0.74		
Eval01			0.85				
Eval02			0.88				
Eval03			0.88				
Eval04			0.86				
Rew02						0.70	
Rew03						0.89	
Rew04						0.88	
Punish01		0.75					
Punish02		0.72					
Punish03		0.75					
Punish04		0.79					
Mand01		0.67					
Mand03		0.70					
Mand04		0.65					
Prec01				0.74			
Prec02				0.74			
Prec03				0.77			
Prec08				0.60			
CSE4	0.80						
CSE5	0.85						
CSE6	0.90						
CSE7	0.84						
CSE8	0.77						
CSE9	0.82						
CSE10	0.81						
Apathy04R							0.51
Apathy05							0.88
Apathy06							0.86

An interesting result of this analysis shows that respondents were unable to differentiate between punishment and mandatoriness in this study. As was noted in Section 2.3.1, mandatory controls are difficult to cognitively differentiate from punishment. Of specification, evaluation, reward, and punishment, the first three (specification, evaluation, and reward) are consistent with Kirsch (2004) and Eisenhardt (1988) while punishment is not typically addressed in this literature. This leaves me with the option to either discard punishment completely from the study or to add the punishment items to the mandatoriness construct introduced in this research. I have chosen to combine the punishment and mandatoriness items together to create a single mandatoriness construct consisting of Mand01, Mand03, Mand04, Punish01 (Mand05), Punish02 (Mand06), Punish03 (Mand07), and Punish04 (Mand08).

Item discriminant validity is tested by examining the correlation coefficients of each item loadings with the construct loadings. The items should correlate highly (and hopefully significantly) with their intended construct, but not as highly with unintended constructs. Acceptable discriminant validity is shown when the correlations with their intended construct exceed their correlations with all other constructs. As shown below in Table 36, this condition holds for all items (item correlations relating to the intended construct are in bold) suggesting that the scales have a high degree of discriminant validity. Additionally, all items correlated significantly with their intended construct.

Table 36 – Item Discriminant Validity

	Specification	Evaluation	Reward	Mandatoriness	Precautions	CSE	Apathy
Spec01	**0.81**	0.40	0.14	0.54	0.32	0.26	-0.21
Spec02	**0.68**	0.48	0.26	0.44	0.30	0.14	-0.14
Spec03	**0.85**	0.48	0.15	0.63	0.31	0.27	-0.17
Spec04	**0.80**	0.51	0.22	0.56	0.33	0.22	-0.18
Eval01	0.50	**0.87**	0.40	0.47	0.30	0.14	-0.16
Eval02	0.47	**0.85**	0.38	0.46	0.29	0.14	-0.14
Eval03	0.49	**0.90**	0.44	0.49	0.31	0.14	-0.15
Eval04	0.46	**0.78**	0.37	0.47	0.31	0.15	-0.16
Rew02	0.21	0.40	**0.87**	0.31	0.16	0.08	-0.03
Rew03	0.12	0.29	**0.70**	0.17	0.08	0.06	-0.06
Rew04	0.14	0.28	**0.73**	0.19	0.10	0.06	-0.04
Mand01	0.54	0.42	0.25	**0.77**	0.39	0.22	-0.21
Mand03	0.44	0.29	0.20	**0.63**	0.29	0.19	-0.17
Mand04	0.47	0.33	0.24	**0.66**	0.31	0.18	-0.20
Mand05	0.51	0.43	0.33	**0.71**	0.33	0.19	-0.18
Mand06	0.49	0.48	0.38	**0.72**	0.32	0.21	-0.21
Mand07	0.48	0.44	0.33	**0.73**	0.31	0.18	-0.17
Mand08	0.45	0.38	0.29	**0.69**	0.31	0.17	-0.18
Prec01	0.35	0.28	0.10	0.45	**0.86**	0.20	-0.33
Prec02	0.28	0.26	0.18	0.32	**0.74**	0.18	-0.29
Prec03	0.28	0.25	0.11	0.33	**0.72**	0.18	-0.27
Prec08	0.19	0.16	0.07	0.23	**0.53**	0.13	-0.19
CSE4	0.20	0.12	0.08	0.17	0.16	**0.75**	-0.07
CSE5	0.25	0.17	0.08	0.25	0.20	**0.84**	-0.09
CSE6	0.23	0.13	0.08	0.21	0.17	**0.76**	-0.08
CSE7	0.22	0.15	0.08	0.20	0.17	**0.82**	-0.06
CSE8	0.17	0.14	0.12	0.13	0.16	**0.69**	-0.06
CSE9	0.25	0.15	0.07	0.27	0.18	**0.78**	-0.10
CSE10	0.24	0.17	0.05	0.27	0.20	**0.71**	-0.12
Apathy04R	-0.22	-0.15	-0.01	-0.24	-0.31	-0.12	**0.70**
Apathy05	-0.15	-0.12	-0.02	-0.16	-0.25	-0.05	**0.73**
Apathy06	-0.12	-0.11	-0.06	-0.16	-0.25	-0.06	**0.67**

A second reliability analysis was performed to re-check the reliability of the scales that grouped punishment and mandatoriness and removed the dropped items. Table 37 provides the relevant reliability statistics for each item (the loadings and residual variance) and for each scale (internal consistency and Chronbach's alpha) after the problematic items were removed and Table 38 shows the revised significance levels of reflected items with their construct.

Table 37 – Second Reliability Analysis

Variable	Loading	Residual Variance	Internal Consistency	Chronbach's Alpha
Spec01	0.83	0.30		
Spec02	0.75	0.44		
Spec03	0.88	0.23		
Spec04	0.89	0.21		
Specification			0.90	0.86
Eval01	0.93	0.13		
Eval02	0.95	0.10		
Eval03	0.95	0.10		
Eval04	0.95	0.10		
Evaluation			0.97	0.96
Rew02	0.91	0.16		
Rew03	0.75	0.43		
Rew04	0.79	0.38		
Reward			0.86	0.81
Mand01	0.84	0.29		
Mand03	0.83	0.30		
Mand04	0.80	0.36		
Mand05	0.80	0.35		
Mand06	0.77	0.40		
Mand07	0.81	0.34		
Mand08	0.77	0.41		
Mandatoriness			0.93	0.91
Prec01	0.87	0.24		
Prec02	0.81	0.34		
Prec03	0.84	0.30		
Prec08	0.66	0.57		
General Precautions			0.87	0.80
Apathy04R	0.75	0.44		
Apathy05	0.82	0.33		
Apathy06	0.81	0.35		
Apathy			0.83	0.70
CSE04	0.79	0.37		
CSE05	0.86	0.26		
CSE06	0.90	0.19		
CSE07	0.85	0.28		
CSE08	0.77	0.41		
CSE09	0.85	0.29		

Variable	Loading	Residual Variance	Internal Consistency	Chronbach's Alpha
CSE10	0.85	0.28		
CSE			0.94	0.93

Table 38 – Second Check of Significance of Reflective Item Loadings

Construct	Item	Entire Sample Estimate	Mean of Subsamples	Standard Error	t-Statistic
Specification	Spec01	0.83	0.83	0.01	75.62**
	Spec02	0.75	0.75	0.02	49.77**
	Spec03	0.88	0.88	0.01	109.22**
	Spec04	0.89	0.89	0.01	128.08**
Evaluation	Eval01	0.93	0.93	0.01	156.95**
	Eval02	0.95	0.95	0.01	180.27**
	Eval03	0.95	0.95	0.00	234.28**
	Eval04	0.95	0.95	0.00	256.98**
Reward	Rew02	0.91	0.92	0.02	41.47**
	Rew03	0.75	0.75	0.04	17.80**
	Rew04	0.79	0.78	0.04	21.31**
Mandatoriness	Mand01	0.84	0.84	0.01	82.48**
	Mand03	0.83	0.83	0.01	79.76**
	Mand04	0.80	0.80	0.01	60.26**
	Mand05	0.80	0.80	0.01	65.98**
	Mand06	0.77	0.77	0.01	53.84**
	Mand07	0.77	0.77	0.01	51.73**
	Mand08	0.81	0.81	0.01	62.02**
General Precautions	Prec01	0.87	0.87	0.01	110.46**
	Prec02	0.81	0.81	0.01	64.48**
	Prec03	0.84	0.84	0.01	78.23**
	Prec08	0.66	0.65	0.02	32.97**
CSE	CSE4	0.79	0.79	0.01	62.31**
	CSE5	0.86	0.86	0.01	96.19**
	CSE6	0.90	0.90	0.01	129.26**
	CSE7	0.85	0.85	0.01	84.26**
	CSE8	0.77	0.77	0.01	62.77**
	CSE9	0.84	0.85	0.01	85.27**
	CSE10	0.85	0.85	0.01	86.01**
Apathy	Apathy04R	0.75	0.74	0.02	31.78**
	Apathy05	0.82	0.82	0.02	46.66**
	Apathy06	0.81	0.81	0.02	48.63**

** $p < 0.01$

This analysis indicates that the scales used in this research are reliable and that the issues noted in the original reliability tests are resolved.

Convergent validity is demonstrated when the average variance extracted (AVE) by a construct's items is at least 0.50 (W. W. Chin & Gopal, 1995). AVE greater than 0.50 shows that the variance explained by the construct is greater than the variance explained by measurement error. An examination of Table 39 below shows that all constructs meet this criterion. Discriminant validity is assessed by comparing the correlations between two constructs with the square root of AVE of each construct. Correlations between two constructs that are greater than the square root of AVE are indicative of poor discriminant validity between the constructs involved. Table 40 shows that the square root of AVE scores (in bold along the diagonal) is larger than the correlations between any two constructs demonstrating discriminant validity of the scales.

Table 39 – Construct Convergent Validity

Variable	Average Variance Extracted	Square Root of AVE
Specification	0.70	0.84
Evaluation	0.89	0.95
Reward	0.68	0.82
Mandatoriness	0.65	0.81
General Precautions	0.64	0.80
Apathy	0.63	0.79
CSE	0.70	0.84

Table 40 – Construct Discriminant Validity

	Specification	Evaluation	Reward	Mandatoriness	Precautions	CSE	Apathy
Specification	**0.84**						
Evaluation	0.52	**0.95**					
Reward	0.13	0.38	**0.82**				
Mandatoriness	0.66	0.53	0.18	**0.81**			
Precautions	0.47	0.40	0.16	0.54	**0.80**		
CSE	0.25	0.13	0.06	0.24	0.31	**0.84**	
Apathy	-0.26	-0.20	-0.05	-0.31	-0.43	-0.13	**0.79**

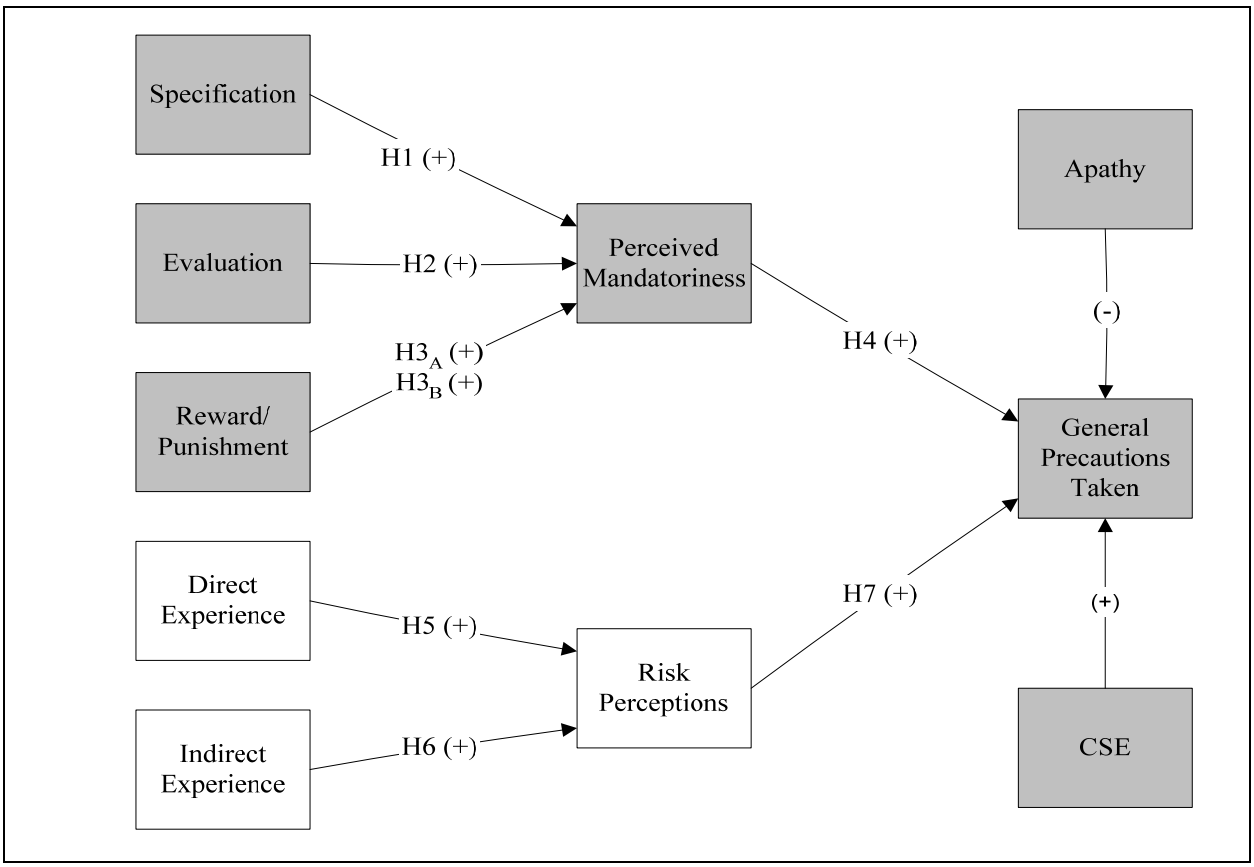
This section has shown convergent and discriminant validity of the measurement model's reflective constructs. Likewise the model's reflective constructs show strong reliability after items were dropped to improve the validity of the constructs. The next step is to examine the reliability and validity of the model's formative constructs.

5.3.3 Formative Construct Reliability and Validity

In general, reliability and validity are not meaningful concepts when applied to formative constructs (W. W. Chin, 1998a; Gray & Meister, 2004) because there is no assumption that formative items of the construct will covary (Bollen & Lennox, 1991; W. W. Chin, 1998b; Hulland, 1999). This results from formative constructs being defined by, rather than reflective of, the items that make up the construct. Examinations of correlations or internal consistency measures for formative constructs therefore are not useful in judging the reliability or validity of

the construct itself.[10] (The formative constructs are shown in Figure 7 below with the reflective portions of the model grayed out.)

Figure 7 – Formative Portion of the Research Model



On the other hand, some measure of reliability and validity should be examined as part of the research process. One important reliability factor in formative constructs is that the construct have an adequate number of indicators to properly "form" the construct (Bollen & Lennox, 1991; Venaik, Midgley, & Devinney, 2005). With nine indicators each for direct experience, indirect experience, and risk, these items fit that criterion. Likewise, the items have content validity as

[10] Some authors (Loch et al., 2003) have constructed a test for convergent and discriminant validity which examines inter-item and between-item correlations of items multiplied by their weight and summed into an overall composite score. This analysis can be seen in 0.

they were taken from extant research and practitioner literature and reviewed by both academic and practitioners as part of the scale building process (Straub et al., 2004).

The weights from the PLS analysis for the items in each of the formative constructs are shown below in Table 41. Weights generally tell how important an item is in forming each construct (Gray & Meister, 2004; Hulland, 1999), but cannot be relied on to help determine the necessity of any individual item in the construct itself as obtaining a "census" of items is of primary importance in the creation of formative constructs (Hulland, 1999).

Table 41 – Formative Item Weights

Items	Weight
Direct Experience	
Dir01	0.20
Dir02	-0.40
Dir03	0.32
Dir04	0.11
Dir05	0.42
Dir06	0.35
Dir07	0.03
Dir08	0.05
Dir09	0.08
Indirect Experience	
Indr01	0.37
Indr02	-0.22
Indr03	0.14
Indr04	0.18
Indr05	0.09
Indr06	0.43
Indr07	-0.27
Indr08	0.47
Indr09	-0.02
Risk	
Risk01	0.01
Risk02	-0.34
Risk03	0.53
Risk04	0.28
Risk05	0.11
Risk06	0.37
Risk07	0.12
Risk08	0.21
Risk09	-0.16

Overall, examination of the weights of the items shows that some items are more important than others in forming the constructs of direct experience, indirect experience, and risk. Further examination of the loadings shows that items that are important in forming the direct experience construct are not necessarily items that are important in forming either of the

other constructs, or vice versa. One issue that is apparent when examining the weights is that the weights of Dir02, Indr02, and Risk02 are very large (comparatively) and negative and could have an effect on the analysis. The question that applies to these items deals with a system being taken over by a hacker (direct experience, indirect experience, or feeling that one is at risk). While this experience does contribute to the overall set of constructs, due to the fact that often individuals are unaware of their system being taken over by a hacker, in addition to the low weight, I have decided to drop this item from all three constructs.

Subsequent to dropping items Dir02, Indr02, and Risk02, the item weights for the formative constructs are shown in Table 42.

