EXAMINATION OF THE FACTORS THAT INFLUENCE TELEWORKERS' WILLINGNESS TO COMPLY WITH INFORMATION SECURITY GUIDELINES

by

Timothy Godlove

A Dissertation Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

University of Fairfax

2011

COPYRIGHT STATEMENT

EXAMINATION OF THE FACTORS THAT INFLUENCE TELEWORKERS’ WILLINGNESS TO COMPLY WITH INFORMATION SECURITY GUIDELINES

by

Timothy R. Godlove

has been approved

2011

We hereby certify that this dissertation, submitted by Timothy Godlove, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

APPROVED:

Jean Gordon, DBA	Chairperson of Dissertation Committee
Dr. Laura Pogue, Ph.D.	Dissertation Committee Member
David Lease, Ph.D.	Dissertation Committee Member

ACCEPTED AND SIGNED:

Signed _______________________05/20/2011
Jean Gordon, DBA Date
Chairperson of Dissertation Committee

Signed _______________________05/20/2011
Ken Bahn, Ph.D. Date
Dean of Doctoral Research

University of Fairfax

2011

Abstract

Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines

by
Timothy R. Godlove

2011

With the increased use of teleworkers, it is important to understand how teleworker attitudes are related to willingness to accept and follow guidelines that maintain data security in the telework environment. The objective of the study was to evaluate the application of the theory of planned behavior and the idea of subjective norms as a means of explaining teleworker compliance in using information technology (IT) security guidelines in a telework environment. A sample of 150 respondents who considered themselves formal and informal teleworkers and were eligible for membership in The Telework Exchange completed a Teleworker Security Survey. Descriptive and linear regression analyses were used to determine relationships existing between willingness to follow organizational teleworker data information security guidelines and practices. The findings of the analyses demonstrated that Personal Attitude, Social Pressure, and Sense of Control represented a weak to moderate model for explaining teleworker willingness to follow an organization's security guidelines. This study is significant to organizations with teleworkers by identifying insight on the risks of teleworkers to data security, knowledge about what they can do to protect the confidentiality and integrity of data, and the intent of teleworkers to follow security protocols in a telework environment.

Dedication

This dissertation is dedicated to my parents, who taught to me to learn everything I can, anytime I can, from anyone I can, and, to my wife Albena for her support, love, care, patience and sacrifice. I also would like to thank Major General Don Davis, USA, (Retired), Major General Walter Stewart, USA, (Retired) and Captain Larry Meacham, USN, (Retired) for their service to the country, visionary thinking, and encouragement.

I would also like to dedicate this research to the University of Fairfax's commitment to strengthen the country's cyber workforce, valuable contributions to higher education, and to an immeasurable enrichment of a number of lives.

Acknowledgements

This dissertation is not just the end of a journey that started at the University of Fairfax, but also a beginning. This accomplishment would not have been possible without the help of many individuals who guided, assisted, and supported me to fulfill my dream of getting the doctorate.

I am thankful to my dissertation advisor Dr. Jean Gordon for her valuable direction, support, and motivation. I am also thankful to Janice Orcutt for her direction, encouragement, and insights throughout the program. I appreciate the feedback given by the various faculty members who helped to improve the quality of this study. I am also thankful to the Telework Exchange who allowed me to conduct the survey via their website to collect data for this dissertation.

Finally, I acknowledge the patience, understanding, support, and motivation of my wife, Albena Godlove and the blessings and wishes of our parents and family members who really helped me to achieve this goal.

.

Table of Contents

List of Tables

List of Figures

Chapter 1

Rationale

1.1 Problem Statement

As the risks and technical challenges of telework multiply, so too does the security and cost to organizations for protecting data in this complex environment. High-capacity broadband networks have provided many advantages and benefits of the use of telework in organizations. Many of the world's most successful companies have embraced the virtual workplace because of the role telework plays as a motivator, morale booster, and environmentally friendly alternative. However, the risks, technical challenges, and cost of replicating the secure office environment limit the use of telework by some organizations (Jones, 2007).

The proliferation of mobile devices for today's telework workforce has moved a vast amount of confidential company data outside the protection of the physical office. To protect data used in the telework environment, companies face the challenge of identifying and assessing the information security risks on a continual basis as well as implementing effective information technology security controls or behavior controls to secure the data.

Given the increasing use of telework, gaining a better understanding of factors related to information security risks is important. The severity of potential risks of security breaches related to employee access to data, devices, peripherals, hardware and software, and current security measures make telework data security a relevant topic for research. One of the greatest challenges to data security faced by organizations relates to the lack of awareness of these security risks and of expertise on how to maintain data securely in a telework environment (Allenby & Roitz, 2003).

The business problems of the current study are the risks, the technical challenges, and the cost of replicating the secure office environment to organizations for protecting data in the telework environment. Organizations using teleworkers must accurately assess the risks, identify the technical challenges that could affect data security, and understand the costs involved in replicating the secure office environment in a telework environment (Allenby & Roitz, 2003). Significant or substantial research has not taken place to investigate the topic of data security in a telework environment, and this study may provide greater understanding to the limited body of knowledge on the topic than what was previously available.

1.1.1 Background

Telework, the practice of using off-site or portable computers to perform company or agency-related duties, has become increasingly prevalent in the 21st century (Antonopoulos, 2007; Kilpatrick, 2007). This ever-growing use of teleworking increases convenience and efficiency; however, telework arrangements can have significant implications for organizational data security and information technology operational strategies. The greater reliance on telework raises numerous information security concerns, including breaches of confidentiality, increased opportunities for unauthorized viewing of data, data theft, and data leakage (Kilpatrick, 2007).

Telework is on the rise, especially for government agencies. Mears (2007) reported federal employees are almost three times more likely than are private sector employees to have the option to work from home. According to Bain (2007), in the recent past, many federal teleworkers had no choice but to use their own computers and equipment, simply because government agencies could not afford to supply their teleworkers with secure, government issued models. However, increasing evidence indicates the price of the equipment is minimal compared to the cost of dangerous security leaks that occur as a result of using non-secure, unauthorized technology.

The theory of planned behavior was chosen as the theoretical framework for this research to help understand what motivating factors influence teleworkers to follow the rules of security guidelines. The theory of planned behavior indicates, “intentions (and behaviors) are a function of three basic determinants: one personal in nature, one reflecting social influence, and a third dealing with issues of control” (Ajzen, 2005, p. 118). The goal of the study was to explore the extent to which the theory of planned behavior provided an explanation of teleworkers’ motivation to comply with information security practices and policies. Based on the premises of the theory of planned behavior, “behavior can be best predicted from a person’s intention, which is an indicator of how hard people are willing to try, and how much effort people plan to exert toward performance of behavior” (Chatzisarantis, Hager, Smith, & Sage, 2006, p. 229).

The theory of planned behavior is relevant to this study because it provides insight and can be used to explain why individuals like or dislike specific behaviors and because it helps predict an individual’s intention to carry out that behavior. Understanding individuals’ intentions to comply with organization’s information security guidelines could be beneficial to organizations. Most organizations spend time and resources to provide, establish, and monitor computer security policies. If teleworkers are not keen or willing to follow the organization’s information security guidelines, these efforts are in vain. This theory helps to determine the problem being studied: What are the motivating factors that influence teleworkers' willingness to follow an organization's information security guidelines in a telework environment?

The study provides fertile ground for research due to its relevance, measurability, research potential, and timeliness as the need for flexible work arrangements continues to be an important factor of workforce management. Indeed, the question of how businesses can zero in on security breaches and increase compliance will only become more critical as technology evolves and telework becomes more common. A goal of the present study was to better understand the role of individual attitudes toward the importance of data security in a telework environment. The increase in the number of teleworkers and the frequency and scope of official and unofficial telework has exposed a vast amount of confidential organization data outside the physical office and has increased the likelihood of security breaches.

The ever-growing use of teleworking increases convenience and efficiency; however, the workforce can have significant influences on organizations' data security and information technology operational strategies. Teleworkers' motivation may be reflective of the seriousness with which an organization regards security measures. Hardware, software, devices, networks, and connections are just some of the variables that can increase or decrease security, along with the competence, diligence, and attitudes of the teleworkers themselves. By researching best practices via literature and a quantitative survey in the current study, potential solutions to these problems were identified and organized in a functional manner.

1.1.2 Definition of Terms

To address the problems related to telework data security, definitions for key terms used in this study are below.

Non-teleworker. An employee who works at the official workplace during his/her regularly scheduled work hours.

Official teleworker. An employee who works outside of the official workplace, via a technological connection, during his/her regularly scheduled work hours, either at home or at an alternative workplace, on a full-time, part-time, or situational basis.

Unofficial teleworker. An employee who works at an official workplace, yet also performs work-related duties off-site on nights or on weekends.

1.2 Background/Introduction

Teleworkers, both official and unofficial, present unique challenges for an organization due to the information technology needed to provide them with a secure working environment while implementing information technology security controls. Despite the ongoing information security issues related to telework, its alleged cost- and time-savings make it an increasingly popular choice.

The Telework Improvements Act of 2009 (H.R. 1722), introduced by Rep. John Sarbanes, D-MD., and the Telework Enhancement Act of 2009 (S. 707), introduced by Sen. Daniel Akaka, D-HI, laid the groundwork for robust telework policies in each executive agency. These acts built on the attempts of Rep. Danny Davis (D-IL) and Rep. John Sarbanes (D-MD), who worked to make telework an even more significant part of the federal workforce by introducing H.R. 4106. The Telework Improvement Acts of 2008 bill, although never passed, would have mandated the option of a telework arrangement unless the agency could prove such an option was not viable. In addition, H.R 4106 would have required federal agencies to incorporate telework into the continuity of operations planning and to equip mission critical personnel to telework in time of a catastrophe. As Mears (2007) reported, "the law says the opposite: that all employees are ineligible unless the federal agency where they work shows that telework is a viable option" (p. 1). On November 18, 2010, the House of Representatives passed H.R. 1722, the Telework Enhancement Act of 2010, with a bipartisan vote of 254 to 152. The legislation granted federal employees eligibility to telework and required federal agencies to establish telework policies and designate a Telework Managing Officer.

Several reasons explain why the government and companies wish to increase teleworkers, including reduced energy consumption and less traffic, resulting from eliminating the need to drive back and forth to work, as well as a greater level of personal contentment for employees who are not forced to deal with the stresses of office life. These factors should result in greater productivity (Mears, 2007).

However, not everyone has agreed with the assessment. According to Antonopoulos (2007), telework has caused the line between personal time and work time to become so blurred that it has become natural for a person to take care of personal business at a time when the person should be taking care of work business. Such actions result in a decrease in productivity and raise the problem of requiring a workforce that is highly self-motivated–something often easier said than done. A more potent problem for opponents of teleworkers is that of information security and maintaining data security in a telework environment.

This most serious of disadvantages—the likelihood of security breaches, depending on location, education, motivation, and attitude of teleworkers—must be the focus of the debate. Information security concerns and yet unproven claims of the increased productivity of telework raise questions as to why telework is on such a steady rise. As Antonopoulos (2007) pointed out, by combining personal business and office business on the same computer, not only do lines between personal and business matters blur, but more importantly, information security can be more easily compromised.

Antonopoulos' suggestion for both present and future generations is as follows: "instead of trying to physically separate different use contexts, we should instead use virtualization on the desktop to logically separate contexts" (2007, p. 1). This virtual solution could allow users to separate work from play without having to use physically separate devices. Computers and laptops could be designed to pretend to be more than one machine to satisfy the desire for information security without a full lockdown. In its simplest implementation, a device could be divided into two virtual machines: red and green (Lampson, 2005). Lampson's point is to partition the device into two worlds: red, less safe and unaccountable, and green, safe environment and accountable.

The virtual solution is just one technical option to mitigate the risks to information security associated with telework. The current study focused on the end-user's behavior: the most efficient possible solution to such risks. In addition to an extensive literature review, a Teleworkers' Security Survey instrument was used to measure the perceptions and experiences of a population sample from The Telework Exchange. The Telework Exchange's membership is comprised of federal teleworkers, teleworker managers, IT professionals, and industry advisors. Approval was granted to post a survey on the Telework Exchange website. The current study is relevant by providing a timely portrait of the attitudes and experiences of the teleworkers' workforce in regard to security. Results illustrate what security breaches are most well-known and understood and which areas still pose a threat, given the current level IT education, to the job orientation to IT security policies and attitudes of teleworkers.

1.2.1 Theoretical Framework

This research applied the theory of planned behavior, an approach utilized by earlier studies of workers' attitudes within the information technology (IT) environment. Herath (2008), for example, used the theory of planned behavior as one component in the development of integrated protection, motivation, and deterrence model of IT security policy compliance (p. xiii). Spitzmuller and Stanton (2006) used the theory as part of a framework for predicting compliance and resistance to monitoring and surveillance technologies, such as e-mail monitoring.

1.2.2 The Theory of Planned Behavior

The theory of planned behavior was developed by Ajzen (2005). It was expanded upon by Herath and Rao (2009), and was used as part of a model on "integrated Protection Motivation and Deterrence." According to the theory of planned behavior, "intentions (and behaviors) are a function of three basic determinants: one personal in nature, one reflecting social influence, and a third dealing with issues of control" (Ajzen, p. 118).

The personal factor is the individual's attitude toward the behavior. Unlike general attitudes toward institutions, people, or determinants that social psychologists have traditionally studied, this personal factor refers to the individual's positive or negative evaluation of performing the particular behavior of interest. The second determinant of intention is the person's perception of social pressure to perform or not perform the behavior under consideration. Because it deals with perceived normative prescriptions, this factor is termed *subjective norm*. The third determinant of intentions is the sense of self-efficacy or ability to perform the behavior of interest, termed PBC or perceived behavioral control (Ajzen, 2005).

Generally, people intend to perform a behavior when they evaluate it positively, when they experience social pressure to perform it, and when they believe that they have the means and opportunities to do so. The theory assumes that the relative importance of attitude toward the behavior, subjective norm, and perceived behavioral control depend in part on the intention under investigation. For some intentions, attitudinal considerations are more important than normative considerations, while for other intentions, normative considerations predominate. Similarly, perceived behavioral control is more important for some behaviors than for others. In some instances, only one determinant or two determinants of the factors are needed to explain the intention; while in others, all three factors are important determinants. In addition, the relative weights of the three factors may vary from one person to another or from one population to another (Ajzen, 2005).

The objective of the current study was to investigate the relationship between the theory of planned behavior and teleworkers' attitudes toward compliance with security requirements in a teleworking environment. Knowledge gained through the research has provided insight into teleworking as it relates to data security, end user behavior, and physical security. All stakeholders stand to gain from a better understanding of what influences compliance with good security practices in a teleworking environment. Such improved understanding can provide a basis for identifying best practices to promote data security for teleworkers in organizations.