Table 42 – Revised Formative Item Weights

Items	Weight
Direct Experience	
Dir01	0.16
Dir03	0.25
Dir04	0.06
Dir05	0.48
Dir06	0.39
Dir07	0.01
Dir08	0.02
Dir09	-0.02
Indirect Experience	
Indr01	0.31
Indr03	0.09
Indr04	0.14
Indr05	0.09
Indr06	0.48
Indr07	-0.29
Indr08	0.45
Indr09	-0.01
Risk	
Risk01	-0.17
Risk03	0.42
Risk04	0.22
Risk05	0.16
Risk06	0.43
Risk07	0.08
Risk08	0.22
Risk09	-0.21

While dropping the items does not eliminate all of the negative weights in the constructs, none of the constructs now has items whose negative weights rival the positive weights. Further, as PLS evaluates the entire model the remaining negative weights may be an artifact of the analysis technique compensating for the pattern of responses. Given this analysis and the parallelism that

exists between the constructs and items pertaining to risk, direct experience, and indirect experience, all of the remaining items will be retained for the measurement model.[11]

5.3.4 Construct Characteristics

Following the removal of the items described above, descriptive statistics were calculated for each of the constructs in their final state. Table 43 shows the descriptive statistics for each of the constructs used in the hypothesis tests.

Table 43 – Final Construct Characteristics

Construct	n	Minimum	Maximum	Mean	Standard Deviation	Skewness	Std. Error	Kurtosis	Std. Error
Specification	1650	1	7	5.20	1.24	-0.73	0.06	0.42	0.12
Evaluation	1649	1	7	4.36	1.52	-0.29	0.06	-0.38	0.12
Reward	1648	1	7	3.30	1.42	0.17	0.06	-0.47	0.12
Mandatoriness	1649	1	7	5.44	1.14	-0.95	0.06	1.32	0.12
Direct Experience	1637	0	1	0.12	0.21	2.09	0.06	4.13	0.12
Indirect Experience	1612	0	1	0.44	0.37	0.14	0.06	-1.44	0.12
Risk	1451	1	49	19.48	10.15	0.62	0.06	0.07	0.13
General Precautions Taken	1650	1	7	5.54	1.08	-0.68	0.06	0.24	0.12
Computer Self Efficacy	1649	1	7	5.17	1.15	-0.55	0.06	0.07	0.12
Apathy	1651	1	7	2.11	1.12	0.97	0.06	0.51	0.12

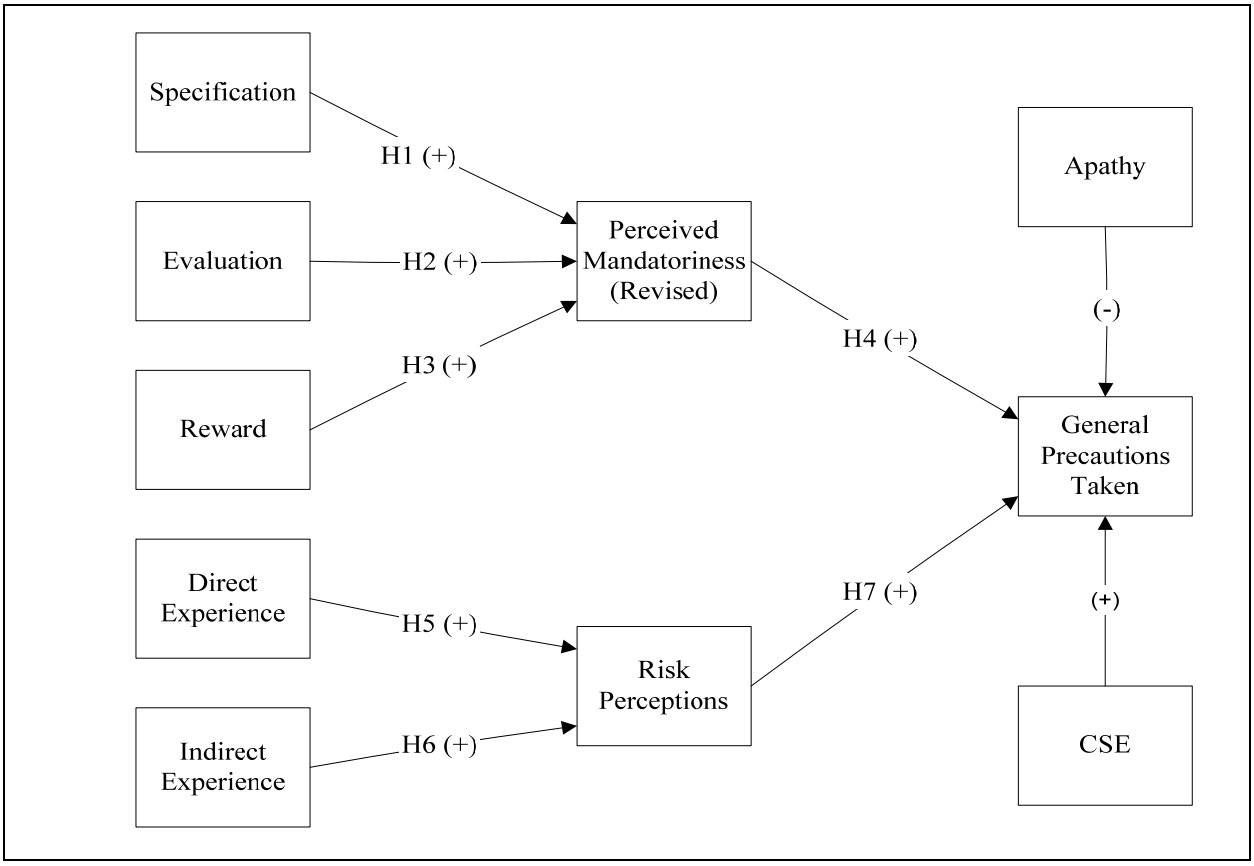
[11] There is concern that large negative weights assigned to the items by the PLS-Graph program adversely affect the results of the model. After removing the largest of the negative weights as described here in the text, an analysis was run removing all of the items with negative weights. The outcome of this analysis did not result either in any change of significance levels or in large changes in either β coefficient or change in R^2.

These results show that in every instance, the full range of possible response was recorded. Skewness ranged from -0.95 to 2.09, and kurtosis ranged from -1.44 to 4.13 showing close to normal results, with the abnormalities occurring in the direct and indirect experience measures which were measured on a binary yes/no basis.

5.4 HYPOTHESIS TESTING

With the reliability and validity of the measurement model now confirmed, the focus shifts to assessing the overall structural model and the linkages within the structural model. The revised theoretical model hypotheses, shown below in Figure 8, were tested using the PLS path modeling technique for assessing the explanatory and predictive power of the proposed model. The revised model drops Hypothesis 3_B and combines the punishment items with the mandatoriness items to create the mandatoriness construct discussed in the previous section.

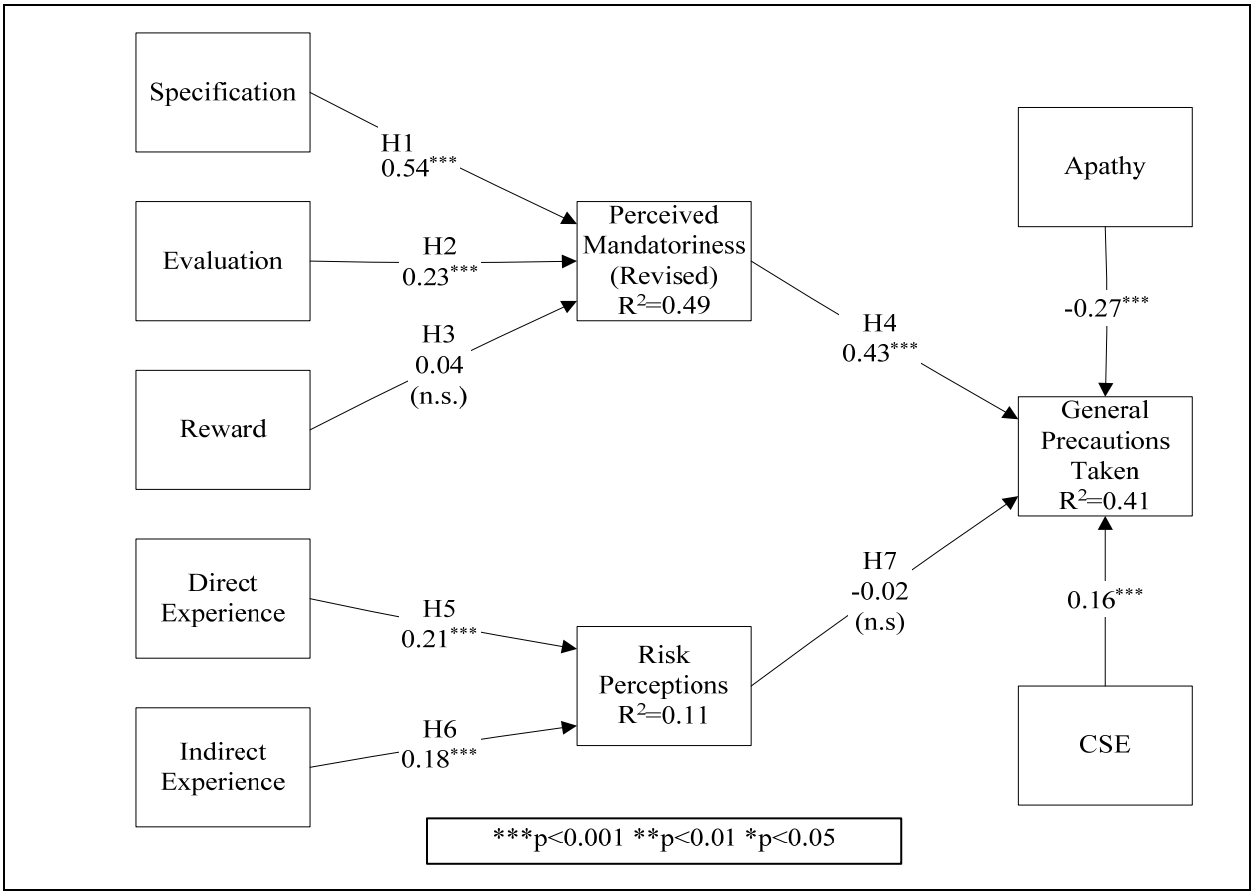
Figure 8 – Revised Theoretical Model



5.4.1 PLS Analysis

As discussed in Chapter 4 the research hypotheses were tested by examining the size and significance of structural paths in the PLS analysis (Wold, 1982). The percentage of variance is shown below in Figure 9, with 49 percent of the variance being explained in the relationships between the control elements and mandatoriness, 11 percent of the variance in the relationships between experience and risk, and 41 percent of the variance being explained by the overall model in predicting precautions taken.

Figure 9 – Path Coefficients and Explanatory Power of the Measurement Model



All but one of the proposed hypotheses were supported by the theoretical model. Specification significantly influences perceptions of mandatoriness (β=0.54, p<.001), as proposed in Hypothesis 1. Evaluation significantly influences mandatoriness (β=0.23, p<.001), as proposed in Hypothesis 2. Mandatoriness also significantly influences the dependent variable, precautions taken (β=0.43, p<.001), as predicted in Hypothesis 4. On the risk side of the model, we see that direct experience significantly influences perceptions of risk (β=0.21, p<.001) as proposed in Hypothesis 5. Finally, indirect experience significantly influences risk perceptions (β=0.18, p<.001) as predicted in Hypothesis 6. Reward does not significantly influence mandatoriness as proposed in Hypothesis 3; Hypothesis 7, the influence of risk on the dependent variable, was also not found to be significant.

5.4.2 Common Method Bias

A common problem in social science research is common method bias. Common method bias is defined as the "variance (in a study) that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al., 2003, p. 897) and is estimated to have affected a significant number of studies over the years (Cote & Buckley, 1987). Sources of common method bias include common rater effects, item characteristics effects, item context effects, and measurement context effects (Podsakoff et al., 2003 p. 882).

5.4.2.1 Types of Common Method Bias

Common rater effects occur when the same individual is providing responses for both the independent and dependent variables and manifests through their responses in the following ways:

1. Consistency – where respondents try to maintain consistency in their responses to questions.
2. Implicit theories – where respondents' beliefs about the interrelationship between independent and dependent variables influence their responses.
3. Social desirability – where respondents attribute social desirability to specific scale answers and answer as they feel is socially acceptable.
4. Leniency bias – where respondents attribute socially desirable traits, attitudes, or behaviors to individuals that they know or like
5. Acquiescence bias – where respondents agree or disagree with questions independent of the content.

6. Mood state – where respondents have the propensity to view themselves (and the world) in either a positive or negative state and bias their answers based on these views.
7. Transient mood state – where respondents react to mood-inducing events to influence their responses.

Item characteristics effects refer to respondents' tendency to attribute characteristics directly to the item on the questionnaire. These effects manifest themselves in the following ways:

1. Item social desirability – where items are written to reflect a social position.
2. Item demand characteristics – where the items convey hidden cues.
3. Item ambiguity – where items that are ambiguous allow the respondents to define the item based on their own definition, not necessarily that of the researcher
4. Common scale formats – where covariation occurs due to the use of a type of scale (Likert, etc.)
5. Common scale anchors – where the use of the same anchors throughout a questionnaire causes variance among the responses.
6. Positive (negative) wording – where the use of positively (negatively) worded items in a questionnaire may produce artificial relationships.

Item context effects are biases that result due to contextual effects of where and how an item appears (priming, scale length, mood). Finally, measurement context effects refer to effects associated with using similar contexts for measuring both independent and dependent variables (same point in time, same location, same medium).

Podsakoff et al. (2003) note that there are both procedural and statistical remedies to control for common method bias. The procedural remedies include the following:

1. Obtaining measures of the dependent and independent variables from different sources.
2. Using temporal, proximal, psychological, or methodological separation of measurement (e.g. measure at different times).
3. Ensuring respondent anonymity.
4. Counterbalancing question order.
5. Improving scale items.

Statistical remedies for common method bias include:

1. Harman's single factor test.
2. Partial correlation procedure.
3. Controlling for directly measured latent variables.
4. Controlling for unmeasured latent variables.
5. Using multiple method factors such as confirmatory factor analysis (CFA) and multitrait-multimethod (MTMM.)

Finally, a decision tree is presented to assist researchers in determining which procedural and statistical methods should be used, based on the study, to reduce common method bias. This study falls under Situation 5 (Podsakoff et al., 2003 p. 898) where:

1. The predictor and criterion variables cannot be obtained from different sources.
2. The predictor and criterion variables cannot be measured in different contexts.
3. The sources of method bias can be identified.
4. The method bias(es) can be validly measured.

Recommendations for studies that fall under Situation 5 are as follows:

1. Use all procedural remedies related to questionnaire design
2. Separate measurement of predictor and criterion variable psychologically

3. Guarantee response anonymity
4. Use single-common-method-factor approach
5. Use multiple-specific-method-factors approach

5.4.2.2 Procedural Remedies

As detailed in Chapter 4, the scale items were subjected to rigorous review by peers and through a pretest and pilot test and improved to provide more consistent and unbiased scales. In this way I controlled for item characteristic effects and item context effects. Likewise, the questionnaire was designed so that criterion and predictor variables were separated. The questions relating to organizational control and mandatoriness were on different pages from the precautions variables, with questions relating to computer self efficacy between the constructs, and variables relating to risk were on separate pages of the questionnaire. Furthermore, the respondents were guaranteed anonymity for their participation (#3), and the steps taken to ensure that anonymity was maintained were reviewed by the Institutional Review Board (IRB) at the University of Pittsburgh. These methods controlled for measurement context effects.

5.4.2.3 Statistical Remedies

Podsakoff et al. (2003) recommend that the single-common-method-factor approach and the multiple-specific-method-factors approach be used to show any common method bias, specifically common rater effects, that might be present in the study. To do this I need to identify the questions that could cause common rater effects. The primary bias that may be shown in this study is social desirability, as there is a strong cultural and legislative emphasis on computer security at the target site. The IS department at the hospital regularly emphasizes security and the HIPAA and Sarbanes-Oxley legislation require that security training be

performed on an ongoing basis. There may also be some leniency effects present in the study if some questions are biased toward positive or negative affectivity, but that is not possible to identify with this study. The variables that could show common method bias are detailed below in Table 44, one of which is included as part of the mandatoriness construct.

Table 44 – Probable Common Rater Bias Questions

Variable	Bias Type	Question
Mand01	Social Desirability	I am required to secure my system according to the organization's documented policies and procedures.
Prec09	Social Desirability	I share my passwords with other people.
Prec10	Social Desirability	I allow non-employees access to my computer.
Prec16	Social Desirability	I regularly download "unauthorized" software to install on my computer.

Using these variables, to test for common method bias, we load the items above to a construct not directly in the path model and examine the overall model to see if it changes significantly. The results of this analysis show that none of the relationships changed in any significant way with t-statistics changing by less than one for any relationship, and the significance levels remaining the same for all relationships. I can thus conclude that common method bias is not a significant factor in this study.

5.5 CHAPTER SUMMARY

This chapter described the data collection, the analysis of the data, and the results of hypothesis testing. The data were examined for response bias and some cases were removed after analysis for inconsistent responses or missing data. Reliability and validity tests were performed on both

the reflective and formative constructs to ensure that the measures were statistically sound and that the model measures what is intended (Straub et al., 2004). The proposed hypotheses were tested using PLS with the proposed model explaining approximately 41 percent of the variance in the study. Common method bias was discussed and tests were performed to see if common method bias exists in the study. While the overall statistics were affected, none of the relationships changed in any significant way as a result of these tests, so common method bias was excluded as a possible weakness in this study.

6.0 DISCUSSION AND CONCLUSION

This research has proposed a model of precaution taking behavior based on the control and fear of crime literatures. This chapter provides a discussion of the results and the implications for both practitioners and researchers. The limitations of the study and the avenues for future research are also discussed.

6.1 DISCUSSION OF THE RESEARCH FINDINGS

Organizations face a dilemma of how to promote security policies and procedures to individual employees in the most effective way. The purpose of this research is to examine this dilemma. Specifically, this dissertation addressed the following research questions:

1. What effects do behavioral controls have on security precautions taken by individuals?
2. What role do individual perceptions of mandatoriness have on the level of precautions taken by individuals?
3. What effects do individual risk perceptions have on security precautions taken by individuals?

The proposed model and theoretical basis of this research suggested that it was not only organizational control aspects related to computer security that encouraged individuals to take precautions, but also individual experience manifested through risk assessment that influence individual choices to take precautions. The results of this research show that both controls and risk have an impact on individual precaution taking. Likewise, mandatoriness is a significant variable that further helps us explain individuals' approach to controls.

The majority of the research hypotheses were supported as shown below in Table 45. The overall model performed very well with 49 percent of the variance being explained in the relationships between the control elements and mandatoriness, 11 percent of the variance being explained in the relationships between experience and risk perceptions, and 41 percent of the variance being explained between mandatoriness, the control variables, experience, risk perceptions, and precautions taken, giving strong support for the overall model.

Table 45 – Tested Hypothesis Results Summary

Hypothesis	Predicted Effect	Result
Hypothesis 1	Specification affects Mandatoriness	Supported
Hypothesis 2	Evaluation affects Mandatoriness	Supported
Hypothesis 3	Reward affects Mandatoriness	Not Supported
Hypothesis 4	Mandatoriness affects Precautions Taken	Supported
Hypothesis 5	Direct Experience affects Risk Perceptions	Supported
Hypothesis 6	Indirect Experience affects Risk Perceptions	Supported
Hypothesis 7	Risk Perceptions affect Precautions Taken	Not Supported

This research has proposed and tested a model that examines security from behavioral, control, and individual risk perspectives simultaneously, while extant literature typically focuses on technical perspectives to ensure security. This research allows us to determine the effectiveness of behavioral controls on the overall security effort within a firm and to determine the extent to which individual characteristics influence individuals' precaution taking behavior.

Overall the model explains more variance than models based on the control perspective or risk perspective alone and is thus a valid contribution to theory and knowledge.

The results of this research emphasize the need for managers to focus on behavioral solutions in addition to the technical ones in the context of computer security. As predicted, the specification of a policy significantly predicts individual perceptions of mandatoriness (Hypothesis 1). Further, specification has indirect effects on precautions taken, mediated by individual perceptions of mandatoriness (Hypothesis 4). The perception that a desired behavior is evaluated in itself contributes to perceptions that the policy is mandatory (Hypothesis 2), as well as indirectly motivating individuals to take precautions (Hypothesis 4). These results suggest that specification of a policy is a mental construct where the simple act of codifying required behavior and then evaluating the behavior itself effects behavioral change as well as conveying a sense of mandatoriness. The results additionally suggest that the specification of computer security policies and evaluation for non-compliance with those policies both contribute to perceptions of mandatoriness (Hypothesis 1 & 2). Likewise, the results indicate that mandatoriness, as defined in this research, is an important construct in determining the intentions of individuals to follow policies and procedures.

Second, the strong loading of punishment items with mandatoriness items indicate that perceptions of mandatoriness are directly linked to the punishment affixed for non-compliance in the security realm. This result, coupled with the lack of support for the reward hypothesis, may indicate that individuals perceive that following computer security policies and procedures is more mandatory when individuals are punished for failure to comply. This supports previous research regarding the need for clear statements regarding punishments for violation of security

policies (Straub, 1990), and indicates that employees will take security policies seriously if they believe that they will be punished if they violate those policies.[12]

Third, the impact of direct experience on risk (Hypothesis 5) and the impact of indirect experience on risk (Hypothesis 6) were supported confirming extant literature results. Individuals perceive risk based not only on their own experiences but also based on the experiences that they hear from others, either personally or through news media.

6.1.1 Reward

The results do not support the prediction that the effects of using reward as an incentive to follow mandatory guidelines (the security policy) impact individual perceptions of mandatoriness (Hypothesis 3). This is contrary to what is typically discussed in the literature, where rewards are used as incentive to change behaviors (Eisenhardt, 1988; Luft, 1994). The reason for the lack of support may be a result of the differences in context between what is typically seen in the literature and the security context. The literature findings usually reflect situations where rewards are used as incentives for individuals to go above and beyond their current compensation level (Luft, 1994) for doing their jobs (endeavoring to keep their computer systems secure) and does not appear to have the desired impact. Other explanations for this finding may either be that the rewards themselves are too distant from the act of securing the

[12] The consolidation of the punishment and mandatoriness constructs has the potential to skew the observed effects in this study. Additional analysis was made where the punishment items were removed from the model. No substantial change occurred either in the strength of the model or in the significance of the paths as a result of this additional analysis.

computer, or that organizations do not typically engage in rewarding precaution-taking behavior. A post-hoc analysis of the reflective variable scores (detailed in Appendix I) shows that there is no significant difference between the results of full-time and part-time employees regarding reward, which excludes the employee status demographic variable as a possible cause for the non-significance of the hypothesis. These results require further research to provide more insight to this finding. Regardless, rewards were not found to impact computer security precaution taking behaviors.

6.1.2 Risk

Likewise, the impact of risk perceptions on the dependent variable (Hypothesis 7) was not supported. The primary reason for this result may be how risk was characterized. Following extant literature, risk was presented as an overall construct composed of the likelihood that (something) would happen multiplied by the impact of the occurrence on the individual (Barki et al., 2001). While this approach to risk allows us to obtain an overall risk measure, it may be that the formation of a multidimensional construct is not necessary. Law, Wong & Mobley (1998) noted that a multidimensional construct "…consists of a number of interrelated attributes or dimensions and exists in multidimensional domains. In contrast to a set of interrelated unidimensional constructs, the dimensions of a multidimensional construct can be conceptualized under an overall abstraction, and it is theoretically meaningful and parsimonious to use this overall abstraction as a representation of the dimensions" (p. 741). The authors further state that a valid multidimensional construct has internal relationships that are both precisely specified and sufficiently exhaustive to make the parsimonious new construct valid. (Law et al., 1998).

The current risk construct takes two aspects of risk from the fear of crime literature, likelihood and impact, and attempts to explain individuals' precaution-taking behaviors. This construct was not designed to be comprehensive, thus examining the component parts may provide more information than the aggregated construct. A post-hoc analysis shows that if risk is split into its component parts, likelihood and impact, as shown below in Figure 10, more of the impact of risk on precautions taken is explained.

With the changed model, hypothesis 5, 6, and 7 need to be restated as follows:

H_{5A} Direct experience with cyber-security incidents will be positively associated with the individuals' perception that a cyber-security incident is likely to happen.

H_{5B} Indirect experience (through media, collegial anecdotes, or other sources) with cyber-security incidents will be positively associated with the individuals' perception that a cyber-security incident is likely to happen.

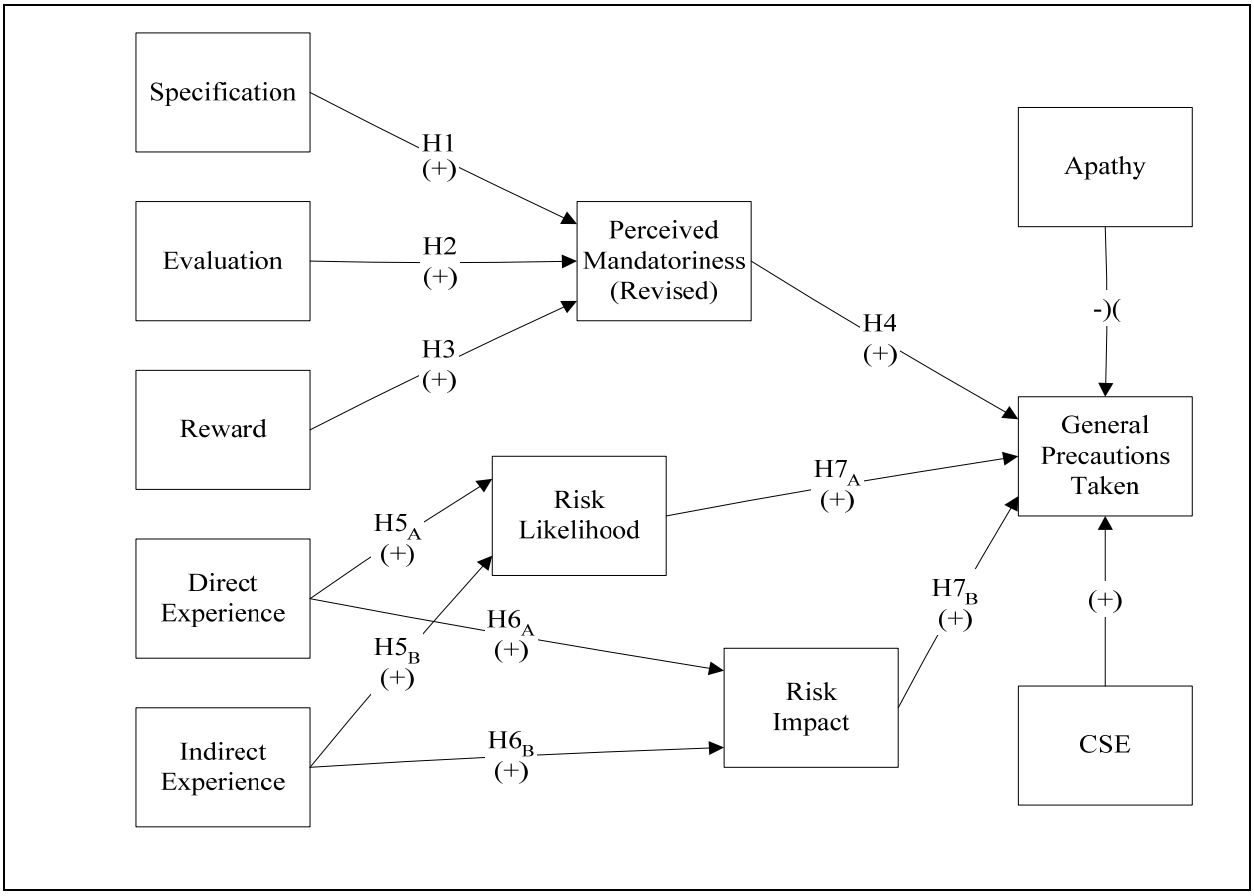
H_{6A} Direct experience with cyber-security incidents will be positively associated with the individuals' perception of the impact of a cyber-security incident on them.

H_{6B} Indirect experience (through media, collegial anecdotes, or other sources) with cyber-security incidents will be positively associated with the individuals' perception of the impact of a cyber-security incident on them.

H_{7A} The perception of the likelihood of a cyber-security incident occurring will be associated with an increased likelihood that the individual will take precautions.

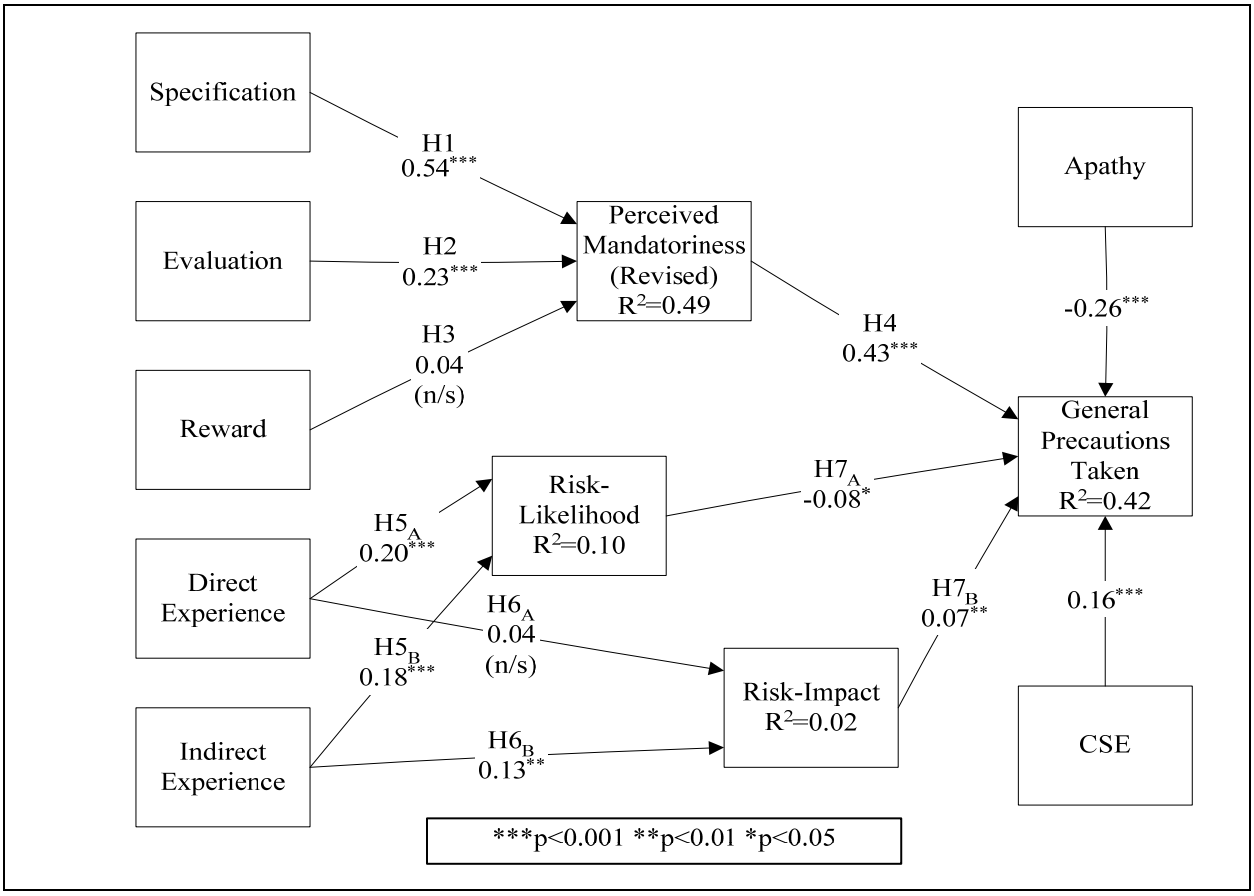
H_{7B} The perception of the impact of a cyber-security incident on the individual will be associated with an increased likelihood that the individual will take precautions.

Figure 10 – Theoretical Model with Risk Split into Component Parts



The revised results are shown below in Figure 11. Additional tests were done as detailed above in Section 5.4.2.2 on the revised model and show no indication of common method bias.

Figure 11 – Revised Path Coefficients and Explanatory Power of the Measurement Model



The results for hypotheses 1-4 are unchanged, but the overall explanatory power of the model (R^2) on has increased (slightly) from 0.41 to 0.42. With the revised hypotheses on the risk side of the model, we see that the effects of both direct experience and indirect experience significantly influence perceptions of risk-likelihood (β=0.20, p<.001, and β=0.18, p<.001 respectively) as proposed in Hypothesis 5_A and 5_B with 10 percent of the variance of likelihood being explained. Likewise, indirect experience significantly influences risk-impact perceptions (β=0.13, p<.01) as predicted in Hypothesis 6_B with 2 percent of the variance explained by both direct and indirect experience. Finally, Hypothesis 7_B, the influence of risk-impact on the dependent variable, precautions taken, was significant (β=0.07, p<.01).

Direct experience does not have any effect on risk-impact as proposed by Hypothesis 6_A. This is consistent with the literature showing that individuals are not good at accurately assessing impact (Frieze et al., 1987). Additionally, individuals' perception of something being likely to happen to them has a negative significant effect on precautions taken (β=-0.08, $p<.05$), in the opposite direction than predicted in Hypothesis 7_A. There are several explanations for why this may be the case. First, it may be that individuals, when perceiving that something is likely to happen to them, become overwhelmed and are thus less likely to take precautions. Second, it may be that the precaution needed to be taken is insufficiently specified, and thus does not provide enough direction to the individuals when presented with the evidence that they are likely to become victims. Lastly, it may be that individuals, recognizing their vulnerability and taking precautions to mitigate that vulnerability, feel that it is less likely that something will occur: In other words, the direction of the path in Hypothesis 7_A may need to be reversed in future studies.[13]

While the overall effect of this change on the model is quite small (a change in R^2 of 0.01) the separation of the risk elements does provide us with more understanding of what is happening than when risk is monolithic. The results show that that individuals feel the potential impact of a scenario is a motivation for precaution taking (Hypothesis 7_B) that wouldn't have been visible without the revised model where risk had no impact on the dependent variable. Likewise, the results show that direct personal experience does not have any effect on individual

[13] Additional analysis was performed to discover if there is any effect from the interaction of risk-likelihood and risk-impact on the dependent variable. The results from this additional analysis did not change the overall strength of the model, but did result in Hypothesis 7 (unsupported and significant in the opposite direction than hypothesized) to no longer be a significant factor.

perceptions of impact (Hypothesis 6_A); rather, all of the impact is shown in the perceptions that individuals are likely to be at risk (Hypothesis 5_A). By taking the model to a more granular level, the results show more explicitly how risk perception works on individual precaution taking. This phenomenon will be investigated in future research.

6.1.3 Control Variables

Both of the control variables significantly affected the likelihood that security precautions would be taken. Higher levels of computer self efficacy (CSE) significantly influence the likelihood that individuals will take precautions (β=0.16, $p<.001$). Likewise, apathy regarding computer security significantly influences precaution taking in the negative direction (β=-0.26, $p<.001$). The significance of apathy in the model shows that individuals do not necessarily pay attention to security, further emphasizing that the attitudes toward computer security are not as strong as they should be considering the seriousness of the issue. One reason for the apathy may be the absence of line authority by those who enforce the policies over those required to follow them. This implies that line management, in addition to IS or security management personnel within the organization, needs to emphasize the importance of security on a regular basis to overcome these effects. Additionally, the significance of CSE emphasizes the need to train all members of the organization on how to use a computer and "demystify" the security aspects. As individuals feel more confident in using the computer to complete their work, they will be more likely to take precautions with the computer.