1.3 Opportunity for Research

The aim of the currents empirical study was to determine the perceptions and experiences of teleworkers and to provide additional insight into the best ways to address information security concerns. No research from this perspective on this significant issue of motivational factors related to the teleworkers' workforce and data security has been performed to date. Cindy Auten, General Manager of The Telework Exchange, granted permission to post a telework survey link on The Telework Exchange website as an instrument to collect data. This survey, conducted with the help of The Telework Exchange, provided real time information into teleworkers' attitudes, an area that had yet to be adequately studied.

This study used the available literature and an original survey to provide insight into the research questions posited. This was of critical importance considering that, "a fair amount of business users remain oblivious or unconcerned about many of the security issues involved with mobile devices, according to a new study published by Cisco and the National Cyber Security Alliance" (Hines, 2007, p. 1). With the vast majority (73%) of the mobile business people surveyed throughout the world giving little thought to security for their mobile devices, a dire need exists for awareness campaigns that alert businesses to the seriousness of security issues.

The importance of telecommuting and the information security challenges it raises will grow as globalization and the need for flexible work arrangements continue to be important factors in workforce management. As Hines (2007) poignantly asserted, "Education is the key to security" (p. 1). Although this area has been studied previously, a meta analysis and synthesis of its lessons and solutions will be helpful and can also be viewed through the prism of The Telework Exchange survey used to examine what has changed and what has not in the habits, education, and attitudes of current teleworkers.

Unfortunately, the existence of awareness and education opportunities offers no assurances that either will be utilized. The findings of a recent survey by the Computing Technology Industry Association (CompTIA), indicated “sixty percent of organizations surveyed recently said that security issues related to handheld devices have increased over the last 12 months, but most still ignore security training” (Jones, 2007, p. 1). It is perhaps for this reason that the failed bill described by Mears (2007) “mandates telework training both for new employees and managers and requires that employee reviews include a discussion of telework options” (p. 1). While having security procedures such as training and awareness initiatives and policy enforcement mechanisms is important, management must have a clearer understanding of end users receive and perceive these messages, according to Herath (2008).

Every argument has a counter-argument, and not all of the literature reviewed reported that teleworkers caused a greater threat to security. Some reports, such as one described by Sternstein (2007), stated federal teleworkers are actually less of a security threat than traditional office federal workers. The report Sternstein referred to was from The Telework Exchange and explained that the reasons security threats are reduced via telework are that materials are not physically transferred from place to place, and that teleworkers tend to be monitored more strictly than in-office workers (Sternstein, 2007).

The Telework Exchange survey described by Sternstein (2007) resulted from “an online poll of 258 federal employees, including sanctioned teleworkers, non-teleworkers, and non-teleworkers who unofficially work at home and revealed that federal data were significantly more mobile and still vulnerable.” The questions asked in the poll varied, but the most significant questions garnered the following results:

> The report found that 63 percent of respondents who worked from home unauthorized—more than half of the non-teleworkers surveyed—used their home computers in doing that work. “People were saving documents on their home computers that were unprotected,” said Josh Wolfe of Utimaco, a data security company that underwrote the study…When teleworkers and non-teleworkers were asked if they had antivirus protection on their laptop or desktop computers, 94 percent of teleworkers responded yes, while only 75 percent of non-teleworkers said yes. (Sternstein, 2007, n.p.)

In addition to the above, the results indicated part of the problem with security stemmed from the failure of agencies to adhere to recommendations of the CIO Council made in 1999 to establish policies for “limited personal use” of government e-mail and Internet systems (Sternstein, 2007, n.p.).

Information security and privacy are two sides of the same coin when it comes to the dangers of telework. The information security side comes from employers whose responsibility is to keep their customer and corporate data away from the prying eyes of competitors and others whose interests are a threat to the organization. The privacy side comes from the employees who are trusted to handle these data and to keep them safe, yet are at risk of losing their own privacy when this effort takes place outside the physical office environment.

Maintaining information security and privacy in cyberspace can be especially difficult, requiring elaborate firewalls and multiple checkpoints that seem to be violable nearly at will by sophisticated hackers. An even more complex problem arises when companies implement powerful security systems and discover they have a negative impact on the functionality of the software that allows them to do business in the first place. Effective information security devices can produce increases in application response times, causing significant delays between data entry and display, limiting call completion when using IP telephony applications, and creating a generally sluggish electronic work environment (Flood, 2001). In addition, the growth of the remote electronic storage industry, already strong in the later 1990s and fueled dramatically by the terrorist attacks of 2001, has become a costly and unwieldy business requirement.

On the other side, 90% of workers in traditional offices surf non-work-related websites during working hours (Cohen, 2001), causing additional demand on bandwidth and infrastructure. A reasonable assumption is that workers in remote locations do the same at least as often. At the traditional worksite, workers are aware that they are using the company connection to make personal purchases, write email, visit chat rooms, play games, conduct personal business, or generally wander around. Such activity is often monitored or, if not actually monitored, can be monitored quite simply.

However, at home, it is less clear that one is using company resources for private activities on company time. The distinction between company time and personal time, company resources and personal resources, is unclear. The availability and use of monitoring devices in workers' homes via the Internet comes dangerously close to wiretapping, which is illegal under most circumstances (Flood, 2001). Moreover, such monitoring is certainly an invasion of the privacy of one's home. Argument can advance that when the employee is working from home, he is on company time, and monitoring should be as lawful as it is in the office; however, sticky legal complications still arise in determining the timeframes in which home-based teleworkers are on the clock.

1.4 Research Objective

Telecommuting information security concerns are an important area of study due to the sheer number of teleworkers and rapidly changing information technology. Greater dependence on communications requires increased remote access to an organization’s data to perform the work, and is to some extent a function of the increasing geographical distance among workers and between workers and the headquarters.

The objective of the current study was to evaluate the theory of planned behavior as a means of understanding teleworkers’ attitudes to compliance with security requirements in a teleworking environment. The study explored whether the theory of planned behavior provided an explanation of teleworkers’ motivation to complying with information security practices and policies. An improved manner of understanding the human element in the maintenance of a secure teleworking environment represents a valuable step towards discovering actionable solutions to security problems in the telework environment.

1.4.1 Significance of the Study

This research addressed the knowledge gap in the area by focusing on teleworkers in organizations. The study was unique in the sense that instead of merely determining the scope of teleworkers and their practices, it focused on what motivating factors influenced teleworkers to follow the rules of security guidelines. This provided valuable information regarding what motivates these workers to comply with security standards, which can, in turn, be used to address specific motivational issues and modify behaviors.

1.5 Research Question

The following research question was used in this study to explore the types of motivational drivers that encourage compliance with security measures among teleworkers:

To what extent are there relationships between personal attitudes, perceptions of social pressure, and sense of control and teleworkers' willingness to follow and organization's information security guidelines?

The dependent variable was the willingness of teleworkers to follow information security guidelines within their particular organization. This variable was operationalized by using a 5-point willingness scale on the survey instrument. The independent variables were the personal attitudes, social pressure, and a sense of control. These were operationalized by using a 5-point Likert-type scale of the survey instrument, which directed questions towards each of these areas.

Chapter 2

Research Review and Synthesis

This review of literature focused on prior research regarding concepts of the theory of planned behavior and teleworkers attitudes about compliance with security requirements in a teleworking environment. The theory of planned behavior (TPB) is examined in this review, particularly with regard to the influence of norms manifested as peer pressure on the subjective norms of teleworkers and how this is translated into teleworkers adhering to telework security policies (Auten, 2008; Edwards, 2005; Friedman & Hoffman, 2008; Knorr, 2004; Liu & Issarny, 2007; Wagner, 2004; Wellman et al., 1996). Also in this review is examined the numerous security problems that have emerged in the teleworking environment, partly because corporate America believes in a technical as opposed to a social answer to the problem (Antonopoulos, 2007; Bain, 2007; Brandel, 2007; Clark, 2006; Clarke & Furnell, 2007; Curran & Canning, 2007; Fitchard, 2004; Freeman, 2005; Friedman & Hoffman, 2008; Garcia , 2008; Jackson, 2008; Jones, 2007; Kaven, 2004; Price, 2008; Simpson, 2004; Thurman, 2006).

The TPB was appropriate for use in the current study because of its focus on the construct of subject norms. The investigation of the construct of subject norms has been examined in a number of studies (Armitage & Conner, 2001; Armitage & Christian, 2003; Johnston & White, 2003). The TPB has been used in several studies to explain compliance or resistance by employees to adhere to security policies (Booker & Kitchens, 2010; Booker, Rebman, & Kitchens, 2009; Bulgurcu, Cavusoglu, & Benbasat, 2010; Dinev & Hu, 2007; Herath & Rao, 2009). Because the majority of research on teleworkers and data security have been conducted on federal agencies, several case studies that examined problems of security in federal agencies will be reviewed (Baginsky, 2004; Denscombe, 2001; Farmer, 2005; Gross, 2008; Hayes, 2008; Hines, 2007; Maier & Sametinger, 2004; Regan, 2003; Spitzmuller & Stanton, 2006; Thibodeau, 2007; Vijayan, 2009).

2.1 Empirical Research in Information Security and Assurance

At the end of the 20th and into the 21st century, the use of the Internet had gained wider use by organizations (Dinev & Hu, 2007). The Internet allowed workers to *telecommute* from home or other remote locations away from the office. The number of teleworkers increased and included staff, managers, technical professionals, and support personnel (Dinev & Hu, 2007; Wellman et al., 1996). Initially, managers were resistant to telecommuting because of concerns over the quality of work because professionals were less visible in the organization (Wellman et al., 1996). Another fear was that employee bonds and informal communication among teleworkers would be weakened and would reduce the effectiveness of peer support and pressure among teleworkers (Wellman et al., 1996).

Increasingly, telecommuting is being used by workers, especially within federal agencies as a means of reducing costs and allowing for greater worker flexibility. According to Edwards (2005), with advances in communications technology, inexpensive and mobile devices such as notebook PCs and laptops, and the creation of superfast wireless networks, mobile computing has become a popular option to office based work. No longer confined to a single desktop computer workstation, many people have become mobile employees (Auten, 2008; Edwards, 2005; Friedman & Hoffman, 2008; Knorr, 2004; Liu & Issarny, 2007; Wagner, 2004; Wellman et al., 1996). Mobile employees make use of their laptops, cell phones, or handheld devices at remote locations to gain access to the company network or database. Friedman and Hoffman (2008) reported that 81% of executives in companies around the world had a mobile device, and that 75% of the U.S. workforce will soon have mobile capabilities allowing them to gain access to company networks.

A primary concern over the use of teleworking and mobile devices has been security over the integrity of the data (Dinev & Hu, 2007; Ransbotham & Mitra, 2008). According to Edwards (2005), disabling devices, firewalls, and other security devices provide a level of security not achieved in the past. Research in Motion RIM) and Good Technology, two data security firms, have developed security solutions and devices that maintain the integrity of data used in the teleworking and mobile device environment. However, any security system to protect the integrity of information and data in a telework environment is effective only to the extent that teleworkers follow security guidelines and protocols (Boss & Kirsch, 2007; Pahnila, Siponen, & Mahmood, 2007; Siponen, 2005; Willison, 2006).

Within the physical organizational setting, the uses of computer systems are governed by security policies that are maintained through oversight by organizational security personnel. However, security assurance of computer systems of teleworkers in a home environment or in remote locations is highly dependent on teleworker behaviors (Dinev & Hu, 2007; Ng & Rahim, 2005; Stanton et al., 2003). The greatest threats to these home or remote location systems is from a virus infection which can compromise a system and threaten the integrity of information stored on the teleworkers’ systems or from hacking into a system and the theft or destruction of data (Dinev & Hu, 2007; Ng & Rahim, 234).

Several studies, primarily of federal agencies, have been conducted to gain a better understanding of the how well security recommendations and practices are followed and how well the practices achieved the confidentiality and integrity of information stored and used on computer systems (Cavusoglu, Cavusoglu, Son, & Benbasat, 2008; Dinev & Hu, 2007; Ng & Rahim, 2005; Siponen, 2000). The most common data security practices include frequent updates of anti-virus software, backing up critical data, and using a personal firewall on the computer system, especially when connecting to the Internet (Dinev & Hu, 2007; Ng & Rahim, 2005).

The safety of remote computer systems is influenced by security behaviors that include the intention to practice computer security, the attitude or user disposition to respond favorably to following organization computer security guidelines, and the teleworkers' perceived behavioral control over the extent that their behavior contributes to compliance or non-compliance with following security guidelines (Dinev & Hu, 2007; Ng & Rahim, 2005; Siponen, 2000, 2005). Ng and Rahim reported that, in terms of using a firewall, attitude and subjective norm had a significant positive relationship with intention and supported the use of the TPB as means of explaining teleworker compliance with organizational security guidelines. However, perceived behavioral control was less clear in terms of teleworker practice of updating anti-virus software or backing up critical data (Ng & Rahim, 2005; Riemenschneider, Hardgrave, & Davis, 2002).

Developing a security culture has been studied as a means of facilitating the intention to follow security guidelines (Boss & Kirsch, 2007; Cavusoglu et al., 2008; Ng & Rahim, 2005; Siponen, 2005). The presence of a security culture has been shown to influence increased compliance with following security guidelines to assurance data security and integrity (Ng & Rahim, 2005). However, this security culture is effective only to the extent that teleworkers are aware of security technology and procedures and have behavioral intentions to follow security guidelines (Dinev & Hu, 2007). That is, the behavioral norms of a social group about data security options such as anti-virus and fire wall software, anti-spy technology and other data security measures are influenced by members of the group's awareness and consequences of the use of these technologies while at the same time shaping the behavioral intentions of individual group members (Dinev & Hu, 2007).

According to Booker and Kitchens (2010), security assurance is highly dependent on workers' intentions. For example, some employees distrust security efforts by their organizations, some engage in activities to circumvent these security measures, and others simply do not comply with security guidelines and policies (Booker & Kitchens, 2007, 2010; Spitzmuller & Stanton, 2006; Stanton, 2000, 2002; Stanton & Weiss, 2000, 2003). Therefore, security assurance is highly dependent on the behavioral intentions of workers to comply with policies. Based on empirical evidence, researchers have concluded that behavior intention and sense of control are related to willingness to comply with security guidelines (Booker & Kitchens, 2007, 2010; James, Pirim, Boswell, Reithel, & Barki, 2006; Spitzmuller & Stanton, 2006; Zweig & Webster, 2002, 2003).

2.2 Review of Empirical Research in Relevant Disciplines

2.2.1 Peers and Telework

While telework continues to develop, a number of barriers persist. Among federal agencies, many workers are unaware of their options to telecommute resulting in a large gap between those eligible to telework and those performing telework (Auten, 2008). Some federal employees may not choose to telecommute because of issues with the organization's IT infrastructure or the reluctance of managers to use teleworkers (Auten, 2008). One way that federal agencies circumvent barriers to telecommuting is to follow the actions of the Defense Information System Agency by adopting an opt-in policy in which every employee in the department is designated "telework eligible," even if not ready to do so (Auten, 2008).

Carefully framing the technological parameters of telework such as outlining which devices and connections can be used is essential to creating a safe and manageable telecommuting environment (Auten, 2008). Only through such a plan can data security issues receive full consideration. Top-down managerial support as well as training is essential for carrying out this plan. Auten mentioned that the top administrator of the General Services Administration set 50% employee eligibility for telework as a department goal by 2010.

2.2.2 Security Concerns

A survey of over 1000 organizations by the Computing Technology Industry Association, reported by Jones (2007), showed that over 60% of companies reported growing concern about mobile security related to teleworking. The expansion of access to company files by teleworkers and mobile employees has resulted in a number of security breaches. The survey results also showed that a major gap remains between practice and concern, with 80% of companies allowing remote workers access to files, but only 32% of those companies having security awareness training or a security policy for teleworkers in place (Jones, 2007). Most companies sought to solve the security problem by being provided with new security devices by their mobile operator partners.

Sixty-three percent of companies who responded to the Computing Technology Industry Association survey reported, “they would change their mobile operator if a comprehensive mobile device management solution (MDM) was offered” (as cited in “Mobility Management,” 2007, p. 6). Ninety-five percent of companies said they were looking for a technological solution to the mobile security issues. Ninety percent expected the operator to manage security, and managed MDM appeared to be the favored way for securing mobile computing. Other companies were torn between the advantages and disadvantages of teleworking, which apparently increased productivity, but has presented companies with increasingly difficult management issues. The idea that one can manage mobile security, however, appears to have taken second seat to the technological solution.

2.2.3 Security and the Teleworker

The popular press and, increasingly, academic literature are filled with reports on malicious attacks on company systems, raising security concerns for all IT systems, especially when remote access is easy (Antonopoulos, 2007; Bain, 2007; Brandel, 2007; Clark, 2006; Clarke & Furnell, 2007; Curran & Canning, 2007; Fitchard, 2004; Freeman, 2005; Friedman & Hoffman, 2008; Garcia , 2008; Jackson, 2008; Jones, 2007; Kaven, 2004; Price, 2008; Simpson, 2004; Thurman, 2006). Jackson reported on a widespread injection of malware into the SONY Playstation Website in July 2006, an example of the increased threat to data security from malware. The malware was injected into the system when the used presses “yes” to a face security scan offer. Jackson remarked that, for the untrained remote user, “This social-engineering scare tactic has become increasingly common among online criminals” (p. 98). Jackson also reported that websites across the world were compromised by the same attack. The fact that the virus was spread through an unsuspecting fan pressing yes to a security offer emphasized the need for user education.

While the boundary between telework and mobile employment is often vague, both are part of a trend which brings with it enormous security risks. Several instances of data loss or theft of confidential employee or customer data from government agencies and leading private companies have proved to be very costly both financially and in terms of organizational reputation (Friedman & Hoffman, 2008, p. 160). Hackers have learned that hacking into mobile or enterprise employees' devices are an excellent way to gain access to corporate networks. Hackers know that mobile devices are the most vulnerable and least protected devices in organizations (Friedman & Hoffman, 2008).

One of the primary problems with mobile devices is that while all non-mobile systems are protected by corporate firewalls located at the corporate perimeter, mobile systems "connect to the Internet or shared networks directly, bypassing the corporate defenses" (Friedman & Hoffman, 2008, p. 160). While employees in the office work inside impervious LANs, mobile workers use Wi-Fi hotspots that are less protected and therefore more vulnerable to the use of spy-ware, mal-ware, spoofing, phishing, and viruses (Friedman & Hoffman, 2008). Loss or theft of company laptops is common and widespread. Many companies spend millions to secure their on-site computers, but take the view that security issues are the individual's concern for privately owned laptops and Blackberries.

Friedman and Hoffman (2008) drew up a taxonomy of security lapses in order to gain a full sense of the seriousness of the problem, noting that laptops can be subject to malware, phishing and social engineering, direct attacks by hackers, data communications interception and spoofing, loss and theft of devices, malicious insider actions, and user policy violations. Malware itself has caused billions of dollars of damage to corporate networks, but new types of malware have been created which specifically target laptops and handheld devices (Friedman & Hoffman, 2008). Moreover, malware creators now use short-span attacks to transmit the malware to millions of users in a few hours, serial variant attacks, whereby variations in the malware allow it to subsequently evade detection, and designer malware targeting specific targets making it extremely difficult to develop the signature of the attack and identify the sender of the malware (Friedman & Hoffman, 2008).

A number of specific malware programs have been created to shut down Blackberries and other handheld devices, and, worse still, "roaming laptops can acquire malware, then infect corporate networks when users return to the office and attach to the corporate LAN from inside the firewall" (Friedman & Hoffman, 2008, p. 163). A common way for a corporate network to become infected is when users synchronize home and work computers, inadvertently transporting malware. Adding to this problem is that most updates for spyware link only to corporate networks, leaving mobile devices vulnerable. The mobile blind spot is a problem created by the fact that mobile devices of teleworkers can travel for weeks without direct contact with the network, and thus miss updates of security in the interim (Friedman & Hoffman, 2008).

Phishing or social engineering involves efforts to "dupe computer users into sending confidential information to a third party" (Friedman & Hoffman, 2008, p. 164). Sending bogus emails, online contests persuading persons to download items with Trojan horses attached, and drive-by downloads are all ways by which phishers can obtain and exploit personal data. Phishing can become so devious that even if a user visits a legitimate site, he or she may inadvertently download a secretly implanted malware. In the case of MySpace, overlays of redirecting URLs were utilized to download malware into victim PCs. Friedman and Hoffman (2008) reported that, “as many as one in ten of all the URLs on the web will attempt to perform a malicious act against site visitors” (p. 165).

Friedman & Hoffman (2008) described mobile users as veritable sitting ducks for direct hacking. Wireless communications are vulnerable to spoofing because of the ease in intercepting then and the frequency in which uses connect to hotspots. Because most Wi-Fi’s do not have encryption capability, data is easily captured by hackers who steal usernames and passwords (Friedman & Hoffman, 2008, p. 166). Friedman and Hoffman described how a sniffing tool called Wireshark could sniff out the presence of mobile workers using a Wi-Fi hotspot to email the office and thus gain access to corporate networks. Because many mobile computer users from remote locations cannot distinguish between real and spoofed hotspots, they inadvertently give away personal information when logging onto the system.

Friedman and Hoffman (2008) described the amount of loss and theft of laptops and the resulting loss of personal information as rampant. Based on a comprehensive list of data breaches recorded and published by the Privacy Rights Clearinghouse, it has been estimated that since 2005 more than 200 million personal records have been made vulnerable to theft or loss (Friedman & Hoffman, 2008). The increasing numbers of teleworkers who are downloading data into USB thumb drives and handheld devices has contributed to such vulnerability. Friedman and Hoffman quoted a case in which “one IT manager found that 80% of his company’s employees were using USB storage devices, despite a clear corporate policy stating that anyone found storing data on removable devices was subject to termination" (p. 167).

Kaven (2004) reported that security is a more difficult problem for small companies who usually cannot afford IT professionals to advise them on security matters. Kaven outlined the features necessary to create an optimal firewall and advised security policies should be established and maintained by a system administrator for enforcement. With regard to teleworkers or employees working away from the office, Kaven recommended that employees never use business emails when signing up for any online newsletter or offer. In general, this approach to security in mobile computing places the burden on management.

2.2.4 Employee policy violation and carelessness

Problems in maintaining security and integrity of data is compounded by employees who fail to following organizational security policies leaving data vulnerable to hackers and phishers (Friedman & Hoffman, 2008). User policy violations related to mobile devices have led to the disabling of firewalls, downloading of malware, unauthorized use of software, copying files against policy to USB thumb drives, and emailing files containing confidential data to inappropriate parties. Friedman and Hoffman concluded that in many cases, teleworkers violated security policy unwittingly, in an effort to improve productivity, or for other harmless motives.

Friedman and Hoffman (2008) reported a case in which 17,000 employee records were exposed when an employee took her laptop home and her husband loaded a file-sharing program on the laptop after which the employee shared the information with any interested peer. Employees also have admitted to witnessing co-workers violating security policies or knowingly violated these policies themselves in order to increase their productivity (Friedman & Hoffman, 2008).

2.2.5 Security versus Usability

Some companies have developed telework by using customer relationship management systems to make assignments, account for work time, and communicate with co-workers (Thurman, 2006). One company reported difficulty in creating a VPN for laptops in client locales, primarily because clients refused to allow laptop use on site. A solution to this problem was to create a CRM application to run on Blackberry phones which required the development of a new set of security controls (Thurman, 2006). As a result, every security precaution installed reduced usability and productivity. But Thurman reported that prudent practices such as setting up authorization for privileged access are necessary for creating a secure system. The overall tendency of Thurman's remarks suggested a reliance on management and technology, not users, to maintain security in applications and developments that are in their infancy, and most likely controlled from above because they were new and uncertain.

2.2.6 Blurred Boundaries

Antonopoulos (2007) addressed the security issues involved in the inherent flexibility of teleworkers' lives, especially the blurring of the lines between work and leisure time. He posited the question, "But while employers might not worry about blurring the working hours, should they mind about employees using the same laptop for both work and play?" (p. 1). The primary concern with such blurring is whether sites contacted in the context of online leisure activity pose a security threat to company equipment. Reconciling the “security policies of one type of use with those of the other” is also difficult (Antonopoulos, 2007, p. 1).

This problem appears to be particularly difficult in managing so-called Millennial employees, whose online lives are complicated. Again, Antonopoulos asked “if is realistic to expect employees to keep home use on the home computer and work use on the work computer?” (2007, p. 1). Employers have addressed this problem through acceptable-use policies which restrict access to sites and forbid certain online activity at work. While such policies may be applicable in office contexts, the degree to which such oversight can be extended to home computers is questionable.

Antonopoulos (2007) therefore proposed that virtualization be used to “logically separate contexts” on the desktop (p. 2). For example, a home computer would have virtual machine attached to it which directed all home-machine traffic to a server at the home computer and directed all company use traffic to a server at the office network. Most teleworkers could use this type of virtual machine by putting it on a secure USB stick so that the “work desktop becomes truly portable and can be used on any machine, whether provided by the employee or not” (Antonopoulos, 2007, p. 2). According to Antonopoulos, this device would clearly separate work from home use, even on a teleworkers’ home computer, thus resolving many teleworker security problems.

2.2.7 Lost or Stolen Laptops

An incident at the Veteran Affairs department in which a laptop and an external drive were stolen compromised the personal data of 5 million veterans and cast a chill over both public and private sector teleworking (Brandel, 2007). One company altered its arrangement with teleworkers, making all workers sign a contract and allow company personnel conduct security checks of their home computing systems. The company felt that as “working from home is a privilege, not a right,” it had the right to address the “very real security risk for the company” presented by teleworking (Brandel, 2007, p. 27). With its new security policies, the company felt that it could continue with its teleworking program.

Brandel (2007) reported that “many U.S. companies haven’t bothered to establish security policies for teleworkers” (p. 27). One survey found that while 62% of companies were concerned about security breaches due to teleworking, only 46% of companies actually had a virtual office or teleworking security policy. Brandel suggested several easy solutions to the teleworking security problem. First, companies could insist that teleworkers only use company-owned equipment, not their home computers. This would ensure that up-to-date anti-virus, anti-spyware, anti-malware and other security protection programs were installed and updated through operating system standardization (Brandel, 2007). The use of company-owned computers also prevented workers from loading personal programs on their systems and not subjecting information policy supervisors from trying to figure out why “Billy’s World of Warcraft installation broke our critical internally developed application” (Brandel, 2007, p. 28).

Requiring teleworkers to use the same system is a second approach to security because all data is then protected by the security programs installed on the main system. This ensures that all computers seeking access to the VPN are up to date in their virus protection software, and that their firewalls also are secure. Programs such as Microsoft’s Safe Access would perform periodical checkups on virus scans done on home computers used by teleworkers to ensure that no viruses got into the company system.

A third approach to security for teleworkers is to implement policies restricting how teleworkers use home computers. For example, one company forbid teleworkers from storing company files on their home computers long term. In order to prevent the loss of data, company teleworkers had to upload data to the VPN system, which was backed up nightly. If the teleworker needed data on the computer for the purpose of a visit to a client, the company urged them to save changes to the network drive and delete any such material from their computers immediately following meetings. Behind this philosophy is the belief that "data should mainly reside in centralized corporate repositories" and not on teleworker home computers (Brandel, 2007, p. 28).

2.2.8 Encryption

Experience has shown that relying on teleworkers encrypt their data when using home based computers is risky. To ensure that data at home is encrypted, recommendations are that the PC be run as a virtual machine whereby logging on brings up the company's workstation in the telework location. Centralized systems encrypt data as it is received and removed from home computers. Currently, companies have enforced this difficult task primarily through having teleworkers sign a contract and training them in data encryption procedures such as changing "default service set identifier and administrator passwords on their wireless access points" (Brandel, 2007, p. 28). Though only 13% of companies currently risk the invasion of private data that a home security check entails and undertake home security checks, Brandel expected this number to rise as security problems develop. The extent to which growing security concerns may thwart the development of teleworking in general remains an issue.

2.2.9 Cell Phones

Fitchard (2004) pointed out that the very recent emergence of the 3G phone meant that every phone had an Internet protocol address, “complete with wide-open ports waiting for a malevolent soul to take it over” (p. 46). Security experts fear that, “such open-ended access could add up to millions of conduits into the corporate network, which in turn could equal millions of new ways for the mischievous and the downright malicious to gain access to critical company data” (Fitchard, 2004, p. 47). A recently reported flood of viruses in corporate networks has only increased concern about vulnerability. As a result, many vendors are offering corporations private IP networks or private-public hybrids.

In developing and implementing security protocols, companies must weigh the benefits of remote access against the dangers involved. For example, MCI segregated remote users in certain limited parts of the corporate network, preventing them from gaining access from whole sectors of the network only accessible on site. While this approach improved security, it limited the so-called benefits of telework. Along the lines of this approach, “for every restriction a company puts on user’s access…the benefits of working remotely start to dwindle” (Fitchard, 2004, p. 49).