6.2 LIMITATIONS

As with all research, there are several limitations to this study that should be noted. First, the use of a single respondent to measure both the dependent and independent variables can be problematic and could lead to common method bias. While this is a concern, the study deals with perceptions that are best measured by a single source. As discussed in Section 5.4.2.2, all possible procedural remedies were taken to limit the possibility of common method bias. Subsequent statistical tests, recommended in the literature (Podsakoff et al., 2003), were also performed and do not indicate the presence of common method bias.

Second, as noted earlier, there is some indication of responder bias in the survey. Respondents who answer the survey after several reminders are theorized to be the closest to individuals who did not participate in the survey. If these individuals have significantly different results than the other respondents, it may be that these results are invalid and not generalizable. Analysis showed that the final set of individuals who responded to the survey had significantly lower computer self efficacy (CSE) scores and lower risk-impact scores. With the survey being conducted online, it makes sense that individuals with lower CSE would put off taking the survey until the last minute, regardless of the requirements of the company. Likewise, individuals with lower CSE would be more likely to underestimate the impact of issues involving the computer such as computer security. Thus, while there are indications of responder bias, it is not deemed to be an issue in this research. Additionally, analysis of the entire model without the late responders does not produce a significant change in the overall strength of the model.

Third, this study is a cross sectional study which could affect the internal validity of the study. The theory presented here indicates directional relationships and effects between variables, yet was measured with a single instrument. The result of this is limitations on the

implications for causality in the model. For example, I speculated that Hypothesis 7_A was not supported because individuals took precautions and thus thought they were less likely to experience a cyber-security incident. Without longitudinal data, this relationship is not possible to examine in the current study. While cross sectional studies have their limitations, this study is grounded in a strong theory base, making it less likely that the directionality of the relationships is spurious.

Finally, due to the fact that the data were gathered at a single organization, the findings of this study may not be generalizable to other populations in other settings. While this is a concern in all research endeavors, the theory used to formulate the hypotheses was not derived from a single source, rather from many researchers' theory and results over many years. As a result, it is likely that the findings of this study are generalizable.

6.3 IMPLICATIONS FOR RESEARCH

This research offers many contributions to the IS literature. First, this research looks at a topic that is largely undeveloped: Information Security. Given the attention security is currently being given in the media and by academic groups, this research is both timely and important to this developing body of knowledge. There are several implications that can be drawn from the results of this research. First, this research allowed me to focus on and test the elements of control proposed by Kirsch (2004) and provide empirical support for existing literature. The model additionally expressly includes a concept that is alluded to within the literature: Mandatoriness. The general assumption in the control literature is that controls would not be specified if they were not mandatory, but often controls which are not perceived to be important

by individuals are disregarded to the detriment of the organization. The strong negative effects of apathy reinforce this view.

Second, the fact that reward did not have a significant affect on mandatoriness as theorized presents an interesting opportunity to examine a basic fixture in the control literature. Extant theory posits that reward will affect individuals' behaviors. This research extended this theory to include reward affecting mandatoriness which in turn affects individuals' behaviors. Analysis of the data shows that, in the computer security context, reward did not have a significant impact on either mandatoriness or precaution taking. The reasons for this have been discussed above, but nevertheless it indicates that individuals do not always react to controls in the same way in different contexts.

Third, this research examines the effects of individual risk assessment on behaviors and allows us to test whether centrally directed policies have more weight than individual assessments of risk. If individual risk perceptions play an important role in the precaution-taking behaviors of employees, organizations should be able to use these results to encourage individuals to take cyber-precautions. These results show that risk itself is not a monolithic structure and should not be treated as such. The literature suggests that both direct and indirect exposure affect individuals' perceptions of overall risk. While there are many definitions of what "risk" is, I have found that characterization of risk as a combination of both likelihood and impact perceptions masks the effects of exposure to security incidents. While the goal of research is to present parsimonious constructs wherever possible, this research indicates that more information can be obtained by splitting the risk construct into its component parts.

Further, the impact of experience on the component parts of risk gives us insights that would otherwise not be seen. Indirect experience has a significant impact on individuals'

perceptions of the impact, while direct experience does not. This is consistent with the fear of crime literature where individuals perceive that bad things happen to others but do not necessarily happen to them (Hanson et al., 2000). Extended into the computer security realm, these perceptions of impact have a direct, significant effect on individuals' likelihood to take precautions. The other aspect of risk identified in the IS literature, likelihood (Barki et al., 2001), has interesting effects on individual precaution taking behavior. This analysis shows that while both direct and indirect experience significantly affect individuals' perceptions that they are likely to become victims (Hypotheses 5_A and 5_B), the overall effect of individuals believing that they are likely to become victims is significant in the opposite direction: Individuals are less likely to take precautions when they believe that they are more likely to become victims.

Finally, the inability of individuals to differentiate between punishment for non-compliance with a policy and individual perceptions that a policy is mandatory based on the factor analysis above has interesting implications for research. The concept of a "mandatory" control is woven throughout control literature, as discussed in the literature review above, but has never been directly addressed. While punishment is not typically addressed in the IS control literature, punishment could be implied through the discussions of reward in that literature. This result, coupled with the insignificant relationship between reward and mandatoriness, indicates that, in the computer security context, the interplay between reward, punishment, and mandatoriness is more complex than originally theorized.

6.4 IMPLICATIONS FOR PRACTICE

The positive results of the revised theoretical model also have strong implications for management decisions when formulating security policies. One implication for managers is in the control mechanisms that they use to encourage individuals to comply with security policies and procedures. This research has shown that the simple act of specifying a policy has a strong effect on both perceptions of mandatoriness and on compliance with the procedure. Likewise, following up to determine whether individuals are complying also has a strong effect on both mandatoriness and compliance. Managers should formulate policies, communicate them to the employees, and then evaluate performance. In this way management shows that they are serious about computer security policy compliance.

This research has shown that organizational sharing and explanation of the impact of cyber-crime on the individual can help to motivate precaution taking behavior. While discussion of a certain scenario's likelihood (statistics) is typical in organizations, it is more helpful to emphasize the impact of the scenario as this research has shown that understanding the impact motivates individuals to take cyber precautions while the statistics on likelihood of exposure does not. Individuals typically do not experience a high volume of cyber attacks; thus, when they hear about the impact of a cyber crime on others it motivates them to take more precautions.

The significance of apathy in the model shows that individuals do not necessarily pay attention to security, further emphasizing that the attitudes toward computer security are not as strong as they should be considering the seriousness of the issue (America Online & National Cyber Security Alliance, 2005). One reason for the apathy may be the absence of line authority by those who enforce the policies over those required to follow them. This implies that line management, in addition to IS or security management personnel within the organization, need

to emphasize the importance of security on a regular basis to overcome these effects. Additionally, the significance of computer self efficacy means that management needs to invest in training programs for their organization. The payoff for this investment will be employees who have a deeper understanding of computers and will be more willing to follow computer security policies because the policies will make more sense.

Managers should also consider the impact of strong punishments on enhancing organizational computer security. Statistically speaking, and to some measure theoretically, individuals are unable to differentiate between punishments and something being mandatory. Additionally, anything that affects individuals' compensation motivates them to view it as mandatory, as shown with the statistical loading of Rew02 with the mandatoriness and punishment construct. Managers should consider implementing punishments for failure to comply if they want employees to take extant policies seriously.

A final implication for managers is that their approach to security is a key issue. When security is viewed (either explicitly or implicitly) as something that is "above and beyond" individuals' job descriptions, it is unlikely that much thought will be given to their part in computer security. The results show that managerial attention is needed to craft meaningful computer security policies and to motivate individuals to follow them. Managers should emphasize the specification of policies and evaluation of those policies for non-compliance, while giving less emphasis to reward.

6.5 FUTURE RESEARCH

A number of future studies can be built upon this research related to the results presented here, the limitations discussed above, and other questions brought up during the course of the research. An obvious addition to this study would be a replication of the study in several different organizations and settings. This study focused on the medical sector, but is not necessarily generalizable to other hospitals or areas of the health care sector. Likewise, other business sectors do not have HIPAA regulations driving the increased interest in computer security, but they do have to comply with the Sarbanes-Oxley laws requiring increased awareness of computer controls and computer security. It would be interesting to examine different organizations in different sectors to gauge the relative effectiveness of the two laws if any differences exist.

A second project would be to examine more closely the relationships between punishment and mandatoriness. The results of this study showed that individuals were not able to differentiate between punishment and a control being mandatory. Whether this is merely because the organization does a poor job of emphasizing necessity without punishment or whether individuals are able to discriminate between punishments and mandatory requirements is a research question worth pursuing as it relates to both the literature and practice.

Another potential area of future research would be to further examine the relationship between reward and mandatoriness. In this study, reward had no significant effect on mandatoriness, contrary to the literature and my predictions. While I have discussed this above, a worthwhile approach to this issue would be to examine both the context and the types of controls that individuals consider to be mandatory and research the impact. While I have

speculated that reward was not set up in the "classic" way, I have no empirical data to back up that assertion.

A fourth area of future research would be to explore the multidimensionality of precaution taking behavior. This research focused primarily on general precautions, but I had to exclude a large number of questions from the study for the sake of a parsimonious model. One potential research question for this line of research is "Does a general level of precaution taking lead to more specific actions?" Another is "To what degree do mandatoriness and risk impact the more specific precaution taking behaviors?" This line of research would be valuable because it could help mangers identify the specific mindsets that would lead to individuals increasing their precaution taking behaviors.

Fifth, this study focused only on formal behavioral controls. It is likely that the presence of a strong security culture (clan control) or outcome controls explains some of the variance that was not captured in this study. The examination of these other types of control in conjunction with formal behavioral controls should be the topic of future studies. Likewise, future research should include the relationships element of control as the security phenomenon is examined in terms of different relationships to help us better understand how control works within organizations.

Finally, to address the second failed hypothesis in this study, a future area of research should address the relationship between individuals' perceptions of the likelihood that they will become victims of some type of cybercrime and their behaviors. This research indicated that there was a significant negative relationship between general precautions taken and risk likelihood perceptions. Some potential research questions include the following: What is the cause of this relationship? Is the hypothesis in the opposite direction? Are there other factors

besides likelihood and impact that more fully explain these relationships? One way I might test these questions could be through a series of controlled experiments where individuals are primed for a specific situation and then asked what they might do.

6.6 CONCLUSION

When the individual is the last line of defense in computer security, it is logical that organizations should craft strong computer policies and procedures and do all they can to motivate individuals to comply. This research shows us that the process of implementing computer security policies goes beyond crafting the policy and telling individuals in the organization that the policies are mandatory. Likewise, this research has shown that appealing to individuals' perceptions of risk can significantly affect behaviors. This dissertation started out with three basic questions regarding the impact of controls, the impact of risk perceptions, and the impact of mandatoriness on individual precaution taking behaviors. This work continues the development of the established control literature by looking at the phenomenon of control at a more granular level and further breaking down control to examine individual attitudes toward those controls. Furthermore, it incorporates additional theory from the fear of crime literature at the individual level to strengthen the proposed control model. This research ends by making a contribution to both the literature and to managerial practices. It additionally provides a stepping off point for additional research and other contributions to theory and practice. These results suggest many ways that theory can be improved and ways that managers can improve their goals of providing secure computer systems for their organizations and, as computer security continues

to increase in importance within organizations, emphasize the increasing need to include the individual in the security equation.

APPENDICES

Appendix A

PRETEST INSTRUMENTS (PAPER VERSION)

Computer Precaution-Taking Research Study

You are being asked to participate in a research study being performed by the University of Pittsburgh, Katz Graduate School of Business to investigate individuals' computer precaution-taking behavior. This research is voluntary and you may withdraw at any time. There are no known risks involved in this research.

In this survey, you will be asked a variety of questions about your attitudes and experiences related to working in an online environment. All responses will be kept anonymous. Your individual responses will not be disclosed to others and your participation in this survey will have no effect on your standing in this class. **Do not write your name on this answer sheet.** Feel free to skip any questions you would rather not answer. When you answer, please do so as accurately and completely as possible.

If you have any questions, please ask the facilitators or contact Scott Boss at scboss@katz.pitt.edu.

I understand the above terms and agree to participate. Yes _____ No _____

Welcome to this study of computer precaution-taking behavior and thank you for your willingness to participate. You will complete a series of questions for which there are no "right" or "wrong" answers. We would like to know honestly how you think about each of these issues. This study is divided into several parts. Each section has specific instructions for you to follow. If at any time you have questions, please see one of the facilitators present.

1. Please indicate the degree to which or the extent to which the following apply to security policies and procedures within your organization.

Scale

		Low			**Moderate**			**High**
a	To what degree is there an understandable, established set of rules that can be followed to ensure that my system is properly secured?	1	2	3	4	5	6	7
c	To what extent are there written rules regarding security policies and procedures?	1	2	3	4	5	6	7
e	To what extent are logs kept computer security behaviors?	1	2	3	4	5	6	7
f	To what degree is management aware of my behavior as it relates to security?	1	2	3	4	5	6	7

2. Please indicate the frequency or extent to which management evaluates security policies and procedures.

Scale

		Low or Not at All		**Moderate**				**High or Very Frequently**
a	How frequently do managers of your organization evaluate your security behaviors?	1	2	3	4	5	6	7
c	To what extent do managers formally evaluate you and your colleagues regarding compliance with security policies?	1	2	3	4	5	6	7
d	To what extent does your manager evaluate data relating to following security policies and procedures?	1	2	3	4	5	6	7
f	To what extent are managers determining whether I follow security procedures?	1	2	3	4	5	6	7

3. Please indicate the degree or extent to which management rewards or punishes individuals for compliance with security policies and procedures.

Scale

		Low			Moderate			High
a	Performance evaluations, pay raises, promotions, and other tangible rewards are dependent on the degree to which I follow documented security policies and procedures.	1	2	3	4	5	6	7
b	To what extent to individuals receive personal mention in oral or written reports for compliance with security policies and procedures?	1	2	3	4	5	6	7
c	To what extent are individuals given monetary or non-monetary rewards for following security policies and procedures?	1	2	3	4	5	6	7
d	To what extent are individuals sanctioned for not complying with documented security policies and procedures?	1	2	3	4	5	6	7
e	To what extent are senior management made aware of individuals who do not follow security policies and procedures?	1	2	3	4	5	6	7
f	To what degree are specific punishments tied to whether you follow security policies and procedures?	1	2	3	4	5	6	7

4. Please indicate the degree to which the following apply to you within this organization.

Scale

		Low Degree			Moderate Degree			High Degree
a	I am required to secure my system according to documented policies and procedures.	1	2	3	4	5	6	7
b	Company policy dictates that I take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.)	1	2	3	4	5	6	7
c	Compliance with security policies and procedures is required by management.	1	2	3	4	5	6	7
e	Company policies emphasize the need for me to follow security polices to the best of my ability.	1	2	3	4	5	6	7

5. Please use the following scale to indicate the degree to which you take precautions to protect your system.

Scale

		Low Degree		**Moderate Degree**				**High Degree**
a	I pay attention to security concerns during my daily routine.	1	2	3	4	5	6	7
b	I try to keep aware of the latest security threats so I can protect my system.	1	2	3	4	5	6	7
c	My system is as secure as I can make it.	1	2	3	4	5	6	7
d	I regularly download security patches for my operating system/computer programs/virus protection software.	1	2	3	4	5	6	7
e	I regularly download virus protection software updates.	1	2	3	4	5	6	7
f	I take precautions with my passwords (Protect them, regularly change them, use multiple passwords, etc.).	1	2	3	4	5	6	7
g	I share my passwords with other people. (R)	1	2	3	4	5	6	7
h	I allow non-employees access to my computer. (R)	1	2	3	4	5	6	7
i	I allow other employees access to my computer. (R)	1	2	3	4	5	6	7
j	I notify a manager/IS personnel if I suspect that my system has been infected by a virus.	1	2	3	4	5	6	7
k	I notify a manager if the system slows down to an unreasonable level.	1	2	3	4	5	6	7
l	I report suspicious e-mails to a supervisor or security personnel in the Information Systems department.	1	2	3	4	5	6	7
m	I open attached executables from friends even if the message doesn't make particular sense. (R)	1	2	3	4	5	6	7
n	I regularly download "unauthorized" software to install on my computer. (R)	1	2	3	4	5	6	7

6. Please indicate the degree to which you believe that you are at risk of experiencing the following.

Scale

		Low Risk		**Moderate Risk**				**High Risk**
a	Computer system corrupted by a virus	1	2	3	4	5	6	7
b	Computer system taken over by a hacker	1	2	3	4	5	6	7
c	Personal information misused on the internet	1	2	3	4	5	6	7
d	Credit card number stolen	1	2	3	4	5	6	7
e	Other financial information stolen	1	2	3	4	5	6	7
f	Current work data corrupted by a virus or cyber-attack	1	2	3	4	5	6	7

		Low Risk			Moderate Risk			High Risk
g	Identity stolen	1	2	3	4	5	6	7
h	Work lost due to virus computer security incident	1	2	3	4	5	6	7
i	Corporate computers inaccessible because of computer security problems	1	2	3	4	5	6	7
j	Problems accessing data over the internet because the system is too slow	1	2	3	4	5	6	7
k	Downloading infected attachments in e-mail	1	2	3	4	5	6	7
l	Work account compromised	1	2	3	4	5	6	7
m	Experiencing a Denial of Service attack	1	2	3	4	5	6	7

7. Please indicate the degree of experience **<u>you personally</u>** have had with each of the following scenarios.

Scale

		Never had any experience		Had a moderate degree of experience			Have had a great deal of experience	
a	Computer system corrupted by a virus	1	2	3	4	5	6	7
b	Computer system taken over by a hacker	1	2	3	4	5	6	7
c	Personal information misused on the internet	1	2	3	4	5	6	7
d	Credit card number stolen	1	2	3	4	5	6	7
e	Other financial information stolen	1	2	3	4	5	6	7
f	Current work data corrupted by a virus or cyber-attack	1	2	3	4	5	6	7
g	Identity stolen	1	2	3	4	5	6	7
h	Work lost due to virus computer security incident	1	2	3	4	5	6	7
i	Corporate computers inaccessible because of computer security problems	1	2	3	4	5	6	7
j	Problems accessing data over the internet because the system was too slow	1	2	3	4	5	6	7
k	Downloaded infected attachments in e-mail	1	2	3	4	5	6	7
l	Work account compromised	1	2	3	4	5	6	7
m	Experienced a Denial of Service attack	1	2	3	4	5	6	7

7 (alternate) Please indicate the number of times **<u>you personally</u>** have had each/any of the following experiences.