Another problem is that networking technology development always has been put into use before proper security measures could be built into the standard (Fitchard, 2004, p. 48). MPLS, for example, came out in an unencrypted form, and the fact that vendors then had to add on proprietary security to each product meant that the market was full of incompatible versions of the technology.

A study by the Computing Technology Industry Association, reported by Jones (2007), found that while over 60% of companies had increased concern about security issues with teleworkers and mobile workers, “only 32% of organizations have implemented any security awareness training for mobile and remote workers” (p. 1). Moreover, only 10% of companies reported that they planned to begin training employees in security issues. This may be indicative of a lack of managerial oversight reflected in the fact that “80% of the organizations surveyed allow data access by remote or mobile employees” (Jones, 2007, p. 1). Nonetheless, evidence indicates those companies who implement security training have reduced problems, with 90% of companies who had implemented training reporting a decrease of remote security incidents.

2.2.10 Measures Addressing Mobile Security in the Information Age

After the Justice Department experienced security leaks, instituted a new policy to reduce security risks that forbid the use of non-agency computers or other devices to access agency files or e-mail (Bain, 2007). One serious security vulnerability was discovered when it was learned that family members of agency personnel were able to eavesdrop on agency activities. This policy no longer allows teleworkers to access agency computers from personal laptops; only agency issued laptops, docking stations, or others communication devices can be used for work at remote locations (Bain, 2007, p. 1). This way, the agency is able to ensure full encryption and monitoring of all Department of Justice computers used both at the agency and at remote locations.

The urgency of this problem with security is highlighted by the fact that 83% of information security officers at federal agencies reported laptop use is increasing and that each federal agency is in charge of setting policies about using personal computers at home to conduct agency business (Bain, 2007). Furthermore, even when workers are restricted to the use of organizational computers, the incident at the Veteran Affairs Department demonstrated a moment of carelessness by an employee can compromise data security (Bain, 2007).

Another security threat is through vishing (voice phishing) in which unsolicited callers are able to extract personal data during calls. Teleworkers are much more susceptible to identity theft scams through vishing (Chow, Gustave, & Vinokurov, 2009). Chow et al. reported that government offices are subject to caller ID spoofing and have developed policies to reduce the possibility of vishing such as requiring authentication of at least one line in a B2B telephone call. However, teleworkers remain more susceptible to hoaxes and scams than office based workers that have communications systems that prevent exposure to vishing on their computer systems (Chow et al., 2009).

2.2.11 Secure Desktops

A number software developers have responded to the need for more security in remote teleworking by developing secure desktops. Tarentalla developed new secure global desktop (SGD) software, reviewed by Chu as (2005), "a robust, nonintrusive software appliance that provides secure application access across enterprise infrastructures with mixed server environments" (p. 45). The marketplace for servers for remote or mobile workers is already crowded with products such as the Citrix System, Inc. Metaframe Presentation Server 3.0, and the Microsoft Corporation Windows Server 2003 Terminal server. The SGD "supports several security protocols to protect remote application sessions" integrated into current authentication systems or not (Chu, 2005, p. 45). The development of security systems such as the Tarantella SGD suggested the urgency of the demand for secure teleworking workstations.

Simpson (2004) described other efforts undertaken by companies to make mobile workers, including teleworkers, more secure. “Solutions such as hardware tokens, tighter software firewalls, and real-time end-point security enforcement are being used to ensure that remote PCs meet or exceed corporate security standards” (Simpson, 2004, p. 32). Simpson noted that security for teleworkers involves many difficult decisions for corporate security officers in trying to strike a balance between security and the freedom of mobile workplaces. He noted that “several layers of security are necessary for true end-to-end protection,” with “Security packages for end-point security . . . deployed in a layered and co-operative manner, with each layer checking and relying upon the others” (Simpson, 2004, p. 33).

2.2.12 Security through the use of Biometrics

While cell phones are often considered the benign enabler of teleworking, envisioning teleworkers as available to office management at all times, Clark (2006) pointed out that cell phones have their own security problems. Cell phones now are capable of storing information and providing access to the internet and other applications (Clarke & Furnell, 2007). There is limited legislation governing electronic surveillance, especially in terms of cell phones (Clark, 2006). The guidelines on what is allowable using tracking devices does not apparently include the cell phone. In fact, the law allows the use of cell phones to track an individual’s location if that person is in a public space. This opens up security risks to teleworkers who use their personal phones for work, especially since 1.3 million handsets stolen in 2001. Clarke and Furnell (2007) pointed out that the use of passwords and PINs provides weak security protections because it “relies heavily on the user to ensure continued validity” (Clarke & Furnell, 2007, p. 1). One study found that only

44% of cell phone users use their PINs, even though 81% were aware of security concerns. As a result of this failure, Clarke and Furnell believed that secret-knowledge approaches must be replaced.

Biometrics has been developed for use as authentication devices. Biometrics technology is based, “not on what the user knows, or what they carry, but who the user is; some unique characteristic” (Clarke & Furnell, 2007, p. 2). For example, keystroke analysis can be used to authenticate “the user based upon their typing characteristics” (Clarke & Furnell, 2007, p. 1). Developed based on pattern recognition, keystroke analysis involves assessing keystroke latency, the time between successive keystrokes, and hold-time characteristic, or the time to press and release a key. Using neural network classifiers Clarke and Furnell (2007) were able to perform classification with an error rate of only about 12%, suggesting that this approach provides cell phone users with more and better security. Overall, “the investigation has shown that ability for classification algorithms to correctly discriminate between the majority of users with a relatively good degree of accuracy based on the hold-time of a key” is viable (Clarke & Furnell, 2007, p. 9). Clarke and Furnell went on to describe how the data collection, classification, and authentication engines would work without inconveniencing the user. The system is best used by those who use cell phones regularly and is not appropriate for users with “large variations in their handset interactions” (p. 16). In the future, cell phones with built-in videoconferencing cameras could adapt facial recognition to strengthen mobile security.

Compared to previous communication technology, wireless security presents a host of new set of security problems. A number of steps have been taken to protect the broadcast footprint of wireless sets, including the development of the 801.11 group of specification developed by the IEEE for WLANs. These specifications “defined an over-the-air interface between a wireless client and an access point, or between two or more wireless clients” (Curran & Canning, 2007, p. 136) as is commonly the basis of what is termed Wi-Fi or wireless fidelity. Wired equivalent privacy (WEP) also can be added to 802.11, as it “generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers” (Curran & Canning, 2007, p. 136). However, WEP has a number of security problems that make it susceptible to attack with such methods as “IV collisions, message injection, and authentication spoofing” (Curran & Canning, 2007, p. 136).

Third-party solutions that “ride on the top of” Wi-Fi to provide “encryption, firewall and authentication services” are becoming more common (Curran & Canning, 2007, p. 137). In this context, looking at mobile devices used by teleworkers exchanging confidential or sensitive information with offices, Curran and Canning developed a solution “that secures both the traffic to the device and the data stored on the device” (p. 139). This technology prevents others from gaining access to a company network even though they have gained possession of a laptop. With this technology, after five failed attempts spaced by specified cooling periods are made to enter the device, all data is automatically erased from it.

2.2.13 Turning Off Security

Another problem posed by teleworker use of laptops is that users tend to want access to everything immediately, meaning that studies show, “users will have a tendency to turn off security features they feel are slowing them down” (Curran & Canning, 2007, p. 139). Thus, a number of devices were developed to make it impossible for users to uninstall security, or to force the computer into hibernation, with the requirement of a password to start it up again, if it goes unused too long. Certificate installation is another approach used to secure computers, entailing “sending a request to the Web service for a user authentication certificate” (Curran & Canning, 2007, p. 142). Overall, Curran and Canning concluded,

> Even though it is difficult to create a secure Wireless LAN, it is possible to combine existing technologies to create an architecture that enables both strong security for the WLAN transport itself and for the process that manages and distributes the credentials that are required to connect to the WLAN that is at the same time straightforward for end users to use. (p. 147)

Such implementation makes it “easy to deploy the security components to the end user devices and it eliminates the risks that are associated with shared secret keys or the insecure deployment of important credentials” (Curran & Canning, 2007, p. 148). The premise behind this and other efforts to find technological solutions to security is that users are unreliable and desire easy and quick access at all times. As a result, security can be taken out of their control to alter in ways that weaken its ability to ensure system security.

2.2.14 Losing Battle

Current security technology and measures are outpaced by the assault against them. According to Friedman and Hoffman (2008), cyber criminals have found ways to get passed personal firewalls and anti-spyware programs such that “The number of malware variants is simply overwhelming the capacity of anti-virus vendors and their customers to keep up” (p. 172). In 2002, there were about 22,000 malware programs; by 2007 it was estimated that 220,000 malware programs were in existence. More troubling is that less than 70% of malware programs are detected by the current level of protection. More effective protection such as virtual private networks do not allow remote access by teleworkers and this is not used in these situations. Other defenses include vulnerability management, configuration management tools, disabling unneeded communication methods, inbuilt or password encryption, restricted access to hotspots, data or disk encryption programs, the use of time bombs that destroy information after time, backup and recovery, and device control technologies among the growing number of defenses against malware and hacking.

2.2.15 Education and Training of Employees

With regard to user policy violations, many of the above technologies can greatly reduce exposure from these violations. However, education and training are essential to reducing the incidence of user policy violations by better informing them of security risks, "of what actions violate corporate policies, and of the consequences of violating the policies to them and to their organizations" (Friedman & Hoffman, 2008, p. 165). Thus, Friedman and Hoffman recommended that telework security breaches could best be prevented by a combination of technology and education.

With regard to education, Friedman and Hoffman (2008) place the responsibility on the organization to analyze the types of information on laptops and to issue a policy to restrict it. Effective security requires companies to know what devices are being used and who is using them, the type of information employees are sending through the network, and how data is being sent. In addition, security policy must be clear on the use of passwords, data encryption, VPNs, the uploading and downloading of software and data files, and other security devices and software (Friedman & Hoffman, 2008).

Friedman and Hoffman (2008) referred to the UK Data Protection Act of 1998, as well as IT governance frameworks such as COBIT 4.0, as guides to creating effective security policy. To avoid security breaches resulting from out-of- date software or misconfigured applications, organizations must "develop a solid infrastructure for deploying, configuring, monitoring and updating system software and security software applications" (Friedman & Hoffman, 2008, p. 178). Friedman and Hoffman recommended that it should be standard practice to issue laptops to teleworkers only after they have been loaded "a personal firewall, an anti-virus package, a zero-day threat protection package, a VPN client, and a VPN enforcement mechanism and data encryption" (p. 178). Emphasizing, then, company policy compliance, Friedman and Hoffman closed by noting that more research is needed on user policy violations "and what combinations of technology, training, and psychology (which would include peer pressure effects) can be used to prevent them" (Friedman & Hoffman, 2008, p. 180).

2.2.16 Mobile Administration

Garcia (2008) described some of the intricacies of mobile administration, or the managing of mobile user networks for teleworkers in companies. Device management, as the most common form of mobile management, provides tools that allow "for managing and monitoring a mobile fleet over the air, allowing administrators to remotely track inventory and maintain consistent firmware revisions across the fleet" (Garcia, 2008, p. 1). Garcia also noted that the pressure from teleworkers to bring consumer-grade devices into networks creates new problems, especially from "users demanding the devices be made to work with the corporate e-mail, VPN, and Wi-Fi networks" (p. 2). Garcia warned that to expand the number of devices onto a network that workers want would make it extremely difficult to deliver "consistent experience across a wide range of devices" (p. 2). The problem is that current mobile security platforms or other security suites would affect device performance. In general, Garcia seemed more interested in ensuring that mobile devices work than in making sure that they are secure.

Price (2008) argued that while protecting applications from threats from either hosts or others is difficult, “another challenge involves securing application from hostile hosts due to insufficient security policy enforcement” (p. 171). The user can place less trust in the host by using a trusted computing base or by using methods, such as debugging, “which are available to the end user to conduct a compromise” (Price, 2008; p. 170). Each type of threat has its own best defense against it. Thus, integrity attacks can be countered by “trusted hardware, trusted execution environments, and detection” (Price, 2008, p. 171). Availability refusal threats can also be detected by agents “recording and tracking their progress or activities” (Price, 2008, p. 172).

Companies can counter confidentiality attacks using encryption and trusted hardware, as well as code obfuscation. The same techniques can be used against hosts claiming to be authentic. Price (2008) maintained that many attacks can be countered with more efficient installation of hardware and software that is made more secure by requiring entry through administrator or system privileges. Safe areas of computation also provide client-side computing by encompassing Internet usage in trusted hardware. Overall, these protection approaches are supported by trust, with trusted references needed “to break the circular security issue experienced between applications and the host environment” (Price, 2008, p. 178). Getting teleworkers and other mobile computing agents to utilized trust agents may be enough to prevent security risks in mobile computing.

2.2.17 Employee Response to Initiatives According to the Theory of Planned Behavior

Proposed in the Theory of Planned Behavior (TPB) is the premise that “behavior can be best predicted from a person’s intention, which is an indicator of how hard people are willing to try, and how much effort people plan to exert toward performance of behavior” (Chatzisarantis et al., 2006, p. 229.) The intention has three subconstructs: (a) attitudes, or evaluation on performing the behavior; (b) “subjective norm, perceived influences that significant others may exert on the execution of behavior; and (c) perceived behavioral control, the extent to which people believe that they can control performance of social behavior” (Chatzisarantis et al., 2006, p. 229). Finally, also encompassed in the TPB is the premise that attitudes, subjective norms, and perceptions of control emerge from personal beliefs that a behavior will lead to certain consequences (behavioral beliefs), and an evaluation of these consequences (Armitage & Christian, 2003; Armitage & Conner, 2001; Johnston & White, 2003). Overall, “the relationship between behavioral beliefs and evaluations is known as the expectancy X value model and is grounded in subjective expected utility theory” (Chatzisarantis et al., 2006, p. 230).

According to Chatzisarantis et al. (2006), subjective norms are a good predictor of intentions “and that intentions and perceptions of control predict behavior” (p. 230). Chatzisarantis et al. suggested this model, “may not be sufficient for predicting and explaining human behavior because human judgment and behavior are not always a function of the computational rules suggested by the expectancy X model” (p. 229). As a result, they superimposed Deci’s self-determination theory over the model, suggesting that intrinsic motive offers the model greater explanatory power. In a study of this possibility, Chatzisarantis et al. found some evidence that intrinsic motivation activates the expectancy model in a more robust way.

Explored through the TPB is the relationship between attitudes and behavior. Researchers have reported that unilateral and memory accessible attitudes are “more predictive of subsequent behavior” than are multilateral or poorly remembered attitudes (Armitage & Christian, 2003, p. 187). It also has been shown that when measures of attitude and behavior correspond, “the correlation between the two is greater” (Armitage & Christian, 2003, p. 189). Though this kind of study has led to the idea that specific as opposed to general attitudes are more likely to lead to behavior, the number of factors that appear to influence attitude makes this generalization difficult to prove.

Researchers have moved to examining various mediators, such as behavioral intentions, as influencing the linkage between attitudes and behaviors. The formulation of this mediator led to the theory of reasoned action, where “behavioral intentions are determined by attitudes (overall positive/negative evaluations of behavior) and the perceived social pressure from significant others, subjective norms” (Armitage & Christian, 2003, p. 190). Only salient behavioral beliefs regarding the outcome and evaluation of doing something are relevant in this mediation. In the same way, “salient normative beliefs underpin subjective norms” and include “referent beliefs and motivation to comply” (Armitage & Christian, 2003, p. 190). The TPB then was also developed to address similar problems in the context of incomplete volitional control, where control beliefs underpin perceived behavioral control. Researchers have found such augmentation of the theory of reasoned action has expanded its accuracy in predicting behavior in various human situations.

The TPB has been studied widely in a number of different fields. In many studies, the construct that accounts for the most “variance in intention and behavior, independent of theory of reasoned action variables” is the perceived behavioral control (Armitage & Conner, 2001, p. 471). The TPB is an extension of the theory of reasoned action, taking into consideration “measures of control belief and perceived behavioral control” (Armitage & Conner, 2001, p. 471). The measure of perceived behavioral control in turn forms the basis of the health belief model and other models, as it is “held to influence both intention and behavior” (Armitage & Conner, 2001, p. 472).

This extension of the theory was needed because while the theory of reasoned action was fairly good at predicting behavior under volitional control, it was less clear in explaining how behavior resulted from intention. The theory of planned behavior also has been used to explain that “in situations where attitudes are strong, or where normative influences are powerful, PBC may be less predictive of intentions” as the nature of the situation strongly influences the formation of intentions (Armitage & Conner, 2001, p. 472). Researchers have reported that “measures of attitude strength and individual differences in sociability increase the relative predictive power of attitudes and subjective norms” (Armitage & Conner, 2001, p. 473). This is because, according to Bandura (1977), individuals are more likely to intend to engage in behaviors “that are believed to be achievable” (Armitage & Conner, 2001, p. 473). Personal and environmental barriers also come into play in blocking or facilitating turning intentions into actions. But with volition, evidence indicates these barriers can be more easily overcome. Thus, PBC’s influence on behavior is strongly moderated by the degree of volition involved.

2.2.18 Focusing on Subjective Norm

Another antecedent of intention includes subjective norm. This refers to “the individual’s perceptions of general social pressure to perform (or not to perform) the behavior” (Armitage & Conner, 2001, p. 475). Endorsement of behavior by a significant other makes it much more likely that a person will intend to perform that behavior. According to the expectancy model, these norms are supported by beliefs, the salience of which often determines the strength of one’s attitude towards the behavior. In this linkage, “subjective norm is considered to be a function of salient normative beliefs” (Armitage & Conner, 2001, p. 475). Thus, while subjective norm is related to “perceptions of general social pressure, the underlying normative beliefs are concerned with the likelihood that specific individuals or groups with whom the individual is motivated to comply will approve or disapprove of the behavior” (Armitage & Conner, 2001, p. 475).

Researchers have examined the utility of the theory of reasoned action and the TPB with regard to numerous activities. One study of tax evasion found that self-reports reflected subjective norms but were unreliable in describing behavior. Another study distinguished between PBC and self-efficacy and found that while PBC predicted discussing safe sex, only self-efficacy predicted actually practicing it. By contrast, it was found in another study that, “self-efficacy only predicted intentions, while PBC predicted exercise behavior” (Armitage & Conner, 2001, p. 477).

Researchers also have suggested that the normative component of the TPB is the “weakest component” in terms of its power to predict intentions (Armitage & Conner, 2001, p. 479). Nonetheless, it was reported in some studies that a clear distinction exists between people whose actions are driven by attitudes and those whose behavior is driven by subjective norms. In their test of the TPB, Armitage and Conner found, “subjective norm shows a reasonably strong relationship with intention when appropriately measured with multiple-item scales” (p. 487). They also found that self-efficacy was the strongest predictor of intentions, meaning that, “individuals form intentions that they are confident they can enact and that translation of intention into action may be facilitated both by self-efficacy and an assessment of more external factors tapped by PBC” (Armitage & Conner, 2001, p. 488).

When compared to self-efficacy, the subjective norm appeared to be weak. Again, the weakness of the subjective norm component has led some researchers to suggest a “reconceptualization of the mechanism by which normative pressure is exerted” (Armitage & Conner, 2001, p. 489). One researcher proposed that the weakness of the construct was primarily due to “a minority of individuals whose actions are driven primarily by perceived social pressure” (Armitage & Conner, 2001, p. 489). But Armitage and Conner doubted this, suggesting a need for reconceptualization of the normative pressure construct. They argued that social pressure is more often exerted in indirect and implicit ways as opposed to direct and explicit ways. In addition, Armitage and Conner proposed that self-categorization and social identity theories explaining how persons identify with “behaviorally relevant” groups “moderate the effects of group norm on intention” (p. 489). The moral nature of norms has also been further differentiated in the literature. Overall, then, “work on additional normative variables may increase the predictive power of the normative component of the model” (Armitage& Conner, 2001, p. 489).

The primary reason for development of the TPB as an extension of the theory of reasoned action was because that the latter theory had difficulty explaining gaps between people’s attitudes and behaviors. The variable factors influencing intention and behavior in the TPB make up for deficiencies in the theory of reasoned action. As a result, researchers have increasingly found the theory of planned behavior useful in predicting intention and behavior with regard to a number of habits ranging from smoking to exercise. Johnston and White (2003) focused on the fact that the subjective norm element of the TPB has been found to have “less predictive power than attitude,” which in turn caused Fishbein and Ajzen (1975) to “contend that the relative importance of attitude and subjective norm as predictors of intentions will vary as a function of the specific population and behavior under consideration” (Johnston & White, 2003, p. 65).

Johnston and White (2003) thus utilized social identity to form a clearer sense of how membership in a group may influence individual behavior. According to social identity theory, when people identify with a group, they categorize themselves as being part of an in-group, and they seek favor of those in the group as opposed to those outside of it. In the context of the group, a norm of behavior makes it much more likely that a person will behave accordingly. Thus, the perception of the group norm “should predict behavioral intentions” (Johnston & White, 2003, p. 67).

Studies testing this thesis have found it to be true in cases in which a person strongly identifies with the group, or thus has a high level of group identification. The research results “suggests that the role of norms in attitude-behavior models becomes stronger under conditions in which people categorize themselves and identify with an in-group that defines membership in terms of specific behaviorally and attitudinally prescriptive norms” (Johnston & White, 2003, p. 67). In testing this theory on the binge-drinking behavior of college students, Johnston and White found that not only were attitudes about drinking predicted by subjective norms according to the TPB, but also that by social identity such that “the effect of group norm of students’ intention to binge-drink was moderated by group identification, whereby the effects of norm were more important for individuals who strongly identified with the reference group” (Johnston & White, 2003, p. 74).

Considering these findings in terms of willingness to comply to data security guidelines, teleworkers might be more likely to comply with security procedures if directly connected through project work with a team based in the office. Furthermore, if teleworkers themselves began to develop an in-group identity according to which they mutually identified with each other and began to police each other’s activities, they might be more likely to comply.

2.2.19 Prior Examples of TPB Explanation

Hrubes, Ajzen, and Daigle (2001) tested the TPB with hunting intentions and hunting behavior. They found hunting intentions predicted self-reported hunting frequency, and that hunting intentions “were strongly influenced by attitudes, subjective norms, and perceptions of behavioral control,” as well as by underlying beliefs (Hrubes et al., 2001, p. 165). This fits the concepts of the TPB such that, “the more favorable the attitudes and subjective norm, and the greater the perceived control, the stronger should be the person’s intention to perform the behavior in question” (Hrubes et al., p. 167). Hrubes et al. concluded that broad values about wildlife form the background to influence beliefs and attitudes that play a role in TPB.

Researchers have used the TPB to understand better the likelihood of persons engaging repeated behavior such as self-care and self-monitoring (Shankar, Conner, &

Bodansky, 2007). The TPB rarely has been studied with regard to these behaviors, which, because carried out over time, “can be said to be engaged in maintaining the behavior” (Shankar et al., 2007, p. 215). Some behaviors develop as routines or habits because of past behavior, while other such behaviors may have to maintain a level of intentional control against obstacles.

In their study of self-care regimen among diabetes patients, Shankar et al. (2007) found that the difficulty and controllability of the task was the most important predictor of carrying out the routine task. While the researchers sought to find if conscientiousness, as a personality factor, predicted behavior, they did not, meaning, “such a broad, general factor is insufficient to understand more frequent behaviors” (p. 222). Shankar et al. also found that social norms had limited impact on user intention and behavior, reinforcing the idea that subjective norms form a weak link in TPB. That said, Shankar et al. reported that patients attending clinics or in the care of specialists behaved more regularly, suggesting some normative influence. The researchers proposed that “helping patients form . . . ‘where, when and how’ plans for self-monitoring might help motivated patients self-monitor more regularly” (Shankar et al., 2007, p. 223).

2.2.20 Case Studies of Peer Pressure Influence to Improve Teleworker Security

Peer pressure as a construct has become a basic tenet of research on youth behavior, with some influence in studies of adults in workplaces (Baginsky, 2004; Denscombe, 2001; Farmer, 2005; Gross, 2008; Hayes, 2008; Hines, 2007; Maier & Sametinger, 2004; Regan, 2003; Spitzmuller & Stanton, 2006; Thibodeau, 2007; Vijayan, 2009). For example, in a study of teen smoking, it was proposed that peer pressure contributed the most to the initiation of smoking, and programs to prevent smoking involve “the development of ‘life skills' to combat such peer pressure" (Denscombe, 2001, p. 8). This idea emerges from findings that, during the teen years, "peer influence is a key factor for young people who may be more likely to take account of the views and behavior of their peers than of adults" (Denscombe, 2001, p. 9). In the study of peer pressure among UK teens, however, researchers reported that, "the way the young people….experienced 'peer group pressure' did not accord with the way the notion has permeated into policy and professional practice" (Denscombe, 2001, p. 9).

Denscombe (2001) rejected the peer group presses and smoking concept. Because no causal relationship between peer pressure and smoking were found in cross-sectional studies, longitudinal studies, and studies of initial smoking situations, Denscombe proposed using a suspect contagion model that views smoking and other ills as a kind of "behavioral disease which spreads from one individual to another through some all-encompassing, yet poorly defined, process conveniently labeled 'peer pressure'" (p. 9). Researchers have pointed out that this concept represents another case of doctors using medicalized explanations for behavior, a model "as outmoded as they are mechanistic" (Denscombe, 2001, p. 9). The model is particularly poor in explaining the dynamics of such pressure, and those who have studied the dynamics found that peer selection rather than pressure is a much more germane influence. Thus, while the peer pressure model sees youth as stuck in groups, the peer selection model sees youth as moving from group to group, with youth having "some choice in the matter" (Denscombe, 2001, p. 11).

Researchers also have reported that peer pressure "does not enjoy a firm foundation built on psychological or sociological theory" (Turner & Shepherd, 1999, as cited in Denscombe, 2001, p. 10) and that youth often do not subscribe to the idea of peer pressure in practice. While peer pressure has taken on an almost legendary status as the cause for many behaviors in youth, it is also true that researchers increasingly have viewed peer support as a positive force. Peers are preferred over older mentors, for example, because "peers demonstrate closer understanding of the particular concerns they face, can have greater credibility and approachability, and may be more readily and regularly available, with the potential to offer support outside formal situations" (Baginsky, 2004, p. 3).

Peer pressure might be operationalized theoretically in the workplace through the concept of quality management. Quality management is "all the activities of the overall management function that determine the quality of policy, objectives, and responsibilities and implement them by using quality planning" (Hyrkas, Koivula, Lehti, & Paunonen-Ilmonen, 2003, p. 48). Peer or peer group supervision has become a topic of discussion in terms of its influence on quality in a number of organizations. It has been identified in the literature about peer supervision that a number of difficulties exists in the process, most of them stemming from the fact that the peers involved were not true peers because of varying levels of job description in the workplace. Peer supervisions also can result in common praising, competition, and transferring one's unpleasant feelings to another.

However, it also has been reported in the literature that a peer group often has a pool of knowledge and expertise that can help all members work more effectively and that reducing isolation expedites worker productivity. In a case study of peer supervision among nurses, Hyrkas et al. (2003) found that peers helped nurses develop a better sense of togetherness, sharing ideas, reflection on practice, and personal growth. Many of those involved also felt that the back-and-forth of peer interaction helped them internalize leadership values and practices. Overall, the subjects felt that peer supervision improved quality management through support and reflection and enhanced personal development (Hyrkas et al., 2003).

2.2.21 Employee Security Compliance According to TPB

Based on a case study, Spitzmuller and Stanton (2006) suggested that there a specific barrier to employee compliance with telework security measures is distrust of their employers. The researchers noted that many companies attempt to control computing by monitoring employee computer use, online and elsewhere, through various monitoring and surveillance technologies (MST). Such systems can track wherever any employee goes online, and “some computer monitoring software allows employers to obtain screenshots of the computer displays of employees connected to the network at any time” (Spitzmuller & Stanton, 2006, p. 245). Emails and any other files stored in company files can be accessed through keyword searchers to “locate and flag suspicious texts” (Spitzmuller & Stanton, 2006, p. 246). Many workers dislike and distrust MST and some actively “thwart their organization’s use of these systems by altering monitoring equipment/software or by avoiding monitored areas” (Spitzmuller & Stanton, 2006, p. 246).

Efforts to circumvent security not only reduce productivity but also have the potential to make such systems ineffective. Researchers have undertaken a number of studies to determine why an employee might or might not comply with such systems. Spitzmuller and Stanton (2006) reported that, “individuals’ group membership, social norms within groups, their workgroup identification, as well as their participation in the implementation of the monitoring system [were] precursors of compliance with the monitoring policy” (p. 246).