Scale

		Never	Once	2-3 Times	Several Times	More than 10 times
a	Computer system corrupted by a virus	1	2	3	4	5
b	Computer system taken over by a hacker	1	2	3	4	5
c	Personal information misused on the internet	1	2	3	4	5
d	Credit card number stolen	1	2	3	4	5
e	Other financial information stolen	1	2	3	4	5
f	Current work data corrupted by a virus or cyber-attack	1	2	3	4	5

		Never	Once	2-3 Times	Several Times	More than 10 times
g	Identity stolen	1	2	3	4	5
h	Work lost due to virus computer security incident	1	2	3	4	5
i	Corporate computers inaccessible because of computer security problems	1	2	3	4	5
j	Problems accessing data over the internet because the system was too slow	1	2	3	4	5
k	Downloaded infected attachments in e-mail	1	2	3	4	5
l	Work account compromised	1	2	3	4	5
m	Experienced a Denial of Service attack	1	2	3	4	5

8. Please indicate the degree to which you have heard (from friends, collegial discussion, or in the media) **of others** (not you personally) having had experience with each of the following scenarios:

Scale

		Never heard of anyone having these experiences		Have heard of a moderate number of people having experience			Have heard a great deal about others having these experiences	
a	Computer system corrupted by a virus	1	2	3	4	5	6	7
b	Computer system taken over by a hacker	1	2	3	4	5	6	7
c	Personal information misused on the internet	1	2	3	4	5	6	7
d	Credit card number stolen	1	2	3	4	5	6	7
e	Other financial information stolen	1	2	3	4	5	6	7
f	Current work data corrupted by a virus or cyber-attack	1	2	3	4	5	6	7
g	Identity stolen	1	2	3	4	5	6	7
h	Work lost due to virus computer security incident	1	2	3	4	5	6	7
i	Corporate computers inaccessible because of computer security problems	1	2	3	4	5	6	7
j	Problems accessing data over the internet because the system was too slow	1	2	3	4	5	6	7
k	Downloaded infected attachments in e-mail	1	2	3	4	5	6	7
l	Work account compromised	1	2	3	4	5	6	7
m	Experienced a Denial of Service attack	1	2	3	4	5	6	7

8 (alternate) Please indicate the number of times you have heard (from friends, collegial discussion, or in the media) **of others** (not you personally) having each/any of the following experiences:

Scale

		Never	Once	2-3 Times	Several Times	More than 10 times
a	Computer system corrupted by a virus	1	2	3	4	5
b	Computer system taken over by a hacker	1	2	3	4	5
c	Personal information misused on the internet	1	2	3	4	5
d	Credit card number stolen	1	2	3	4	5
e	Other financial information stolen	1	2	3	4	5
f	Current work data corrupted by a virus or cyber-attack	1	2	3	4	5
g	Identity stolen	1	2	3	4	5
h	Work lost due to virus computer security incident	1	2	3	4	5
i	Corporate computers inaccessible because of computer security problems	1	2	3	4	5
j	Problems accessing data over the internet because the system was too slow	1	2	3	4	5
k	Downloaded infected attachments in e-mail	1	2	3	4	5
l	Work account compromised	1	2	3	4	5
m	Experienced a Denial of Service attack	1	2	3	4	5

9. When was the last time you personally had an experience with any of the scenarios described above? (please indicate the amount of time or "never")

_____ Never
_____ Days
_____ Weeks
_____ Months
_____ Years

10. If you feel comfortable discussing it, please describe the situation.
_____
_____
_____
_____
_____
_____
_____

11. Age _____

12. Sex Male _____ Female _____

Thank you very much for your assistance with this research project.

If you have other questions about how this study or survey,
please contact Scott Boss at scboss@katz.pitt.edu

Appendix B

PILOT TEST INSTRUMENTS (WEB VERSION)

***Introduction Page

Computer Security Survey

You are being asked to participate in a research study being performed by the University of Pittsburgh, Katz Graduate School of Business to investigate individuals' computer security behavior. This research is voluntary and you may withdraw at any time. There are no known risks involved in this research. To show our gratitude for your participation, once you have completed the questionnaire you will be entered into a drawing for an iPod.

In this survey, you will be asked a variety of questions about your attitudes and experiences related to working in an online environment. The entire questionnaire will take approximately 15 minutes to complete. All responses are confidential and your individual responses will not be disclosed to others and your participation in this survey will have no effect on your standing in this organization. When you answer, please do so as accurately and completely as possible.

If you have any questions, please contact Scott Boss at scboss@katz.pitt.edu.

Inputting my survey login id and pressing Submit indicates that I understand the above terms and agree to participate.

Enter Login ID _____

***Page Break Here

***Page 1

***General Instructions

Welcome to this study of computer precaution-taking behavior and thank you for your willingness to participate. You will complete a series of questions for which there are no "right" or "wrong" answers. We would like to know honestly how you think about each of these issues. This study is divided into several sections, and each section has specific instructions. When the question refers to the "organization," please consider the "organization" to be your department within the University of Pittsburgh.

Please indicate the degree to which you agree or disagree with the following statements.

	Strongly Disagree			**Neutral**			**Strongly Agree**
I am familiar with the University's IT security policies, procedures, and guidelines.	1	2	3	4	5	6	7
I am required to know a lot of existing, written procedures and general practices to secure my computer system.	1	2	3	4	5	6	7
There are written rules regarding security policies and procedures at the University.	1	2	3	4	5	6	7
The University's existing policies and guidelines cover how to protect my computer system.	1	2	3	4	5	6	7
Managers in my department frequently evaluate my security behaviors.	1	2	3	4	5	6	7
Managers regularly examine data relating to how well I follow security policies and procedures.	1	2	3	4	5	6	7
Managers formally evaluate me and my colleagues regarding compliance with security policies.	1	2	3	4	5	6	7
Management assesses whether I follow University security procedures and guidelines.	1	2	3	4	5	6	7

***Page Break Here

***Page 2

Please indicate the degree to which you agree or disagree with the following statements.

	Strongly Disagree			**Neutral**			**Strongly Agree**
My pay raises and/or promotions depend on whether I follow documented security policies and procedures.	1	2	3	4	5	6	7
I will receive personal mention in oral or written reports if I comply with security policies and procedures at the University.	1	2	3	4	5	6	7
I will be given monetary or non-monetary rewards for following security policies and procedures.	1	2	3	4	5	6	7
Tangible rewards are tied to whether I follow the University's IT security policies, procedures and guidelines.	1	2	3	4	5	6	7
I will be sanctioned for not complying with documented security policies and procedures.	1	2	3	4	5	6	7
Senior management will be notified if I do not follow the University's IT security policies, procedures and guidelines.	1	2	3	4	5	6	7
There are specific punishments tied to whether I follow security policies and procedures.	1	2	3	4	5	6	7
Failure to secure my system by following the University's IT security policies, procedures and guidelines can have repercussions on my career.	1	2	3	4	5	6	7

***Page Break Here

***Page 3

Please indicate the degree to which you agree or disagree with the following statements regarding this organization.

	Strongly Disagree			**Neutral**			**Strongly Agree**
I am required to secure my system according to the University's documented policies and procedures.	1	2	3	4	5	6	7
It is expected that I will take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.)	1	2	3	4	5	6	7
There is a general understanding that I will comply with University security policies, procedures, and procedures.	1	2	3	4	5	6	7
Regulatory compliance requirements (FERPA, HIPAA, etc.) emphasize the need for me to follow the University's IT security policies, procedures and guidelines to the best of my ability.	1	2	3	4	5	6	7

***Page Break Here

***Page 4

Please indicate the degree to which you agree or disagree with the following statements about how you take precautions to protect your computer system.

	Strongly Disagree			**Neutral**			**Strongly Agree**
I pay attention to security concerns during my daily routine.	1	2	3	4	5	6	7
I keep aware of the latest security threats so I can protect my system.	1	2	3	4	5	6	7
My system is as secure as I can make it.	1	2	3	4	5	6	7
I regularly download security patches for my operating system/computer programs.	1	2	3	4	5	6	7
I regularly download virus protection software updates.	1	2	3	4	5	6	7
I regularly update the anti-spyware software on my computer.	1	2	3	4	5	6	7
I update my e-mail spam filter on a regular basis.	1	2	3	4	5	6	7
I take precautions with my passwords (Protect them, regularly change them, use multiple passwords, etc.).	1	2	3	4	5	6	7
I share my passwords with other people.	1	2	3	4	5	6	7
I allow non-employees access to my computer.	1	2	3	4	5	6	7
I allow other employees access to my computer.	1	2	3	4	5	6	7
I notify a manager or IS personnel if I suspect that my system has been infected by a virus.	1	2	3	4	5	6	7
I notify a manager if the system slows down to an unreasonable level.	1	2	3	4	5	6	7
I report suspicious e-mails to a supervisor or security personnel in the Information Systems department.	1	2	3	4	5	6	7
I open attached executables from friends even if the message doesn't make particular sense.	1	2	3	4	5	6	7
I regularly download "unauthorized" software to install on my computer.	1	2	3	4	5	6	7

***Page Break Here

***Page 5

Please indicate the degree to which agree or disagree with the following statements about security:

	Strongly Disagree			**Neutral**			**Strongly Agree**
My computer doesn't have anything on it worth stealing.	1	2	3	4	5	6	7
It is not really important for me to be aware of security.	1	2	3	4	5	6	7
Someone in Information Systems takes care of security problems.	1	2	3	4	5	6	7
I pay attention when people talk about computer security.	1	2	3	4	5	6	7
Paying attention to security takes too much time.	1	2	3	4	5	6	7
I'm too busy to be bothered by information security concerns.	1	2	3	4	5	6	7

***Page Break Here

***Page 6

This section asks you about your ability to use an unfamiliar piece of software. Often in our jobs we are told about software packages or systems that are available to make work easier. For the following section, imagine that you were given a new software package for some aspect of your work. It doesn't matter specifically what this software package does, only that it is intended to make your job easier and that you have never used it before.

The following questions ask you to indicate whether you could use this unfamiliar software package under a variety of conditions. For each condition please rate your confidence about your judgment, by circling a number from 1 to 7, where 1 indicates "Not at all confident," 4 indicates "Moderately confident," and 7 indicates "Totally confident."

This section asks you about your ability to use an unfamiliar piece of software.

I could complete my job using the software package . . .

	Not at all Confident						**Totally Confident**
... if there was no one around to tell me what to do	1	2	3	4	5	6	7
... if I had never used a package like it before.	1	2	3	4	5	6	7
... if I had only the software manuals for reference.	1	2	3	4	5	6	7
... if I had seen someone else using it before trying it myself.	1	2	3	4	5	6	7
... if I could call someone for help if I got stuck.	1	2	3	4	5	6	7
... if someone else helped me get started.	1	2	3	4	5	6	7
... if I had a lot of time to complete the job for which the software was provided.	1	2	3	4	5	6	7
... if I had just the built-in help facility for assistance	1	2	3	4	5	6	7
... if someone showed me how to do it first.	1	2	3	4	5	6	7
... if I had used similar packages like this one before to do the job.	1	2	3	4	5	6	7

***Page Break Here

***Page 7

Please indicate the degree to which you believe that you are at risk of experiencing the following either at home or at work.

	Low Risk			**Moderate Risk**			**High Risk**
My computer system corrupted by a virus or worm.	1	2	3	4	5	6	7
My computer system taken over by a hacker	1	2	3	4	5	6	7
Current work data corrupted by a virus or cyber-attack	1	2	3	4	5	6	7
Identity stolen (credit card number, SSN, Bank account information, etc.)	1	2	3	4	5	6	7
Work lost due to a virus or worm on my computer.	1	2	3	4	5	6	7
Computer resources (Peoplesoft, E-mail, Courseweb, University portal) inaccessible because of computer security problems	1	2	3	4	5	6	7
Downloading a file that is infected with a virus from the internet.	1	2	3	4	5	6	7
Downloading a file that is infected with a virus through my e-mail.	1	2	3	4	5	6	7
Account being used by someone else without your knowledge.	1	2	3	4	5	6	7

***Page Break Here

***Page 8

Please indicate the number of times you have heard (from friends, collegial discussion, or in the media) **of others** (not you personally) having each/any of the following experiences either at home or at work.

	Never	**Once**	**2-3 Times**	**Several Times**	**More than 5 times**
A computer system corrupted by a virus or worm.	1	2	3	4	5
A computer system taken over by a hacker.	1	2	3	4	5
Someone's work data corrupted by a virus or cyber-attack.	1	2	3	4	5
Identity stolen (credit card number, SSN, Bank account information, etc.).	1	2	3	4	5
Work lost due to a virus or worm on my computer.	1	2	3	4	5
Computer resources inaccessible because of computer security problems.	1	2	3	4	5
Downloading a file that is infected with a virus from the internet.	1	2	3	4	5
Downloading a file that is infected with a virus through my e-mail.	1	2	3	4	5
Account being used by someone else without their knowledge.	1	2	3	4	5

***Page Break Here

***Page 9

Please indicate the number of times **<u>you personally</u>** have had each/any of the following experiences either at home or at work.

	Never	Once	2-3 Times	Several Times	More than 5 times
My computer system corrupted by a virus or worm.	1	2	3	4	5
My computer system taken over by a hacker.	1	2	3	4	5
Current work data corrupted by a virus or cyber-attack.	1	2	3	4	5
Identity stolen (credit card number, SSN, Bank account information, etc.).	1	2	3	4	5
Work lost due to a virus or worm on my computer.	1	2	3	4	5
Computer resources (Peoplesoft, E-mail, CourseWeb, University portal) inaccessible because of computer security problems.	1	2	3	4	5
Downloading a file that is infected with a virus from the internet.	1	2	3	4	5
Downloading a file that is infected with a virus through my e-mail.	1	2	3	4	5
Account being used by someone else without your knowledge.	1	2	3	4	5

When was the last time you personally had an experience with any of the scenarios described above?

_____

If you feel comfortable discussing your experience, please describe the situation.

***Open Ended Question

_____
_____
_____
_____
_____
_____

***Page Break Here

Page 10

Please indicate the degree to which you agree or disagree with the following statements.

	Strongly Disagree			Neutral			Strongly Agree
Managers in my department communicate to me and my colleagues about the importance of complying with the University's IT security policies, procedures and guidelines.	1	2	3	4	5	6	7
I understand my responsibilities for maintaining security on my computer system.	1	2	3	4	5	6	7
The University provides me with information on how I can comply with the University's IT security policies, procedures and guidelines.	1	2	3	4	5	6	7
The University's policies, procedures, and guidelines are sufficient to help me protect the computer systems I use.	1	2	3	4	5	6	7

***Page Break Here

Note, these questions were added by the client.

Page 11 – Last Page

How long have you worked at this organization? _____Years

What is your current title? _____

How long have you been working with computers? _____Years

Please indicate your highest level of education:

_____ High School

_____ Some College

_____ Associates Degree

_____ Bachelors Degree/ 4 Year Degree

_____ Graduate Degree

Age _____ (*Optional*)

Gender: Male _____ Female _____ (*Optional*)

Thank you very much for your assistance with this research project.

If you have other questions about how this study or survey, please contact Scott Boss at scboss@katz.pitt.edu

Appendix C

FINAL DATA COLLECTION INSTRUMENTS (WEB VERSION)

***Introduction Page

SEMC Computer Security Survey Login

Please enter your Employee ID (no leading 0's):

_____ (e.g., Employee ID# 03901=3901)

Please enter your password (Birthday (DDMMYYYY) + Gender (M/F) see example below:

_____ (For Example: If your birthday is Sep 18, 1968, Gender = F, then, your Password is "18091968F").

Note: Gender (M/F) is case sensitive. Please use a CAPITAL M or F)

***Page Break Here

***Page 1

SEMC Computer Security Survey

Welcome to this study of computer security behavior and thank you for your willingness to participate. You will complete a series of questions for which there are no right or wrong answers. We would like to know how you honestly think about each of these issues. This study is divided into several sections, and each section has specific instructions. When the question refers to the organization, please consider the organization to be your department within SEMC.

Please indicate the degree to which you agree or disagree with the following statements.

	Strongly Disagree			Neutral			Strongly Agree
I am familiar with the organization's IT security policies, procedures, and guidelines.	1	2	3	4	5	6	7
I am required to know a lot of existing written procedures and general practices to secure my computer system.	1	2	3	4	5	6	7
There are written rules regarding security policies and procedures at the organization.	1	2	3	4	5	6	7
The organization's existing policies and guidelines cover how to protect my computer system.	1	2	3	4	5	6	7
Managers in my department frequently evaluate my security behaviors.	1	2	3	4	5	6	7
Managers regularly examine data relating to how well I follow security policies and procedures.	1	2	3	4	5	6	7
Managers formally evaluate me and my colleagues regarding compliance with security policies.	1	2	3	4	5	6	7
Managers assess whether I follow organizational security procedures and guidelines.	1	2	3	4	5	6	7

***Page Break Here

***Page 2

Organizations use different approaches to reward and sanction employees. Please indicate the degree to which you agree or disagree with the following statements.

	Strongly Disagree			Neutral			Strongly Agree
My pay raises and/or promotions depend on whether I follow documented security policies and procedures.	1	2	3	4	5	6	7
I will be sanctioned for not complying with documented security policies and procedures.	1	2	3	4	5	6	7
I will receive personal mention in oral or written reports if I comply with security policies and procedures at this organization.	1	2	3	4	5	6	7
Senior management will be notified if I do not follow the organization's IT security policies, procedures, and guidelines.	1	2	3	4	5	6	7
I will be given monetary or non-monetary rewards for following security policies and procedures.	1	2	3	4	5	6	7
There are specific punishments tied to whether I follow security policies and procedures.	1	2	3	4	5	6	7
Tangible rewards are tied to whether I follow the organization's IT security policies, procedures, and guidelines.	1	2	3	4	5	6	7
Failure to secure my system by following the organization's IT security policies, procedures, and guidelines can have repercussions on my career.	1	2	3	4	5	6	7

***Page Break Here

***Page 3

Please indicate the degree to which you agree or disagree with the following statements regarding this organization.

	Strongly Disagree			Neutral			Strongly Agree
I am required to secure my system according to the organization's documented policies and procedures.	1	2	3	4	5	6	7
It is expected that I will take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.).	1	2	3	4	5	6	7
There is an understanding that I will comply with organization security policies and procedures.	1	2	3	4	5	6	7
Regulatory compliance requirements (FERPA, HIPAA, Sarbanes-Oxley etc.) emphasize the need for me to follow the organization's IT security policies, procedures and guidelines to the best of my ability.	1	2	3	4	5	6	7

***Page Break Here

***Page 4

This section is intended to measure how you feel about unfamiliar software. It is not intended to reflect how SEMC presents software to you. Hypothetically, organizations present new software packages to us or systems to make work easier. For the following section, imagine that you were given a new software package for some aspect of your work. It doesn't matter specifically what this software package does, only that it is intended to make your job easier and that you have never used it before.

The following questions ask you to indicate whether you could use this unfamiliar software package under a variety of conditions. For each condition please rate your confidence about your judgment, by circling a number from 1 to 7, where 1 indicates "Not at all confident," 4 indicates "Moderately confident," and 7 indicates "Totally confident."

This section asks you about your ability to use an unfamiliar piece of software.

I could complete my job using the software package . . .

	Not at all Confident			Moderately Confident			Totally Confident
... if there was no one around to tell me what to do.	1	2	3	4	5	6	7
... if I had never used a package like it before.	1	2	3	4	5	6	7
... if I had only the software manuals for reference.	1	2	3	4	5	6	7
... if I had seen someone else using it before trying it myself.	1	2	3	4	5	6	7
... if I could call someone for help if I got stuck.	1	2	3	4	5	6	7
... if someone else helped me get started.	1	2	3	4	5	6	7
... if I had a lot of time to complete the job for which the software was provided.	1	2	3	4	5	6	7
... if I had just the built-in help facility for assistance.	1	2	3	4	5	6	7
... if someone showed me how to do it first.	1	2	3	4	5	6	7
... if I had used similar packages like this one before to do the job.	1	2	3	4	5	6	7

***Page Break Here

***Page 5

33% Complete

Please indicate the degree to which you agree or disagree with the following statements about how you take precautions to protect your computer system.

	Strongly Disagree			Neutral			Strongly Agree
I pay attention to computer security during my daily routine.	1	2	3	4	5	6	7
I keep aware of the latest security threats so I can protect my system.	1	2	3	4	5	6	7
My system is as secure as I can make it.	1	2	3	4	5	6	7
I regularly download security patches for my operating system/computer programs.	1	2	3	4	5	6	7
I regularly download virus protection software updates.	1	2	3	4	5	6	7
I regularly update the anti-spyware software on my computer.	1	2	3	4	5	6	7
I update my e-mail spam filter on a regular basis.	1	2	3	4	5	6	7
I take precautions with my passwords (Protect them, regularly change them, use multiple passwords, etc.).	1	2	3	4	5	6	7
I share my passwords with other people.	1	2	3	4	5	6	7
I allow non-employees access to my computer.	1	2	3	4	5	6	7
I allow other employees access to my computer.	1	2	3	4	5	6	7
I notify a manager or IS personnel if I suspect that my system has been infected by a virus.	1	2	3	4	5	6	7
I notify a manager if the system slows down to an unreasonable level.	1	2	3	4	5	6	7
I report suspicious e-mails to a supervisor or security personnel in the Information Systems department.	1	2	3	4	5	6	7
I open attached executables from friends even if the message doesn't make particular sense.	1	2	3	4	5	6	7
I regularly download "unauthorized" software to install on my computer.	1	2	3	4	5	6	7

***Page Break Here

***Page 6

50% Complete

Please indicate the degree to which you believe that one of the following scenarios is likely to happen **TO YOU** at some point in the future**.** Additionally, please indicate the impact that it would have on you if it were to occur (in terms of time lost, data lost, monetary losses, etc.).

	How Likely? *(answer below)*							**Impact to you if this occurred** *(answer below)*						
	Low Likelihood		Moderate Likelihood				High Likelihood	Low Impact		Moderate Impact				High Impact
A computer system corrupted by a virus or worm.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
A computer system taken over by a hacker.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
My work data corrupted by a virus or cyber-attack.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
My identity stolen (credit card number, Social Security Number, Bank account information, etc.).	1	2	3	4	5	6	7	1	2	3	4	5	6	7
Work lost due to a virus or worm on my computer.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
Computer resources (internal network, the Internet) inaccessible because of computer security problems.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
Downloading a file that is infected with a virus from the internet.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
Downloading a file that is infected with a virus through my e-mail.	1	2	3	4	5	6	7	1	2	3	4	5	6	7
Account being used by someone else without their knowledge.	1	2	3	4	5	6	7	1	2	3	4	5	6	7

***Page Break Here

***Page 7

In general, when I use computers, I feel I am at risk. _____Yes _____No

	Low Risk			Moderate Risk			High Risk
If Yes, please indicate the degree to which you feel you are at risk.	1	2	3	4	5	6	7

***Page Break Here

***Page 8

65% Complete

Please indicate the number of times in the last year you have heard of others (**NOT YOU**) having the following experiences (e.g.: from friends, in discussions at work, in the media, etc.). If you have heard of others having these experiences, in general, to what degree do you think it impacted those people (in terms of time lost, data lost, monetary losses, etc.)?

		Impact To Others *(if YES answer below)*						
		Low Impact			Moderate Impact			High Impact
Their computer system corrupted by a virus or worm.	Yes/No	1	2	3	4	5	6	7
Someone's computer system taken over by a hacker.	Yes/No	1	2	3	4	5	6	7
Someone's work data corrupted by a virus or cyber-attack.	Yes/No	1	2	3	4	5	6	7
Identity stolen (credit card number, Social Security Number, Bank account information, etc.).	Yes/No	1	2	3	4	5	6	7
Work lost due to a virus or worm on their computer.	Yes/No	1	2	3	4	5	6	7
Computer resources (internal network, the Internet) inaccessible because of computer security problems.	Yes/No	1	2	3	4	5	6	7
Other people downloading a file that is infected with a virus from the internet.	Yes/No	1	2	3	4	5	6	7
Others downloading a file that is infected with a virus through my e-mail.	Yes/No	1	2	3	4	5	6	7
Someone else's accounts being used by someone else without their knowledge.	Yes/No	1	2	3	4	5	6	7

***Page Break Here

***Page 9

75% Complete

Please indicate whether or not you have ever experienced any of the following situations. If **YES**, please indicate the degree to which that experience impacted you (in terms of time lost, data lost, monetary losses, etc.).

		Impact to you when it occurred? *(if YES answer below)*						
		Low Impact			Moderate Impact			High Impact
My computer system corrupted by a virus or worm.	Yes/No	1	2	3	4	5	6	7
My computer system taken over by a hacker.	Yes/No	1	2	3	4	5	6	7
My current work data corrupted by a virus or cyber-attack.	Yes/No	1	2	3	4	5	6	7
My identity stolen (credit card number, Social Security Number, Bank account information, etc.).	Yes/No	1	2	3	4	5	6	7
My work lost due to a virus or worm on my computer.	Yes/No	1	2	3	4	5	6	7
Computer resources (internal network, the Internet) inaccessible because of computer security problems.	Yes/No	1	2	3	4	5	6	7
Downloading a file that is infected with a virus from the internet.	Yes/No	1	2	3	4	5	6	7
Downloading a file that is infected with a virus through my e-mail.	Yes/No	1	2	3	4	5	6	7
Any of my accounts being used by someone else without my knowledge.	Yes/No	1	2	3	4	5	6	7

When was the last time you personally had an experience with any of the scenarios described above?

_____

Please describe the situation. (optional)

_____

_____

_____

***Page Break Here

***Page 10

85% Complete

Please indicate the degree to which you agree or disagree with the following statements about security:

	Strongly Disagree			Neutral			Strongly Agree
My computer doesn't have anything on it worth stealing.	1	2	3	4	5	6	7
It is not really important for me to be aware of security.	1	2	3	4	5	6	7
Someone in Information Systems takes care of security problems.	1	2	3	4	5	6	7
I pay attention when people talk about computer security.	1	2	3	4	5	6	7
Paying attention to security takes too much time.	1	2	3	4	5	6	7
I'm too busy to be bothered by information security concerns.	1	2	3	4	5	6	7

***Page Break Here

Page 11 – Last Page

92% Complete (last page)

84. How long have you been working with computers (in years)?_____

85. Which of the following best describes the shift on which you work?
    1. Day Shift
    2. Evening Shift
    3. Night Shift
    4. Rotate Shift

86. What is your employment status?
    1. Full-Time
    2. Part-Time
    3. PRN

87. Please indicate your highest level of education:
    1. High School
    2. Some College
    3. Undergraduate Degree
    4. Some Graduate School
    5. Graduate Degree

88. Are you a member of the RN Pride Program?
    1. Yes
    2. No

89. Which of the following categories best describes your current position? (Please choose only one)
    1. Office and Clerical (secretary, legal assistant, transcriptionist, registrar, clerk, etc.)
    2. Support Services (maintenance, environmental service, facilities, security, nutrition services, materials management/purchasing, etc.)
    3. Professional Services (non-managerial positions such as Pharmacist, PT, OT, Speech Therapist, Accountant, Auditor, Dietitian, COTA, CPTA, etc.)
    4. Technical Services (non-managerial positions such as Medical Lab Tech, Cyto-tech, Radiology Tech, Rehab Tech, Respiratory Therapist, CRTT, etc.)
    5. Staff RN
    6. Other Nursing Services (LPN, Nurse Tech, PCA, etc.)
    7. Physician
    8. Coordinator
    9. Team Leader, PDS
    10. Manager
    11. Director
    12. Administration (Executive Director, Vice President, CEO)

90. What is your ethnicity?
    1. African-American
    2. Asian
    3. Caucasian
    4. Hispanic
    5. Native American
    6. Others

91. Do you hold Personal Management Interviews (PMIs) with your immediate supervisor?
    1. Regular PMIs
    2. Irregular PMIs
    3. No PMIs

***Page Break Here

Thank you very much for your assistance with this research project.

If you have other questions about this study or survey,
please contact Scott Boss at scboss@katz.pitt.edu

Appendix D

E-MAIL MESSAGES SENT TO RESPONDENTS

The following are the e-mail messages sent to participants of the pilot test and the main data collection.

D.1 PILOT TEST INVITATION AND REMINDER E-MAIL MESSAGES

D.1.1 Invitation to Participate E-mail From Management

Subject: Take ISD's Security Survey--Win a Free iPod!

In order to better understand the current level of IT security awareness within our organization, ISD's IT Security Team is working with the Katz School of Business to conduct a security awareness survey.

All members of ISD are encouraged to take this on-line security survey, using a web site created by the Katz School of Business and the Legacy Alliance research firm. The survey takes about 10 minutes to complete.

Your survey choices are entirely confidential. Each member of ISD will shortly receive an e-mail with instructions and a login ID to access the on-line survey. As this is a blind survey, your answers will not be associated with your name.

Those completing the security survey will be entered into a drawing for a free Apple iPod Shuffle.

The security survey starts November 1, and closes November 14.

If you have any questions, please contact Matt Tolbert.

D.1.2 Invitation to Participate E-mail From the Trusted 3rd Party

Subject: ISD Computer Security Survey – Response Requested

In order to more effectively understand the perceptions of security policies and procedures at the University of Pittsburgh, we are conducting a Computer Security Survey for the ISD department.

The assessment takes approximately 15 minutes to complete. Please begin the assessment when you can work on it uninterrupted.

This is a confidential assessment. You will be given a login ID below which will allow us to control access to the survey, to track the survey responses and to send reminder messages only to those who have not responded. Your name and login ID are in no way associated with the feedback or the report. Your ID is used for data integrity purposes only and is kept strictly confidential within Legacy Alliance.

You can access the instrument through the following link:

http://www.legacysurveys.com/asmt/security/security2.htm

Your login id is <CUSTOMIZED ID PLACED HERE>.

If clicking on the above link does not work, copy it and then paste it into the address field of your web browser.

The last day to participate will be November 14, 2005

If you have any questions or difficulties, please respond to this e-mail.

Thank you,

D.1.3 First Reminder E-Mail

Subject: ISD Computer Security Survey – Response Requested

Reminder: There is only XX days left to complete the Computer Security Survey. Please click on the link below to begin the survey.

[The customized Invitation to Participate E-mail From the Trusted 3rd Party (above) was added to this message]

D.2 FULL DATA COLLECTION INVITATION AND REMINDER E-MAIL MESSAGES

D.2.1 Invitation to Participate E-mail From Management

From: Ingo [Name Withheld], President and CEO

Subject: Computer Security Survey

As I'm sure all of you are aware, we have been working to implement state-of-the-art computer systems here at SEMC to help us provide exceptional care for our patients as well as to increase our efficiency. With these new systems, we find that we have additional concerns regarding computer security and patient privacy that were not relevant to a non-computer environment. Also, Congress has passed several laws requiring that we provide a secure environment for computerized patient records with extremely harsh penalties for groups who do not do all that they can to ensure patient confidentiality.

To better understand the risk we face, we are conducting a computer security survey here at SEMC. We are targeting the groups at SEMC with the most exposure to computers to help us understand how we can provide a safer "electronic" environment.

Lastly, I know surveys take time and that some are suffering from "survey burnout". To recognize this, we have made the survey as short as possible.

It will take about 15 minutes to complete the survey, and you will be paid for the time it takes to fill it out. As a token of our appreciation, a fully completed survey will automatically make you eligible to win one of three $1,500 Dell laptop computers.

Thank you for helping to make us better!

To begin the survey, please click here:

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

D.2.2 First Reminder E-Mail

Subject: Computer Security Survey

Reminder: There are only 10 days left to complete the Computer Security Survey and be entered into the drawing to win one of three laptop computers.

Please click on the link below to begin the survey.

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

[The Invitation to Participate E-mail From the CEO (above) was added to this message]

D.2.3 Second Reminder E-Mail

Subject: Reminder: Computer Security Survey

Reminder: There are only 4 days left to complete the Computer Security Survey and be entered into the drawing to win one of three laptop computers.

Please click on the link below to begin the survey.

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

[The Invitation to Participate E-mail From the CEO (above) was added to this message]

D.2.4 Third (FINAL) Reminder E-Mail

Subject: Final Reminder: Computer Security Survey

Reminder: Today (May 22, 2006) is the last day to complete the Computer Security Survey and be entered into the drawing to win one of three laptop computers. The survey will close tonight at 12:00 pm.

Please note that if you have "paused" or "saved" your survey it is incomplete and you will not be eligible for the drawing.

Please click on the link below to begin the survey.

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

[The Invitation to Participate E-mail From the CEO (above) was added to this message]

D.2.5 Data Collection Extension E-Mail – Sent by the Organization Administration

Subject: Good News – Survey Deadline Extended

If you haven't already responded to the Computer Security Survey, the administration has decided to extend the deadline to complete the survey from tonight to the day after Memorial Day (Tuesday, May 30th). You still have the chance to win one of the three (3) $1,500 Dell Laptop Computers.

If you have already completed the survey, thank you for your participation. You have been automatically entered into the drawing for the computers.

Please click on the link below to begin the survey.

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

[The Invitation to Participate E-mail From the CEO (above) was added to this message]

D.2.6 Fourth Reminder E-Mail

Subject: Only 5 days left

Reminder: There are only 5 days left to complete the Computer Security Survey and be entered into the drawing to win one of three $1,500 laptop computers. The survey will end this coming Tuesday.

Please click on the link below to begin the survey.

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

[The Invitation to Participate E-mail From the CEO (above) was added to this message]

D.2.7 Fifth (Actual Final) Final Reminder E-Mail

Subject: Last Chance!

You have one last chance to be entered to win one of three (3) fully loaded Dell Laptop Computers. Today (May 30, 2006) is the last day to complete the Computer Security Survey. Finishing the survey automatically enters you into the drawing.

The survey will close tonight at 11:59 pm. (Midnight)

Please note that if you have "paused" or "saved" your survey it is incomplete and you will not be eligible for the drawing.

Please click on the link below to begin the survey.

http://www.legacysurveys.com/SEMC/Security/SEMCsecurity.htm

[The Invitation to Participate E-mail From the CEO (above) was added to this message]

Appendix E

CONTROL VARIABLE CONSTRUCTS

The following are additional constructs added after the pretest based on the theory described in the main text body. The two control variables added are Computer Self Efficacy (CSE) and Apathy..