Spitzmuller and Stanton (2006) used the TPB to investigate factors that could lead to employee compliance of computer-use surveillance systems and examined if individual attitudes towards one's company further influenced compliance practice. In terms of the role of social norms within the organization, Spitzmuller and Stanton concluded that based on the original perception of Fishbein and Ajzen (1975), "perceived social norms provided the individual with information about which behaviors are socially rewarded and which are socially prescribed in a given situation" (Spitzmuller & Stanton, 2006, p. 248).

In an organization, a norm represents, "what employees believe to be shared standards for acceptable and unacceptable behavior in the workplace" (Spitzmuller & Stanton, 2006, p. 249). Thus, a profit-motivated company might sanction more aggressive profit-oriented behavior. According to Trevino, within an organizational context, individuals make ethnical decisions based on the promotion and compensation system of the company, aligning personals values to the company's motives and goals (as cited in Spitzmuller & Stanton, 2006, p. 248). If a person is committed to the organization, he or she is less likely to circumvent rules and more likely to comply with new rules and strategies. In their study, Spitzmuller and Stanton stated, "surveillance attitudes and affective organizational commitment were consistently positively related to the outcome variables, while normative commitment and organizational identification had weaker or non-significant relationships with intentions" (p. 263).

Technology skills and the presence of a caring, ethical climate in the company also moderated the relationship between surveillance attitudes and intentions to circumvent. Spitzmuller and Stanton (2006), using Trevino's model of ethical decision making, expected that social norms about what is believed to be the right thing to do would influence employee perceptions of “what is deemed acceptable” (p. 264) in responding to security initiatives. But the findings “support theory of planned behavior propositions pertaining to behavioral control: individuals tend to be more likely to act upon their attitudes if they feel they have the necessary control and knowledge to actually behave according to their attitudes” (Spitzmuller & Stanton, 2006, p. 264).

Spitzmuller and Stanton (2006) found a caring environment at work meant less sabotage and more benefit-of-the-doubt attitude. In addition, that those who breached security were more likely to be reported. This suggests a caring company has stronger and more positive peer interaction, which in turn leads to more compliance among peers, as opposed to an uncaring environment. These results “suggest that social constraints on behavior function differently depending upon whether one considers a behavior that breaks the rules versus a behavior that supports the rules” (Spitzmuller & Stanton, 2006, p. 264). Thus, “normative and personal constraints on behavior, such as prevailing ethical climate or prior technology experience, influence how strongly attitudinal components relate to behavioral intention” (Spitzmuller & Stanton, 2006, p. 264). In this case study, the theory of planned behavior had a high degree of explanatory power only when linked to ethical decision-making theories.

2.2.22 People in IT Security and TPB

Pahnila et al. (2007) noted that one of the most serious problems with corporate America’s apparent determination to solve information system (IS) security problems with technology and policy was, “employees seldom comply with these IS security procedures and techniques” (p. 1). Current practice of making employees more aware of security issues has been critiqued as “lacking not only theoretically grounded methods, but also empirical evidence on their effectiveness" (Pahnila et al., 2007, p. 1). It has been shown through a number of studies that IT security awareness programs are not effective in improving compliance.

Another approach of the literature has been to build explanatory models to explain theoretically why employees do not comply, though none of these theories has been empirically tested. Some of the models used have been, "the model of computer abuse, based on social bonds theory, the theory of planned behavior, the social learning theory and the general deterrence theory" (Pahnila et al., 2007, p. 2). On an empirical level, one study results indicated deterrence theory as implemented through making known policies and penalties found that stating penalties was an effective way to deter noncompliance. Another study showed that when employees perceived that the penalty or problem resulting from noncompliance was severe, they were more likely to behave well. Pahnila et al. claimed that none of these models or studies explains why employees do not comply.

The authors combined general deterrence theory, protection motivation theory, the theory of reasoned action, information systems success theory, and Triandis' behavioral framework to seek an explanation for such behavior. The theory of reasoned action, which linked "attitude towards compliance, intention to comply and actual compliance with IS security policies" was at the heart of the study (Pahnila et al., 2007, p. 2). Other factors included were threat appraisal, coping appraisal, quality of information dealt with, and habits and rewards. Overall, the researchers found that while sanctions did not have an effect on intention to comply and rewards did not have an effect on actual compliance, information quality did impact IS security policy compliance, and "attitudes, normative beliefs, and habits have significant effect on intention to comply with IS security policies" (Pahnila et al., 2007, p. 7).

Habit was found to have an especially strong impact on compliance, "it is important to IS security staff to get their organization's employees into the habit of complying with IS security policies" (Pahnila et al., 2007, p. 7). According to Pahnila et al., "practitioners should realize that positive social pressure (normative belief) towards IS security policy compliance from top management, immediate supervisor, and IS security staff is important for ensuring employees' IS security policy compliance" (p. 7). Pahnila et al. also proposed that because security techniques and policies do not seem to work in compliance, creating positive social pressure from the top down in an organization is a viable way to inculcate security-compliant habits in employees.

While in practice, most companies continue to rely on technology to ensure security, more researchers are finding, "information security cannot be achieved through only technological tools, and effective organizational information security depends on . . . . people, processes, and technology" (Herath & Rao, 2009, p. 154). Based on recent events, nor does security policy alone prevent breaches Thus, a number of researchers criticize current IS security governance programs because they "do not address the means to encourage conformity with policies" (Herath & Rao, 2009, p. 154).

Herath and Rao (2009) looked at agency theory in conjunction with the impact of penalties (extrinsic incentive), social pressures (extrinsic incentive) and perceived value or contribution (intrinsic incentive) on organizational security compliance. Herath and Rao first reviewed most studies of current security policy and noted they were written by higher-level security officers and contained little reporting on actual end-user compliance.

By contrast, researchers who studied end-users indicated many end-users remained confused about policy, and in general, policies are ineffective in ensuring compliance.

Hearth and Rao (2009) thus utilized agency theory to describe how a bond forms between one party and another based on personal costs related to devotion of time and effort to a firm, usually maintained by incentives. "Agency theory can provide a systematic way to think about incentive/disincentive mechanisms to encourage higher level of policy conformance" (Herath & Rao, 2009, p. 155). Among the noted incentives, social pressure has been found to influence behavior. Herath and Rao hypothesized that "social pressures exerted by subjective norms (perceived expectation) and descriptive norms (observation) positively influence the compliance intentions" of employees (p. 159).

Researchers also distinguish between the "*is"* and the "*ought"* of social norms and how individuals are under the influence of both extrinsic and intrinsic elements of social pressures. "The view that individuals are more likely to comply with relevant others' expectations when those others have the ability to reward the desired behavior or punish non-compliance behavior is consistent with findings in the technology acceptance literature" (Herath & Rao, 2009, p. 160). Subjective norms motivate compliance through the "possibility of gaining approval from the significant others" (Herath & Rao, 2009, p. 160). If an employee sees his or her peers routinely complying with security issues, then he or she is more likely to do so.

Various kinds of rewards or penalties also mediate this response. Thus both explicit incentives and implicit psychological contracts with regard to obligations and expectations contribute to manage compliance. Herath and Rao (2009) found that "both the intrinsic and extrinsic motivators influence employee intentions of security policy compliance in organizations," especially if employees see compliance as helping the organization (p. 160). More importantly, researchers reported that social influence plays a major role in compliance and "normative beliefs have a significant impact on employee behaviors, suggesting that the beliefs regarding expectations of superiors, IT management, and peers seem to have the most impact on employee security behaviors" (Herath & Rao, p. 160).

According to Herath and Rao (2009), if employees saw other employees complying with security issues, they too complied. Higher likelihood of being caught in noncompliance was also influential, though not the severity of penalty. It appeared that the overall opinions of others rather than the exact nature of penalty were the major influence on compliance. Thus, the appearance of penalty was more important than the actual penalty, leading Herath and Rao to suggested that "informal walk-in checks, to monitor the workplace, to evaluation of logs" might be enough to create an overall climate where compliance is the norm (p. 161).

In additional studies, Herath (2008) extended the literature on IS adoption by developing the integrated protection motivation and deterrence model of security policy, which advances that compliance is affected by organizational, environmental, and behavioral factors. Herath (2008) also utilized the Taylor-Dodd decomposition of the theory of planned behavior to examine compliance. Herath reported that "perceptions about the severity of breach and response efficacy are likely to affect compliance intentions by shaping attitudes, and this is supported by both organizational commitment and resource availability" (Herath, 2008, p. 62).

Taylor and Dodd's model was developed to explain better the multiple dimensions of subjective norms in the TPB as applied to information technology contexts (Herath, 2008). The protection motivation theory of fear appeals brings fear into the equation, while protection motivation “arises from the cognitive appraisal of three processes: appraised severity, expectancy of exposure and belief in coping response efficacy” (Herath, 2008, p. 69). In IT, “the role of social influence in technology acceptance decisions is complex and subject to a wide range of contingent influences” (p. 69).

Based on the results of a case study, Herath (2008) reported that “the severity of the threat significantly affects (employee) concern regarding security breaches” and “the perceived effectiveness of employee actions” (p. 87) also played a role in compliance. Generally, if employees understand that compliance has a positive impact on the organization, they are more likely to comply. Social influence was shown to play a role in that, “normative beliefs related to expectations from relevant others have a significant impact on employee behaviors” (p. 87). Both the expectations of others, superiors and peers, and the “perceived behavior of similar others” were found to improve compliance (Herath, 2008, p.88).

Herath (2008) also studied the impact of employee perception of the security climate in a company as expressed by training, awareness, and policy enforcement. Herath reported that “individual employee policy compliance intentions are predicted in their security climate perceptions, which in turn were highly associated with the employee perceived training and awareness as well as policy enforcement effects in their organization” (p. 94). Overall, while this finding implied that training is important for setting a climate, actual policy compliance intentions by employees is “mainly driven by personally held beliefs” (Herath, 2008, p. 94).

Warner (2009) sought to create a multidimensional model for IT security user behavior using the TPB and a study of individual level climate perceptions. The purpose of the study was to determine if the overall IT security climate of an organization was responsible for or impacted individual employee IT security behavior. The study results indicated a positive relationship between the overall IT security climate in a company and employee beliefs about the efficacy of anti-spyware efforts by the company, as well as various aspects of the protection and implementation of the anti-spyware.

Warner (2009) undertook the study to counteract the functionalist perspective focusing solely on a technological solution to security by considering the role of the human firewall of the internal users and examining how the employees could participate in complying with security. He used a socio-organizational approach to IT security, focusing in particular on the role of organizational climate as mediated by TPB to motivate employees to comply with IT security. Warner used the TPB to target intentions to comply with use of anti-spyware specifically, but used the construct of psychological IT security climate as an antecedent to normative and control beliefs in the TPB framework to provide further insight into the socio-organizational IT security processes. Warner reported that the TPB was useful in the area of IT security behavior research in that it described salient user beliefs that mediated between climate and compliance in IT security matters. While the study therefore built on a trend in the security literature to focusing on people not technology, it described employees only on-site in organizations, not teleworkers (Warner, 2009).

2.2.23 The Peer in Telework

Cisco recently issued a study with results indicating “a fair amount of business users remain oblivious or unconcerned about many of the security issues involved with mobile devices” (Hines, 2007, p. 8). Hines found that with the number of employees carrying mobile devices and laptops, whether for telework or mobile working, “a good number of people either ignore security threats related to the machines or policies meant to protect them from attack or data loss” (p. 8). Based on interviews with over 700 business people across the world using mobile devices, Hines concluded that “a great deal of end-user education still needs to occur to help people avoid making bad decisions in protecting mobile devices against potential attacks or data loss” (Hines, 2007, p. 8).

Seventy-three percent of users reported not always considering security issues, while “28 percent admitted that they hardly ever give thought to adhering to recommended procedures” (Hines, 2007, p. 9). One third of users reported that they had logged on to unknown or untrustworthy sources, while 44% of users said they had opened unknown email messages or attachments and 76% of users said, “they have a hard time differentiating such messages from legitimate content” (p. 9). The National Cyber Security Alliance has recommended that all users of mobile devices use passwords, “use anti-virus programs, download any recommended security patches, and back up all important content on their machines” (as cited in Hines, 2007, p. 10). As one expert remarked, “As more workers become mobile, proactively educating them to practice good security behavior should be a key tenet of any business’ approach to IT security and risk management” (Hines, 2007, p. 9).

Most people generally believe telework alleviates employee stress by offering them flexibility in balancing work-life stress issues and to avoid commuting (Hartig, Kylin, & Johansson, 2007, p. 231). However, more researchers have begun to assess the cost-benefit payoff of telework, with some arguing that its coping effectiveness is limited. The obvious fact that teleworking also separates employees from the office and from each other would seem to offset any possible impact of peer pressure on teleworkers. Hartig et al. presented an ecological model whereby people rotate through cycles of activity and restoration to meet the demands of their lives.

Home has become a place of control where people seek out activities and settings to "mitigate recurring demands, to enhance the possibilities for restoration" (Hartig et al., 2007, p. 234). This emerges from the modern idea of "home as refuge or haven (which) implies escape from a demanding and threatening 'outside world'" (Hartig et al., p. 234). This aspect of home life is often enhanced by "supportive family members" (Hartig et al., p. 234).

Hartig et al. (2007) noted that any fusion of home and work that "diminishes the restorative quality of the home may subsequently hinder the recovery of energetic resources" (p. 235), which may result in "constrained restoration" in which the cycle of restoration is replaced by chronic stress and even coping does not restore health. Hartig et al. found that while "managers cited greater working efficiency as the primary benefit of teleworking . . . clerical workers emphasized family and stress-reduction benefits" (p. 236). While not directly addressing the reverse side of the problem, it is likely that the efficiencies imagined by managers for telework are often compromised, and many of the advantages of in-office work, such as the efficacy of peer support or pressure, are also lost in translation. Nonetheless, Hartig et al. suggested an ecological model by which researchers can surmise that telework has the overall effect of compromising peer pressure, thus reducing its impact on teleworker behavior.

2.2.24 A Model of Peer Behavior Online

Ubiquitous computing is yet another term used to describe a world where everything is linked by computers. Liu and Issarny (2007) described how mobile ad hoc networks or MANET allowing the spontaneous linking of mobile devices has contributed to the notion of ubiquitous computing. They reported such networks function well only with a trustworthiness evaluation of service providers to screen dishonest service providers. This approach may be better than traditional security measures such as authentication and access control which “fall short . . . because of their reliance on security infrastructure such as Certificate Authority” (Liu & Issarny, 2007, p. 298). Such techniques provide no access control information.

By contrast, trust “deals with the estimation of a node’s future behavior” and reputation is a “perception that a node creates trust through past actions about its intentions and norms” (Liu & Issarny, 2007, p. 299). Researchers studying the use of trust validation on eBay and other systems have found that fear of future revenge from a poor evaluation by such mechanisms causes users to behave. Trust is established not only by the users’ previous direct contact with each other, but also by recommendations of the trustee by others. Recommendations help fill gaps caused by long breaks in direct contact between users, thus building up a more general level of trust. Though working well, Liu and Issarny (2007) noted some problems with existing reputation mechanisms and proposed “a distributed reputation mechanism that motivates entities to recommend truthfully and actively” (p. 298).

Liu and Issarny (2007) reviewed the existing service and recommendation reputation mechanisms used by various services, especially efforts by the systems to identify lies or malicious attempts to undermine the system. They reported that most current mechanisms “lack measures to enforce voluntary and honest recommending” (p. 301). The system proposed by Liu and Issarny stores all recommendations by users and creates a trustworthy network of users. “This requires strong group support, as the group members need to trust each other and have common interests such that they are motivated to protect the group’s reputation” (p. 310). While this system still leaves open the possibility of so-called Sybil attacks, when a malicious user creates a number of identities to “challenge the use of majority in reputation systems” it nonetheless highlights a means by which peer pressure through reputation recommendations can be used to enforce fair play in virtual environments (Liu & Issarny, 2007, p. 313).

2.2.25 Situational Leadership for Teleworkers

The founders of situational leadership, Hersey and Blanchard, combined situational theory and contingency theory to form their model (Hersey, Blanchard, & Johnson, 2008). At the core of situational leadership theory is the perspective that the level of success that a leader experiences depends a great deal on the maturity level, or follower readiness of his or her followers. Follower readiness has four different levels:

L1. Low follower readiness (low ability and low willingness). These followers are entirely resistant to leadership and are not likely to follow anyone but themselves.

L2. Low to moderate follower readiness (low ability and high willingness). These followers can see the value of the leadership effort and are eager to act on it, but are simply not able to do so.

L3. Moderate to high follower readiness (high ability and low willingness). Where at this level, leader-directed decisions begin to turn into self-directed decisions, because the followers have become more capable of handling tasks and decisions themselves. However, their level of willingness is low because they are not as confident in their abilities as they should be.

L4. High follower readiness (high ability and high willingness). These followers are both willing and able to perform to their optimum level due to their confidence, maturity, and motivation (Hersey et al., 2008).

Situational leadership also has four different leadership styles:

1. Structuring (Telling) Style (high task and low relationship). This style focuses on guiding the follower through the task but holding back on emotional support and relationship building. It is a highly directive approach in which the leader tells the followers exactly what they should be doing, how they should be doing it, and when they should be doing it. This is most appropriate for low follower readiness (L1) because these followers require the most amount of instruction and motivation.

2. Coaching (Selling) Style (high task and high relationship). This style combines directive guidance with relationship building and support, and it involves significant influence or the "selling" of ideas on the part of the leader. This is best for low to moderate follower readiness (L2) because it capitalizes on their high willingness while not overestimating their abilities.

3. Encouraging (Participating) Style (low task and high relationship). In this style, the leader is not nearly as directive and instead places emphasis on two-way communication between the leaders and the followers. This is a participatory style in which the followers are permitted to contribute their own ideas and opinions to the process. This is the most appropriate leadership style for moderate to high follower readiness (L3) because it helps to increase follower confidence.

4. Delegating Style (low task and low relationship). Neither a great amount of guidance nor relationship building is incorporated into delegating style, because the leader trusts the followers enough to delegate responsibilities to them. This is the most appropriate leadership style for high follower readiness because it allows followers to take the reins and do what they do best (Hersey et al., 2008).

Farmer (2005) proposed that managing teleworkers is different in many ways from managing office workers and that situational leadership is the only model effective for dealing with telecommuters. Based on the notion of open communication "while helping staff with competence, commitment, and independence," situational leaders help teleworkers feels more "connected," which "can be linked to job satisfaction and retention" (Farmer, 2005, p. 484). The primary principle of situational leadership is that the appropriate style of leadership "is based on the subordinate and the task" (p. 488) and leaders must use whatever style is called for in any given situation in order to help the follower become more self-reliant.

Most managers who are successful in managing telecommuters work hard to eliminate obstacles and provide adequate resources to the teleworker. "Managers and other team members need to be available by e-mail to promote effective communication, and guidelines have to be set regarding response times to e-mail etc." (Farmer, 2005, p. 488). While only addressing the issue of changing leadership style to best accommodate the needs of teleworkers, also implied in this model is that teamwork and a sense of belonging to a team, a possible source of peer support or pressure, is also a critical element in successful teleworking.

Kambourakis, Maglogiannis, and Rouskas (2005) reported on a case study of the use of confidential and personal health records by remote users in telemedicine or remote patient telemonitoring. The health industry primarily makes use of public-key cryptography to secure records, and Kambourakis et al. demonstrated how "robust security mechanisms and effective trust control can be obtained and implemented" through various applications (p. 512). The public key system is a role-based access control device, replacing discretionary and mandatory access controls, which limits access to authorized personnel only. The users of these codes "derive their access rights and permissions from the roles they are assigned" (Kambourakis et al., 2005, p. 514).

In their case study of access of sensitive medical records through a mobile device by doctors remotely located, and essentially behaving as teleworkers in this context, Kambourakis et al. (2005) found that access with security "is attainable even with current technology" (p. 525). With regard to social identity theory as added to the theory of planned behavior, it may be that this success arose from the fact that all users were identified as part of a select in-group with a strong identity as group members, thus adhered unquestionably to norms.

2.2.26 Knowledge Intensity and Peers

One element that may make peer pressure more pertinent to teleworkers is that more products and services are becoming knowledge-intensive (Maier & Sametinger, 2004), meaning that more workers "collaborate in teams, networks, and communities and have to be supported with an adequate organizational as well as an information and communication technological infrastructure" (Maier & Sametinger, 2004, p. 79). Thus, peer group collaboration, as well as pressure, may become institutionalized through knowledge management systems that consider teleworkers as well. InfoTop is a workspace designed to help workers share context and collaboration, primarily because they are in peer-to-peer information workspaces (Maier & Sametinger, 2004). Because of the demands placed on knowledge workers, "virtual teams, expert networks, best practice groups, and communities complement traditional organizational forms, such as work groups or project teams" aiding collaboration across organizations (p. 82). Lifestream, Timescape, and Presto are among a number of new filing structures used in knowledge management to overcome the limitations of hierarchical files and allow for a richer interaction with documents. Personal Brain is another organizational tool that organizes information, “according to whatever scheme makes sense to the user” (Maier & Sametinger, 2004, p. 87).

Groupware platforms such as Lotus Notes and Microsoft Exchange also “provide general support for collecting, organizing, and sharing information within collectives of people” (Maier & Sametinger, p. 87). In a workspace like InfoTop, “participation should be no more of a problem than in centralized KMS within organizational boundaries” (p. 90). Maier and Sametinger suggested that in this context, peer-to-peer knowledge networks might serve as communities that “act as a kind of social infrastructure that induces social regulations and also trust into the peer-to-peer network” (p. 90). They also believed that InfoTop-type workspaces would allow more participants to handle information in organizations with less worry about security issues.

2.2.27 Case Study of Federal Employee Teleworkers Improving Security Through Peer Pressure

Only one case study was found in a search of the literature specifically addressing the effects of peer pressure on federal teleworkers’ tendency to improve security measures. Vijayan (2009) examined new requirements passed by the state of Massachusetts to force companies using online data to ensure the compliance of third parties handling data to new security rules. A number of states have begun to impose security laws on companies doing business online in the state, such as mandating encryption or other data security measures. But the rules in Massachusetts are particularly stringent, both in the steps needed to comply and in defining the various elements of personal data, resulting in slow compliance.

A survey of companies in the state found that a majority of organizational leaders did not know about these new regulations and that the deadline for compliance was unrealistic. Many company leaders, “questioned the wisdom of requiring companies to adopt costly new security measures at a time when many are struggling just to make payroll because of the economic recession” (Vijayan, 2009, p. 12). It was countered that it is not unreasonable to require companies to take “all reasonable steps” in ensuring third-party compliance, as the current regulation would require companies to rewrite contracts and change the way of doing business with third parties. Vijayan reasoned that making senior executives aware of the new rules might be the best way to ensure compliance. Even so, predictions are that most companies will take many years to comply with security requirements. Overall, Vijayan recounted a familiar scenario of the difficulty of implementing change in governmental contexts.

2.2.28 Added Federal Concerns

Government agencies support teleworking for the added reason that the decentralization involved in such work “may keep their operations running in the event of an influenza pandemic” or similar catastrophe (Thibodeau, 2007, p. 6). Thibodeau noted such plans could be stalled by the heavy increase in online traffic during an emergency. A surge in information-seeking traffic would trigger restriction efforts and “government action might well follow” (p. 6). Government agencies could reduce traffic by “using redundant communications systems and techniques such as diverse routing” (p. 6), but Thibodeau believed that teleworkers would most likely experience remote access difficulty. Teleworkers, then, seemed particularly vulnerable during emergencies, and the security problems they posed might call their efficacy into question. Overall, Thibodeau (2007) found that government agencies have an added level of concern about the security of teleworkers.

2.2.29 Resistance to Telework: Inhibiting the Emergence of Peer Support

A special consideration in discussing the case of federal teleworkers is that it appears federal agencies have held back the growth of telework (Gross, 2008). On the level of the federal government, an additional argument made on behalf of telework is that it gives departments “the ability to continue operations during a national disaster or terrorist attack” (Gross, 2008, p. 21). However, many federal managers are not convinced telework is beneficial and they question their own ability to manage telework. Some reported in a survey that because excess funding must be returned in federal agencies, telework will not result in savings. The primary problem in such managerial negativity about telework on the federal level is that such views percolate down to employees short-circuiting hope that positive peer support and attitudes towards telework would support telework development and adherence to security issues (Gross, 2008).

The federal government “requires its agencies to encrypt all sensitive data on laptops and mobile devices” (Hayes, 2008, p. 36). However, the GAO recently reported, “70 percent of such devices didn’t encrypt, and the other 30% weren’t in great shape either” (p. 36). This means that even those computers believed to by encrypted had improperly installed security codes, or “users hadn’t been trained, sensitive information hadn’t been inventoried, and crypto key control procedures hadn’t been established” (p. 36). Overall, the GAO suggested a scenario in which, if the technical side of encryption cannot be mastered for use on mobile devices, creation of a level of peer support to effectively influence teleworkers to encrypt their laptops and work on them safely is unlikely. In other words, teleworkers will resist encryption and other safety measures if they are not properly trained or are not confident in using such measures (Hayes, 2008).

2.3 Theoretical Foundation

The intent of the current study was to examine the application of the theory of planned behavior to the teleworkers' attitudes about compliance with security requirements in a teleworking environment. The conceptual model in Figure 1 provides the framework of analysis of the study.

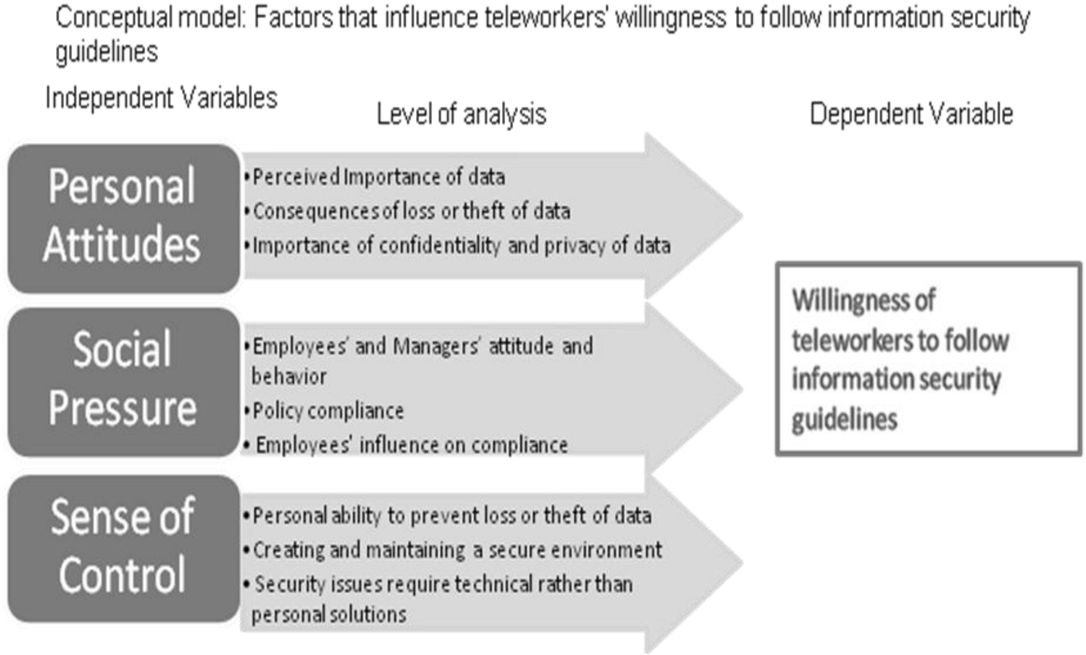

Conceptual model: Factors that influence teleworkers' willingness to follow information security guidelines
Independent Variables
Level of analysis
Dependent Variable
Personal Attitudes
•Perceived Importance of data
•Consequences of loss or theft of data
•Importance of confidentiality and privacy of data
Social Pressure
•Employees' and Managers' attitude and behavior
•Policy compliance
• Employees' influence on compliance
Sense of Control
•Personal ability to prevent loss or theft of data
•Creating and maintaining a secure environment
• Security issues require technical rather than personal solutions
Willingness of teleworkers to follow information security guidelines

Figure 1. Conceptual model for the framework of the study

2.4 Justification for Research

The purpose of the current study was to examine the problem of teleworker compliance with security policy. The dependent variable in the study was the willingness of teleworkers to follow prescribed security measures as outlined with their particular organization. The independent variables were the effects of personal attitudes, social pressure, and a sense of control. Based on a review of the literature, it has become evident that with the growth of telework, as well as the broader development of mobile computing, companies and agencies have begun to have concerns about security issues (Auten, 2008; Edwards, 2005; Friedman & Hoffman, 2008; Knorr, 2004; Liu & Issarny, 2007; Wagner, 2004; Wellman et al., 1996). For example, a number of recent highly publicized lapses in security in government agencies has raised alarms about how easy it is for intruders to breach corporate or agency security through portable devices such as laptops or personal computers used by teleworkers at home (Antonopoulos, 2007; Bain, 2007; Brandel, 2007; Clark, 2006; Clarke & Furnell, 2007; Curran & Canning, 2007; Fitchard, 2004; Freeman, 2005; Friedman & Hoffman, 2008; Garcia , 2008; Jackson, 2008; Jones, 2007; Kaven, 2004; Price, 2008; Simpson, 2004; Thurman, 2006).