E.1 COMPUTER SELF EFFICACY CONSTRUCT

This section is intended to measure how you feel about unfamiliar software. It is not intended to reflect how SEMC presents software to you. Hypothetically, organizations present new software packages to us or systems to make work easier. For the following section, imagine that you were given a new software package for some aspect of your work. It doesn't matter specifically what this software package does, only that it is intended to make your job easier and that you have never used it before.

The following questions ask you to indicate whether you could use this unfamiliar software package under a variety of conditions. For each condition please rate your confidence about your judgment, by circling a number from 1 to 7, where 1 indicates "Not at all confident," 4 indicates "Moderately confident," and 7 indicates "Totally confident."

This section asks you about your ability to use an unfamiliar piece of software.

I could complete my job using the software package . . .

	Not at all Confident				Moderately Confident		Totally Confident
... if there was no one around to tell me what to do.	1	2	3	4	5	6	7
... if I had never used a package like it before.	1	2	3	4	5	6	7
... if I had only the software manuals for reference.	1	2	3	4	5	6	7
... if I had seen someone else using it before trying it myself.	1	2	3	4	5	6	7
... if I could call someone for help if I got stuck.	1	2	3	4	5	6	7
... if someone else helped me get started.	1	2	3	4	5	6	7
... if I had a lot of time to complete the job for which the software was provided.	1	2	3	4	5	6	7
... if I had just the built-in help facility for assistance.	1	2	3	4	5	6	7
... if someone showed me how to do it first.	1	2	3	4	5	6	7
... if I had used similar packages like this one before to do the job.	1	2	3	4	5	6	7

E.2 APATHY CONSTRUCT

Please indicate the degree to which you agree or disagree with the following statements about security:

	Strongly Disagree			Neutral			Strongly Agree
My computer doesn't have anything on it worth stealing.	1	2	3	4	5	6	7
It is not really important for me to be aware of security.	1	2	3	4	5	6	7
Someone in Information Systems takes care of security problems.	1	2	3	4	5	6	7
I pay attention when people talk about computer security.	1	2	3	4	5	6	7
Paying attention to security takes too much time.	1	2	3	4	5	6	7
I'm too busy to be bothered by information security concerns.	1	2	3	4	5	6	7

Appendix F

DATA RECODING FREQUENCIES

The following are the frequencies of the Experience and Impact items from the data collection showing both before (b) and after (a) re-coding the impact items along with any explanatory notes (if needed).

Dir01

	Experience	Impact (b)	Impact (a)	Notes
Yes	384			
No	1,274			
Missing	39	1,158	51	12 people who said yes to the experience question didn't answer the Impact question
0			1,274	
1		93	8	
2		21	12	
3		22	16	
4		65	51	
5		51	45	
6		86	71	
7		201	169	

Dir02

	Experience	Impact (b)	Impact (a)	Notes
Yes	29			
No	1,627			
Missing	41	1,481	48	7 people who said yes to the experience question didn't answer the Impact question
0			1,627	
1		99	0	
2		13	1	

3		8	3	
4		20	3	
5		8	4	
6		11	0	
7		57	11	

Dir03

	Experience	**Impact (b)**	**Impact (a)**	**Notes**
Yes	1,531			
No	119			
Missing	47	1,417	54	7 people who said yes to the experience question didn't answer the Impact question
0			1,531	
1		88	2	
2		11	1	
3		7	2	
4		32	17	
5		17	14	
6		36	24	
7		89	52	

Dir04

	Experience	**Impact (b)**	**Impact (a)**	**Notes**
Yes	1,548			
No	109			
Missing	40	1,425		7 people who said yes to the experience question didn't answer the Impact question
0			1,548	
1		90	3	
2		8	1	
3		6	1	
4		23	10	
5		10	6	
6		24	16	
7		111	65	

Dir05

	Experience	Impact (b)	Impact (a)	Notes
Yes	192			
No	1,457			
Missing	48	1,365	64	16 people who said yes to the experience question didn't answer the Impact question
0			1,457	
1		82	5	
2		10	1	
3		11	5	
4		25	15	
5		31	22	
6		43	32	
7		130	96	

Dir06

	Experience	Impact (b)	Impact (a)	Notes
Yes	274			
No	1,380			
Missing	43	1,278	57	14 people who said yes to the experience question didn't answer the Impact question
0			1,380	
1		69	3	
2		17	8	
3		33	26	
4		46	33	
5		59	46	
6		68	51	
7		127	93	

Dir07

	Experience	Impact (b)	Impact (a)	Notes
Yes	189			
No	1,456			
Missing	52	1,364	65	13 people who said yes to the experience question didn't answer the Impact question
0			1,456	
1		84	5	
2		18	9	
3		13	7	
4		36	22	
5		29	24	
6		48	36	
7		105	73	

Dir08

	Experience	Impact (b)	Impact (a)	Notes
Yes	205			
No	1,429			
Missing	63	1,357	75	12 people who said yes to the experience question didn't answer the Impact question
0			1,429	
1		82	5	
2		17	8	
3		11	8	
4		40	27	
5		31	25	
6		42	31	
7		117	89	

Dir09

	Experience	Impact (b)	Impact (a)	Notes
Yes	1,571			
No	67			
Missing	59	1,473	70	11 people who said yes to the experience question didn't answer the Impact question
0			1,571	
1		82	1	
2		13	3	
3		5	0	
4		14	2	
5		9	5	
6		20	8	
7		81	37	

Indr01

	Experience	Impact (b)	Impact (a)	Notes
Yes	918			
No	704			
Missing	75	662	96	21 people who said yes to the experience question didn't answer the Impact question
0			704	
1		64	6	
2		15	11	
3		33	26	
4		147	131	
5		141	130	
6		215	204	
7		420	389	

Indr02

	Experience	Impact (b)	Impact (a)	Notes
Yes	305			
No	1,315			
Missing	77	1,124	87	10 people who said yes to the experience question didn't answer the Impact question
0			1,315	
1		110	4	
2		16	4	
3		11	4	
4		46	19	
5		39	20	
6		91	57	
7		260	187	

Indr03

	Experience	Impact (b)	Impact (a)	Notes
Yes	574			
No	1,045			
Missing	78	938	94	16 people who said yes to the experience question didn't answer the Impact question
0			1,045	
1		84	6	
2		14	6	
3		16	9	
4		61	42	
5		78	65	
6		162	142	
7		344	288	

Indr04

	Experience	Impact (b)	Impact (a)	Notes
Yes	811			
No	813			
Missing	73	765	99	26 people who said yes to the experience question didn't answer the Impact question
0			813	
1		70	11	
2		13	7	
3		14	8	
4		29	25	
5		37	31	
6		124	112	
7		645	591	

Indr05

	Experience	Impact (b)	Impact (a)	Notes
Yes	705			
No	908			
Missing	84	857	110	26 people who said yes to the experience question didn't answer the Impact question
0			908	
1		67	11	
2		16	7	
3		18	15	
4		66	45	
5		92	79	
6		179	164	
7		402	358	

Indr06

	Experience	Impact (b)	Impact (a)	Notes
Yes	607			
No	1,012			
Missing	78	923	99	21 people who said yes to the experience question didn't answer the Impact question
0			1,012	
1		74	15	
2		21	6	
3		27	17	
4		79	54	
5		114	97	
6		165	150	
7		294	247	

Indr07

	Experience	Impact (b)	Impact (a)	Notes
Yes	788			
No	826			
Missing	83	797	108	25 people who said yes to the experience question didn't answer the Impact question
0			826	
1		63	13	
2		17	7	
3		18	14	
4		85	76	
5		115	109	
6		217	197	
7		385	347	

Indr08

	Experience	Impact (b)	Impact (a)	Notes
Yes	807			
No	798			
Missing	92	783	118	26 people who said yes to the experience question didn't answer the Impact question
0			798	
1		59	10	
2		22	11	
3		23	19	
4		82	70	
5		113	106	
6		204	189	
7		411	376	

Indr09

	Experience	Impact (b)	Impact (a)	Notes
Yes	533			
No	1,082			
Missing	82	998	117	35 people who said yes to the experience question didn't answer the Impact question
0			1,082	
1		75	11	
2		23	9	
3		19	12	
4		61	40	
5		49	40	
6		114	93	
7		358	293	

Appendix G

USER ID'S OF DROPPED CASES

Dropped Case ID's
4741
4827
5638
5708
6443
8126
8575
9042
9412
9774
10040
10079
10489
10996
11221
11393
11504
11584
12636
12998
13079
13710
13825
13923
14232

Dropped Case ID's
14297
14777
14863
14992
15490
15980
16363
16492
16498
16610
16892
17280
17616
17798
17888
17997
18474
18495
18760
18895
18928
18994
19017
19216
19764

Dropped Case ID's
20549
20593
20905
21232
21464
21524
21602
21667
21701
21808
22186
22669
22964
23072
23087
23165
23199
23255
23427
23468
23621
23794
23810
23824
24070

Dropped Case ID's
24352
24425
24520
24741
24754
25430
25494
25622
26186
26225
26436
26582
26644
26664
26811
26836
26993
27075
27414
27921
28112
50360
60699

Appendix H

FORMATIVE CONSTRUCT VALIDITY TESTS

Loch et al. (2003) propose two validation tests for formative measures where multiple methods for measuring constructs (Straub et al., 2004) is not feasible: It is possible to compare the scale items based on the properties of formative constructs and data generated from the PLS analysis. PLS weights for formative items are roughly analogous to loadings for reflective items. A weighted score (indicator) for each formative measure can be created by multiplying each item by its' PLS weight. A construct score is then created by summing the weighted score by case. The convergent and discriminant validity tests are then followed in the standard way where individual measures should correlate significantly with their construct value to show convergent validity and inter-item and item-to-construct correlations should correlate more highly with each other than with the items of the other constructs or the other constructs themselves show discriminant validity. The results of this analysis are shown below in Table 46.

Table 46 – Formative Construct Correlations

	Direct	Indirect	Risk	Risk – Likelihood	Risk – Impact
Dir01	**0.75**	0.34	0.21	0.20	0.19
Dir02	**-0.19**	-0.10	-0.02	-0.02	-0.05
Dir03	**0.70**	0.22	0.22	0.21	0.21
Dir04	**0.24**	0.15	0.09	0.09	0.08
Dir05	**0.82**	0.26	0.24	0.22	0.21
Dir06	**0.69**	0.38	0.19	0.19	0.19
Dir07	**0.58**	0.27	0.17	0.16	0.15
Dir08	**0.61**	0.27	0.17	0.19	0.18
Dir09	**-0.28**	-0.14	-0.10	-0.11	-0.11
Indr01	0.33	**0.81**	0.22	0.21	0.20
Indr02	-0.16	**-0.34**	-0.07	-0.07	-0.09
Indr03	0.31	**0.67**	0.17	0.16	0.17
Indr04	0.23	**0.59**	0.15	0.15	0.15
Indr05	0.34	**0.71**	0.19	0.19	0.19
Indr06	0.39	**0.76**	0.20	0.20	0.21
Indr07	-0.34	**-0.66**	-0.17	-0.18	-0.18
Indr08	0.33	**0.80**	0.20	0.20	0.20
Indr09	-0.19	**-0.46**	-0.13	-0.15	-0.15
Risk01	0.23	0.18	**0.76**	0.80	0.80
Risk02	-0.20	-0.17	**-0.69**	-0.70	-0.80
Risk03	0.25	0.22	**0.86**	0.82	0.86
Risk04	0.19	0.20	**0.75**	0.70	0.67
Risk05	0.24	0.19	**0.83**	0.80	0.76
Risk06	0.24	0.22	**0.84**	0.86	0.82
Risk07	0.23	0.18	**0.76**	0.78	0.69
Risk08	0.21	0.21	**0.77**	0.83	0.86
Risk09	-0.14	-0.14	**-0.53**	-0.68	-0.65
Risk01L	0.23	0.18	0.76	**0.80**	0.80
Risk02L	-0.20	-0.17	-0.69	**-0.70**	-0.80
Risk03L	0.25	0.22	0.86	**0.82**	0.86
Risk04L	0.19	0.20	0.75	**0.70**	0.67
Risk05L	0.24	0.19	0.83	**0.80**	0.76
Risk06L	0.24	0.22	0.84	**0.86**	0.82
Risk07L	0.23	0.18	0.76	**0.78**	0.69
Risk08L	0.21	0.21	0.77	**0.83**	0.86
Risk09L	0.14	0.14	0.53	**0.68**	0.65
Risk01IM	0.23	0.18	0.76	0.80	**0.80**
Risk02IM	0.20	0.17	0.69	0.70	**0.80**

	Direct	Indirect	Risk	Risk – Likelihood	Risk – Impact
Risk03IM	0.25	0.22	0.86	0.82	**0.86**
Risk04IM	0.19	0.20	0.75	0.70	**0.67**
Risk05IM	-0.24	-0.19	-0.83	-0.80	**-0.76**
Risk06IM	0.24	0.22	0.84	0.86	**0.82**
Risk07IM	-0.23	-0.18	-0.76	-0.78	**-0.69**
Risk08IM	0.21	0.21	0.77	0.83	**0.86**
Risk09IM	0.14	0.14	0.53	0.68	**0.65**

The analysis showed that items loaded significantly with their intended construct (the only item that wasn't significantly correlated in the table above was Dir02 with Risk) showing convergent validity. Discriminant validity is shown by the highest correlation (either positive or negative) with the intended construct. Note that there are high loadings (in some cases higher than with the intended construct) between Risk and Risk-Likelihood and Risk-Impact. This is because Risk is a score derived from Risk-Likelihood and Risk-Impact.

Appendix I

POST-HOC ANALYSIS FOR REFLECTIVE CONSTRUCT MEAN DIFFERENCES

The following are the results of an one-way ANOVA analysis using employee status (full vs. part-time) as the factor for all of the reflective constructs.

Variable	Factor	N	Mean	Standard Deviation
Specification	Part Time	4.92	1.19	4.92
	Full Time	5.24	1.24	5.24
	Difference	**0.32*** **		
Evaluation	Part Time	4.38	1.40	4.38
	Full Time	4.36	1.54	4.36
	Difference	-0.02		
Reward	Part Time	3.29	1.30	3.29
	Full Time	3.31	1.43	3.31
	Difference	0.01		
Mandatoriness	Part Time	5.29	1.14	5.29
	Full Time	5.46	1.14	5.46
	Difference	0.17		
Precautions	Part Time	5.44	1.09	5.44
	Full Time	5.56	1.08	5.56
	Difference	0.11		
CSE	Part Time	5.14	1.13	5.14
	Full Time	5.18	1.15	5.18
	Difference	0.03		
Apathy	Part Time	2.16	1.23	2.16
	Full Time	2.10	1.11	2.10
	Difference	-0.06		

*** p>0.001

The only significant difference between the full and part-time employees is in the degree to which individuals feel that the security policies and procedures are sufficiently specified.

BIBLIOGRAPHY

Abbey, A. (1982). *Technological Innovation: R&D Work Environment*. Unpublished manuscript, Ann Arbor, MI.

Adler, P. S., & Borys, B. (1996). Two types of bureaucracy: Enabling and coercive. *Administrative Science Quarterly, 41*(1), 61-89.

Ahlbrecht, M., & Weber, M. (1997). An empirical study on intertemporal decision making under risk. *Management Science, 43*(6), 813-826.

Aiken, M. S., & Hage, J. (1968). Organizational interdependence and intraorganizational structure. *American Sociological Review, 33*, 912-930.

America Online, & National Cyber Security Alliance. (2004). *AOL/NCSA Online Safety Study*. Dulles, Virginia: National Cyber Security Alliance, Time Warner Inc.

America Online, & National Cyber Security Alliance. (2005). *AOL/NCSA Online Safety Study*. Dulles, Virginia: National Cyber Security Alliance, Time Warner Inc.

American National Standards Institute. (2005). ISO ICS 35 Information Technology. Retrieved April, 2005, from http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=330

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 100*(3), 411 - 423.

Anti-Phishing Working Group. (2007). Phishing Activity Trends, Report for the Month of March, 2007. Retrieved May 19, 2007

Armstrong, J. S., & Overton, T. S. (1977). Estimating Nonresponse Bias in Mail Surveys. *Journal of Marketing Research, 14*(3), 396-402.

Associated Press. (2004). New Microsoft security flaws found. Retrieved August 20, 2004, from http://www.abc.net.au/news/newsitems/200408/s1181192.htm

Barki, H., Rivard, S., & Talbot, J. (1992). Risk Assessment of an Information-System Development Project. *Revue Canadienne Des Sciences De L Administration-Canadian Journal of Administrative Sciences, 9*(3), 213-228.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems, 17*(4), 37-69.

Baron, R. M., & Kenny, D. A. (1986). The Moderator Mediator Variable Distinction in Social Psychological-Research - Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology, 51*(6), 1173-1182.

Blumstein, A. (1978). Introduction. In A. Blumstien, J. Cohen & D. Nagin (Eds.), *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*. Washington, DC: National Academy of Sciences.

Bollen, K., & Lennox, R. (1991). Conventional Wisdom on Measurement - a Structural Equation Perspective. *Psychological Bulletin, 110*(2), 305-314.

Boss, S. R., Butler, B. S., & Frieze, I. H. (2005). *Exposure to and Fear of Cybercrime: Do You Look Over Your Shoulder in Cyberspace?* Unpublished manuscript, Pittsburgh, PA.

Campbell, C. M. (2000, Oct 2000). Hacking rises despite increased security spending. Retrieved Jan 29, 2005

Cardinal, L. B. (2001). Technological innovation in the pharmaceutical industry: The use of organizational control in managing research and development. *Organization Science, 12*(1), 19-36.

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment*. Beverly Hills, Calif.: Sage Publications.

CERT Coordination Center. (2004a, May 25, 2004). 2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes. Retrieved August 20, 2004, from http://www.cert.org/about/ecrime.html

CERT Coordination Center. (2004b). CERT/CC Statistics 1988 - 2004 [Web Page]. Pittsburgh, PA: Carnegie Mellon University.

Chae, B., & Poole, M. S. (2005). Mandates and technology acceptance: A tale of two enterprise technologies. *Journal of Strategic Information Systems, 14*(2), 147-166.

Statement of Michael Chertoff Assistant Attorney General, Criminal Division, U.S. Department Of Justice before the Subcommittee on Crime Committee on the Judiciary U.S. House of Representatives, (2001).

Chin, S. K. (1999). High-confidence design for security. *Communications of the ACM, 42*(7), 33-37.

Chin, W. W. (1998a). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), Vii-Xvi.

Chin, W. W. (1998b). The partial least squares approach for structural equation modelling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. viii, 437 p.). Mahwah, N.J.: Lawrence Erlbaum.

Chin, W. W., & Gopal, A. (1995). Adoption Intention in GSS - Relative Importance of Beliefs. *Data Base for Advances in Information Systems, 26*(2-3), 42-64.

Choudhury, V., & Sabherwal, R. (2003). Portfolios of control in outsourced software development projects. *Information Systems Research, 14*(3), 291-314.

Chow, C. W., Hirst, M., & Shields, M. D. (1995). The effects of pay schemes and probabilistic management audits on subordinate misrepresentation of private information: An experimental investigation in a resource allocation context. *Behavioral Research in Accounting, 7*, 1 - 15.

Clarke, L. (1993). The disqualification heuristic: When do organizations misperceive risk? *Research in Social Problems and Public Policy, 5*, 289-312.

Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy - Development of a Measure and Initial Test. *MIS Quarterly, 19*(2), 189-211.

Coren, M. (2005, Jan 24). Experts: Cyber-crime bigger threat than cyber-terror. Retrieved Jan 26, 2005

Cote, J. A., & Buckley, M. R. (1987). Estimating Trait, Method, and Error Variance - Generalizing across 70 Construct-Validation Studies. *Journal of Marketing Research, 24*(3), 315-318.

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

Cryer, J. D., & Miller, R. B. (1991). *Statistics for business : data analysis and modelling*. Boston: PWS-Kent.

D'Aquila, J. M. (2001). Financial accountants' perceptions of management's ethical standards. *Journal of Business Ethics, 31*(3), 233-244.

Daft, R. L., & Macintosh, N. B. (1981). A Tentative Exploration into the Amount and Equivocality of Information-Processing in Organizational Work Units. *Administrative Science Quarterly, 26*(2), 207-224.

Dale, M., & The Associated Press. (2006, May 2, 2006). Verizon could offer settlements over blocked e-mails. Retrieved May 2, 2006

Das, T. K., & Teng, B. S. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review, 23*(3), 491-512.

Deephouse, C., Mukhopadhyay, T., Goldenson, D. R., & Kellner, M. I. (1995). Software processes and project performance. *Journal of Management Information Systems, 12*(3), 187-205.

Dewar, R., & Werbel, J. (1979). Universalistic and Contingency Predictions of Employee Satisfaction and Conflict. *Administrative Science Quarterly, 24*(3), 426-448.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dopuch, N., Birnberg, J. G., & Demski, J. S. (1982). *Cost accounting: accounting data for management's decisions* (3rd ed.). New York: Harcourt Brace Jovanovich.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-+.

Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31*(2), 134-149.

Eisenhardt, K. M. (1988). Agency-Theory and Institutional-Theory Explanations - the Case of Retail Sales Compensation. *Academy of Management Journal, 31*(3), 488-511.

Feldman, R. S. (1998). *Social psychology* (2nd ed.). Upper Saddle River, N.J.: Prentice Hall.

Fernandes, A. D. (2001). Risking "trust" in a public key infrastructure: old techniques of managing risk applied to new technology. *Decision Support Systems, 31*(3), 303-322.

Finne, T. (1998). A conceptual framework for information security management. *Computers & Security, 17*(4), 303-307.

Finne, T. (2000). Information systems risk management: Key concepts and business processes. *Computers & Security, 19*(3), 234-242.

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

Fowler, F. J. (2002). *Survey research methods* (3rd ed.). Thousand Oaks, Calif.: Sage Publications.

Frederickson, J. R., & Waller, W. (2005). Carrot or stick? Contract frame and use of decision-influencing information in a principal-agent setting. *Journal of Accounting Research, 43*(5), 709-733.

Frieze, I. H., Hymer, S., & Greenberg, M. S. (1987). Describing the crime victim: psychological reactions to victimization. *Professional Psychology: Research and Practice, 18*(4), 299 - 315.

Garfinkel, R., Gopal, R., & Goes, P. (2002). Privacy protection of binary confidential data against deterministic, stochastic, and insider threat. *Management Science, 48*(6), 749-764.

Garfinkel, S., Spafford, G., & Schwartz, A. (2003). *Practical UNIX and Internet security* (3rd ed.). Beijing ; Sebastopol, CA: O'Reilly.

Gattiker, U. E., & Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research, 10*(3), 233-254.

Germain, J. M. (2007, March 28). TraceSecurity CTO Jim Stickley: Robbing Banks With Impunity. Retrieved May 19, 2007, from http://www.technewsworld.com/story/56547.html

Gray, P. H., & Meister, D. B. (2004). Knowledge sourcing effectiveness. *Management Science, 50*(6), 821-834.

GRIDtoday. (2006, Nov 20). IT Security Spending to Hit $61 Billion for 2006, says Info-Tech. Retrieved May 21, 2007

Hall, R. H. (1968). Professionalization and bureaucratization. *American Sociological Review, 33*, 92-104.

Han, P. (2004). *Development and validation of a scale to measure concern about cancer risk*. Unpublished manuscript, Pittsburgh, PA.

Hanson, R. F., Smith, D. W., Kilpatrick, D. G., & Freedy, J. R. (2000). Crime-related fears and demographic diversity in Los Angeles County after the 1992 civil disturbances. *Journal of Community Psychology, 28*(6), 607-623.

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.

Hartwick, J., & Barki, H. (1994). Explaining the Role of User Participation in Information-System Use. *Management Science, 40*(4), 440-465.

Hastings, A., & Dean, J. (2003). Challenging images: tackling stigma through estate regeneration. *Policy and Politics, 31*(2), 171-184.

Hone, K., & Eloff, J. H. P. (2002). Information security policy - what do international information security standards say? *Computers & Security, 21*(5), 402-409.

Hughes, L. A., & DeLone, G. J. (2007). Viruses, worms, and Trojan horses - Serious crimes, nuisance, or both? *Social Science Computer Review, 25*(1), 78-98.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195-204.

Ivancevich, J. M. (1983). Contrast effects in performance evaluation and reward practices. *Academy of Management Journal, 26*, 465 - 476.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Jaworski, B. J. (1988). Toward a Theory of Marketing Control: Environmental Context, Control Types, and Consequences. *Theory of Marketing Control, 52*, 23 - 39.

Jèoreskog, K. G., & Wold, H. O. A. (1982). *Systems under indirect observation : causality, structure, prediction*. Amsterdam ; New York, New York: North-Holland Press.

Jia, J. M., & Dyer, J. S. (1996). A standard measure of risk and risk-value models. *Management Science, 42*(12), 1691-1705.

Jia, J. M., Dyer, J. S., & Butler, J. C. (1999). Measures of perceived risk. *Management Science, 45*(4), 519-532.

Kappelman, L. A., & McLean, E. R. (1994). *User engagement in the development, implementation, and use of information technologies.* Paper presented at the Twenty-Seventh Hawaii International Conference on System Sciences, Maui, HI.

Karahanna, E., & Straub, D. W. (1999). The psychological origins of perceived usefulness and ease-of-use. *Information & Management, 35*(4), 237-250.

Kendall, K. (1999). *A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems.* Unpublished Dissertation, Massachusetts Institute of Technology, Boston, MA.

Kirsch, L. J. (1996). The Management of Complex Tasks in Organizations: Controlling the Systems Development Process. *Organization Science, 7*(1), 1-21.

Kirsch, L. J. (1997). Portfolios of control modes and IS project management. *Information Systems Research, 8*(3), 215-239.

Kirsch, L. J. (2000). Software Project Management: An Integrated Perspective for an Emerging Paradigm. In R. W. Zmud (Ed.), *Framing the Domains of IT Management: Projecting the Future ... Through the Past* (pp. 285 - 304). Cincinnati, OH: Pinnaflex Educational Resources.

Kirsch, L. J. (2004). Deploying common solutions globally: The dynamics of control. *Information Systems Research, 15*(4), 374-395.

Kirsch, L. J., & Cummings, L. L. (1996). Contextual influences on self-control of IS professionals engaged in systems development. *Accounting, Management, & Information Technology, 6*(3), 191-219.

Kirsch, L. J., Sambamurthy, V., Ko, D. G., & Purvis, R. L. (2002). Controlling information systems development projects: The view from the client. *Management Science, 48*(4), 484-498.

Koberg, C. S. (1988). Dissimilar Structural and Control Profiles of Educational and Technical Organizations. *Journal of Management Studies, 25*(2), 121-130.

Kopelman, R. E. (1976). Organizational control responsiveness, expectancy theory constructs, and work motivation. *Personnel Psychology, 29*, 205 - 220.

Kren, L. (1990). Performance in a Budget-Based Control System: An Extended Expectancy Theory Model Approach. *Journal of Management Accounting Research, 2*, 100 - 112.

Law, K. S., Wong, C. S., & Mobley, W. H. (1998). Toward a taxonomy of multidimensional constructs. *Academy of Management Review, 23*(4), 741-755.

Lawler, E. E. (1981). *Pay and organization development*. Reading, Mass.: Addison-Wesley Pub. Co.

Levi, M. (2001). Business, cities and fears about crimes. *Urban Studies, 38*(5-6), 849-868.

Lim, V. K. G., Teo, T. S. H., & Loo, G. L. (2002). How do I loaf here? Let me count the ways. *Communications of the ACM, 45*(1), 66-70.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114-121.

Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and technological culturation. *IEEE Transactions on Engineering Management, 50*(1), 45-63.

Lorange, P., & Scott-Morton, M. S. (1974). A Framework for Management Control Systems. *Sloan Management Review, 16*(1), 47 - 56.

Luft, J. (1994). Bonus and Penalty Incentives Contract Choice by Employees. *Journal of Accounting & Economics, 18*(2), 181-206.

Luo, X. M. (2002). Trust production and privacy concerns on the Internet - A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*(2), 111-118.

Mangione, T. W. (1995). *Mail surveys : improving the quality*. Thousand Oaks, Calif.: Sage Publications.

McCoy, H. V., Wooldredge, J. D., Cullen, F. T., Dubeck, P. J., & Browning, S. L. (1996). Lifestyles of the old and not so fearful: Life situation and older persons' fear of crime. *Journal of Criminal Justice, 24*(3), 191-205.

Mercuri, R. T. (2002). Security watch - Computer security: Quality rather than quantity. *Communications of the ACM, 45*(10), 11-14.

Milgram, S. (1974). *Obedience to authority; an experimental view* (1st ed.). New York,: Harper & Row.

Muralidhar, K., Batra, D., & Kirs, P. J. (1995). Accessibility, Security, and Accuracy in Statistical Databases - the Case for the Multiplicative Fixed Data Perturbation Approach. *Management Science, 41*(9), 1549-1564.

Muralidhar, K., Sarathy, R., & Parsa, R. (2001). An improved security requirement for data perturbation with implications for e-commerce. *Decision Sciences, 32*(4), 683-698.

Naraine, R. (2006, April 10, 2006). Return of the Web Mob. *eWeek.com* Retrieved April 25, 2006

National Cyber Security Alliance. (2005). Top Ten Cybersecurity Tips. Retrieved Mar 28, 2005, from http://www.staysafeonline.info/home-tips.html

Neter, J., Wasserman, W., & Kutner, M. H. (1990). *Applied linear statistical models : regression, analysis of variance, and experimental designs* (3rd ed.). Homewood, IL: Irwin.

Nidumolu, S. R. (1995). The Effect of Coordination and Uncertainty on Software Project Performance - Residual Performance Risk as an Intervening Variable. *Information Systems Research, 6*(3), 191-219.

Nidumolu, S. R., & Subramani, M. R. (2003). The matrix of control: Combining process and structure approaches to managing software development. *Journal of Management Information Systems, 20*(3), 159-196.

Nunnally, J. C. (1978). *Psychometric theory* (2d ed.). New York: McGraw-Hill.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York: McGraw-Hill.

Oreilly, C. A., & Weitz, B. A. (1980). Managing Marginal Employees - the Use of Warnings and Dismissals. *Administrative Science Quarterly, 25*(3), 467-484.

Ouchi, W. G. (1977). Relationship between Organizational-Structure and Organizational Control. *Administrative Science Quarterly, 22*(1), 95-113.

Ouchi, W. G. (1978). Transmission of Control through Organizational Hierarchy. *Academy of Management Journal, 21*(2), 173-192.

Ouchi, W. G. (1979). Conceptual-Framework for the Design of Organizational Control Mechanisms. *Management Science, 25*(9), 833-848.

Ouchi, W. G. (1980). Markets, Bureaucracies, and Clans. *Administrative Science Quarterly, 25*, 129 - 141.

Ouchi, W. G., & Maguire, M. A. (1975). Organizational Control - 2 Functions. *Administrative Science Quarterly, 20*(4), 559-569.

Pain, R. (2000). Place, social relations and the fear of crime: a review. *Progress in Human Geography, 24*(3), 365-387.

Pain, R. (2001). Gender, race, age and fear in the city. *Urban Studies, 38*(5-6), 899-913.

Parker, K. D., McMorris, B. J., Smith, E., & Murty, K. S. (1993). Fear of Crime and the likelihood of victimization - A bi-ethnic comparison. *Journal of Social Psychology, 133*(5), 723-732.

Pearson, F. S., & Weiner, N. A. (1985). Toward an Integration of Criminological Theories. *Journal of Crime and Criminology, 76*(1), 116 - 150.

Piccoli, G., & Ives, B. (2003). Trust and the unintended effects of behavior control in virtual teams. *MIS Quarterly, 27*(3), 365-395.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

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

Prakash, P., & Rappaport, A. (1975). Informational Interdependencies - System Structure Induced by Accounting Information. *Accounting Review, 50*(4), 723-734.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM, 46*(7), 101-106.

Rogers, L. R. (2002). Home Computer Security. Retrieved May 18, 2007, from http://www.cert.org/homeusers/HomeComputerSecurity/

Rosenthal, P. (2004). Management control as an employee resource: The case of front-line service workers. *Journal of Management Studies, 41*(4), 601-622.

Rountree, P. W., & Land, K. C. (1996). Perceived risk versus fear of crime: Empirical evidence of conceptually distinct reactions in survey data. *Social Forces, 74*(4), 1353-1376.

Sarathy, R., & Muralidhar, K. (2002). The security of confidential numerical data in databases. *Information Systems Research, 13*(4), 389-403.

Schneider, F. W., Gruman, J. A., & Coutts, L. M. (2005). *Applied social psychology : understanding and addressing social and practical problems*. Thousand Oaks, Calif.: SAGE Publications.

Skogan, W. G., & Maxfield, M. G. (1981). *Coping with crime: Individual and neighborhood reactions*. Beverly Hills: Sage Publications.

Smith, L. N., & Hill, G. D. (1991). Victimization and fear of crime. *Criminal Justice and Behavior, 18*, 217 - 239.

Stinchcombe, A. L., Adams, R., Heimer, C. A., Scheppele, K. L., Smith, T. W., & Taylor, D. G. (1980). *Crime and punishment--changing attitudes in America* (1st ed.). San Francisco: Jossey-Bass Publishers.

Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255 - 273.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for positivist research. *Communications of the ACM, 13*, 380-427.

Straub, D. W., & Collins, R. W. (1990). Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Property Rights. *MIS Quarterly, 14*(2), 143 - 156.

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

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Sturrock, S. (2005, June 16, 2005). Psycho (but not) logical fears. *Palm Beach Post, 2005*.

Swartz, J. (2005, December 29, 2006). 2005 worst year for breaches of computer security. *USA Today* Retrieved April 26, 2006

Symantec Corporation. (2004). Latest Virus Threats. Retrieved August 20, 2004, from http://securityresponse.symantec.com/avcenter/vinfodb.html#threat_list

Symantec Corporation. (2007). Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain. Retrieved May 19, 2007, from http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01

Taylor, J. W. (2005). Generating Volatility Forecasts from Value at Risk Estimates. *Management Science, 51*(5), 712-725.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561-570.

Tyler, T. R. (1980). Impact of directly and indirectly experienced events: The origins of crime-related judgments and behaviors. *Journal of Personality and Social Psychology, 39*, 13 - 28.

USDOJ. (2001). National Crime Victimization Survey.

Venaik, S., Midgley, D. F., & Devinney, T. M. (2005). Dual paths to performance: the impact of global pressures on MNC subsidiary conduct and performance. *Journal of International Business Studies, 36*(6), 655-675.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Walklate, S. L. (2001). Fearful communities? *Urban Studies, 38*(5-6), 929-939.

Waller, W. S. (1988). Slack in Participative Budgeting: The Joint Effect of a Truth Inducing Pay Scheme and Risk Preferences. *Accounting, Organizations and Society, 13*(1), 87 - 98.

Weinrath, M., & Gartrell, J. (1996). Victimization and fear of crime. *Journal of Research in Childhood Education, 11*, 187 - 197.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91-95.

Wold, H. O. A. (Ed.). (1982). *Soft Modeling: The basic design and some extensions.* Amsterdam ; New York, New York: North Holland Press.