Part of the problem has been the inability of policy to catch up with reality. Furthermore, organizational leaders adhere to technological solutions to the problem and deal with increased threat by adding more security devices. However, many organizational leaders fail to address security compliance among teleworkers through peer support and pressure. The theory of planned behavior, with a focus on the construct of the influence of norms on individual intention to carry out a behavior such as implementing security policy, was reviewed in the current study. One study paralleling the goal of the current study found that the theory of planned behavior accounted for employee behavior with regard to compliance to policy (Armitage & Christian, 2003; Armitage & Conner, 2001; Johnston & White, 2003). Based on a number of case studies, researchers reported mixed results in explaining whether peer pressure could close the gap between theory and practice in terms of teleworker compliance to security policy. The problem appeared to be even more difficult in the context of government agencies, if only because teleworking has been initiated more slowly in the public sector, as opposed to the private sector, and many managers remain wary of security problems they believe to be inherent to mobile computing and telework (Baginsky, 2004; Denscombe, 2001; Farmer, 2005; Gross, 2008; Hayes, 2008; Hines, 2007; Maier & Sametinger, 2004; Regan, 2003; Spitzmuller & Stanton, 2006; Thibodeau, 2007; Vijayan, 2009).

Chapter 3

Methodology

3.1 Theoretical Framework

In the current study, members of The Telework Exchange community were sampled to gather quantitative data to draw provisional conclusions of the relationships among factors that motivate teleworkers to follow rules of information security guidelines as explained by the theory of planned behavior (TPB). The results of the survey provided a basis for evaluating whether the subjective norm alone was more predictive of willingness to adhere to the security procedures and was a better explanatory model for teleworkers' decisions with respect to the IT security environment: personal attitudes, social pressure, and a sense of control. Because the subjective norm encompasses peer pressure (Ajzen, 2005), such an analysis provided a strong indication of whether the TPB is a useful explanatory model in this context.

3.1.1 Research Question and Hypotheses

Research Question: To what extent are there relationships between personal attitudes, perceptions of social pressure, and sense of control and teleworkers' willingness to follow an organization's information security guidelines?

RQ1a. To what extent are there relationships between items on the Personal Attitude Scale and teleworkers' willingness to follow an organization's information security guidelines?

$H1a_0$: There is no relationship between items on the Personal Attitude Scale and teleworkers' willingness to follow an organization's information security guidelines.

$H1a_a$: There is a relationship between items on the Personal Attitude Scale and teleworkers' willingness to follow an organization's information security guidelines.

RQ1b. To what extent are there relationships between items on the Social Pressure Scale and teleworkers' willingness to follow an organization's information security guidelines?

$H1b_0$: There is no relationship between items on the Social Pressure Scale and teleworkers' willingness to follow an organization's information security guidelines.

$H1b_a$: There is a relationship between items on the Social Pressure Scale and teleworkers' willingness to follow an organization's information security guidelines.

RQ1c. To what extent are there relationships between items on the Sense of Control Scale and teleworkers' willingness to follow an organization's information security guidelines?

$H1c_0$: There is no relationship between items on the Sense of Control Scale and teleworkers' willingness to follow an organization's information security guidelines.

$H1c_a$: There is a relationship between items on the Sense of Control Scale and teleworkers' willingness to follow an organization's information security guidelines.

3.1.2 Operational Definitions of Variables

Both dependent and independent variables were operationalized based on the TPB. The dependent variable was the willingness of teleworkers to follow information security guidelines within their particular organization. This variable was operationalized by using a 5-point willingness scale included on The Teleworker Security survey. The 9-item Personal Attitude Scale, 9-item Social Pressure Scale, and the 9-item Sense of Control Scale served as the independent variables. All 28 items of The Teleworker Security survey were presented using a 5-point Likert-type scale with response anchors ranging from 1 = *strongly disagree* to 5 = *strongly agree* for all independent variables and from 1 = *very unwilling* to 5 = *very willing* for the dependent variable.

The first independent variable, personal attitude, was measured by respondents' agreement or disagreement with statements relating telework and the importance of the security of organizational data and the consequences of loss or theft to the organization and to the respondent, as well as with statements relating to security, confidentiality, and privacy in a broader social and personal context.

The second independent variable, social pressure, was measured by respondents' agreement or disagreement with statements relating telework to the extent to which employees, managers, and policies created pressure to either comply or not comply with practices and whether other employees' compliance with good security practices was likely or unlikely to influence the respondents' compliance.

The third independent variable, the sense of control, was measured by respondents' agreement or disagreement with statements relating telework to the extent to which they believed their own actions and decisions were likely or unlikely to prevent loss or theft of organizational data, the extent to which they feel they participate in the creation and maintenance of a security environment, and their agreement or disagreement with the proposition that IT security problems require a technical rather than a personal solution.

3.1.3 Rival Hypotheses

The theory of reasoned action (TRA) is an alternative theoretical basis for interpreting attitudes and behavior (Armitage & Conner, 2001, p. 471). This theory attempts to relate self-reported volitional attitudes to behavioral outcome. Researchers have shown it to be deficient, however, in explaining observed discrepancies between reported beliefs, attitudes, and motives and actual behavioral outcomes.

Another theoretical basis that has proven inadequate focuses on the individual's perception of social endorsement of certain behaviors–the so-called subjective norm (Armitage & Conner, 2001, p. 475). This accounts only for those individuals motivated primarily by social pressures, and again, discrepancies have been observed between self-reported normative influences and actual behavioral outcomes.

The theory of planned behavior offers a more complex and potentially more fruitful framework for analyzing intention than accepting an individual's self-reported evaluations of the attitudes, influences, and norms underlying their actions. The independent variables are personal attitudes, social pressure, and sense of control and the dependent variable is the willingness to follow information security guidelines as outlined within a particular organization.

3.1.4 Plausibility Assessment of Rival Hypotheses

In the current study, the survey questions were designed to distinguish the role of the three reported determinants of intention under the TPB. The first is personal attitude, the second social norm or social/peer pressure, and the third is perceived behavioral control: the extent to which the individual believes his or her attitudes and actions can influence outcome.

The TPB essentially combines the TRA and the social norm theory and adds the important element of perceived behavioral control (Chatzisarantis et al., 2006). From survey responses, therefore, estimating the explanatory power of self-reported volitional attitudes alone and the explanatory power of the social norm alone should be possible, providing a basis to evaluate the extent to which the TPB provides richer explanatory and predictive power than the competing hypotheses.

3.2 Research Design Approach

This quantitative study consisted of the analysis of the results from the Teleworker Security Survey completed by a sample of the members of The Telework Exchange and others eligible for membership in the organization. Published studies have supported the hypothesis that a community such as the teleworker community is especially open to management approaches that empower members to take ownership of the responsibility for the security environment. Farmer (2005), in particular, emphasized that teleworkers present a management challenge distinct from that presented by office-based workers. The researchers of the Farmer study recommended a management approach to the teleworking community labeled “situational leadership.” Situational leadership is based on an assumption of open communication and has the aim of promoting a sense of connectedness among remote staff (Farmer, 2005, p. 484).

Herath (2008) and Warner (2009) used the TPB to model user behavior with respect to IT security, and some studies have specifically examined the effect of peer pressure on teleworkers’ attitudes to the security environment (e.g., Hines, 2007, and Hartig et al., 2007). Given the ever-present and increasing threats to security in the telework environment; the increase in teleworking, especially in federal agencies (Mears, 2007); and the publication of foundational research on factors influencing teleworkers’ attitudes to the security environment, it is timely, and likely to be fruitful, to gather data from a sample of current self-identified teleworkers and examine it using the TPB.

3.3 Context of Study

It was considered important that the data for this study be gathered from a community of actual, current, or potential teleworkers. Fortunately, access was available to the membership of The Telework Exchange, a community that self-identifies as actively involved in the telework environment. One feasible topic for preliminary examination was to investigate whether teleworkers present fewer security problems than do regular workers. In other words, was there justification for the widespread assumption that remotely accessing employer data, or transporting data on mobile devices, was riskier than performing work duties in the office environment?

Teleworkers present unique challenges for an organization in implementation-related issues due to the information technology needed to provide teleworkers a secure working environment while implementing IT security controls. This research focused on the relationship between the theory of planned behavior and teleworkers' attitudes about compliance with security requirements in a teleworking environment.

With the lines between work and home increasingly blurred (Antonopoulos, 2007), some of the most challenging questions faced by agencies relate to the difficulty in identifying and assessing the continued security risk and the need to develop and implement effective IT security controls to secure the data of employees who work from home, with or without permission. According to Hines (2007, n.p.), "a fair amount of business users remain oblivious or unconcerned about many of the security issues involved with the use of mobile devices, according to a new study published by Cisco and the National Cyber Security Alliance."

With the vast majority (73%) of the mobile business people surveyed throughout the world giving little thought to security for their mobile devices, a clear and dire need for awareness campaigns exists to alert businesses to the seriousness of security issues (Hines, 2007). The importance of telecommuting and the information security challenges it raises will grow as globalization and the need for flexible work arrangements continue to be important factors in workforce management.

No significant or substantial research or data collection had taken place to allow the use of existing data sets to study this problem. For this reason, a field study of a relevant sample of teleworkers was appropriate and necessary. Access to The Telework Exchange community was available through several means. The General Manager had requested an article for *The Teleworker*, a bi-monthly publication, and a discussion of the research at a Telework Exchange Town Hall meeting to promote the research. The Telework Exchange's website offered to post details regarding the research survey prior, during, and after the study. Having had a good working relationship with the General Manager in the past and her continued support were of great assistance to provide good communication with The Telework Exchange community.

3.3.1 Setting

The Telework Exchange is a public-private partnership focused on demonstrating the tangible value of telework and serving the emerging educational and communication requirements of the federal teleworker community. The Telework Exchange office is in Alexandria, Virginia. The community originated in April 2005 as a joint effort of four companies and the federal government, with a website (www.teleworkexchange.org). In addition, the Telework Exchange includes an advisory board with congressional, Office of

Management and Budget, and industry representatives. The Telework Exchange has grown to a robust organization featuring many capabilities, including telework value calculators, online eligibility gizmo, The Water Cooler collaboration and discussion platform, research studies, *The Teleworker* bi-monthly publication, and major events such as regularly scheduled Town Hall meetings.

The public relations manager, LeeAnn Merritt, is the gatekeeper and point of contact for the purpose of this research. Merritt verbally agreed and approved the posting of a survey link on the website. A working relationship was established with Cindy Auten, General Manager, Telework Exchange, in June 2008 when developing a telework presentation for a group of senior leaders at the Department of Veterans Affairs.

The current research focused on the relationship between the TPB and teleworkers' attitudes about compliance with security requirements in a teleworking environment. The greater reliance on teleworking raises numerous security concerns, including breaches of confidentiality, increased opportunities for unauthorized viewing of data, data theft, and data leakage (Kilpatrick, 2007). Teleworkers present challenges for an agency in implementation-related issues due to the information technology necessary to provide teleworkers a secure working environment while implementing IT security controls.

In the current study, teleworkers were classified as: (a) an official teleworker, an employee who works outside of the official workplace during their regularly scheduled work hours, either at home or an alternative workplace, on a full-time, part-time, or situational basis; (b) a non-teleworker, an employee who works at the official workplace; and (c) an unofficial teleworker, an employee who works at an official workplace, yet also works at home on nights or on weekends.

Teleworkers use various client devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDAs) to read and send email, access Web sites, review and edit documents, and perform many other tasks. Most teleworkers use some type of remote access to an organization's resources and data from locations other than the organization's facilities (National Institute of Standards and Technology [NIST] SP 800-114, 2007). The use of remote devices can increase the chance of security breaches through inadequate training or general carelessness.

3.3.2 Population

The relevant population for this study included persons who considered themselves formal or informal teleworkers. The Telework Exchange, with its membership of federal teleworkers, telework managers, IT professionals, and industry advisors, provided ready access to a relevant sample of this population. The link to the survey instrument on The Telework Exchange website was available to all members of The Telework Exchange and to other individuals with access to the website who were able to choose whether or not to participate.

The sample size was calculated based on the following formula by Yamane (1967, p. 886): $n = N/[1 + N(e)^2]$, where N = population, n = sample size, and e = level of precision. Therefore, $n = 10{,}000/[1 + 10{,}000(.05)^2] = 10{,}000/26 = 385$. An attempt was made to obtain a minimum sample of 385 qualified respondents. The survey link was available on The Telework Exchange website for 30 days. In these 30 days, the Telework Exchange website registered 500 visitors, 180 of whom provided complete sets of responses to the Teleworker Security Survey and of those 150 indicated that the respondent was a teleworker.

3.3.3 Limitations

The Telework Exchange supported the current research, and the gatekeeper verbally granted permission to access relevant materials and subjects. Because the organization is voluntary, no legal or regulatory concerns were encountered. Among the limitations of this research is the consideration that respondents' insight might not be forthcoming if they engaged in informal telework without official approval. The influence of this foreseen factor was reduced, as the methodologies and design of the survey acknowledged the limitation upfront and controlled for it during the analysis. The survey was administered in a way that ensured the greatest level of privacy and was supplemented by an informed consent statement describing the purpose of the study and how the data were to be used, analyzed, and presented (in the aggregate without identifying individual respondents).

Another limitation of the study was that the survey relied on respondents' self-selection: individuals responded because they accessed The Telework Exchange website and had an interest in the topic of the survey. Given the fact that anyone can access this website and take the survey, a question was added to the tool to confirm the telework status of the respondents. Though the desired sample size was 385, only 180 complete a survey and of those 150 indicated that the respondent was a teleworker. Only these 150 complete response sets from teleworkers were used in the analysis. The smaller than needed sample size may pose a limitation to the findings. Although it was practically impossible for the researcher to verify the teleworker status of the respondents, the facts that respondents were accessing the survey tool only through The Telework Exchange website and had no incentives to respond to the survey or identify themselves as teleworkers, are considered sufficient to argue that the sample is a good proxy for the teleworker community. The relatively short duration for the administration of the survey, one month, did not affect the reliability of the conclusions, as the sample of respondents proved to be large enough and representative of the population of formal and informal telecommuters.

Finally, as with every research, a social scientist has to choose a framework of analysis and conduct this analysis through the examination and application of specific theories and a limited number of hypotheses. The presumption is not that the theory of planned behavior is the only possible framework of analysis for the questions examined in this study. It is the theory selected as the lens through which correlations between variables or the lack thereof were examined. The selection of a different theory as the explanatory model or analytical frame would have shifted the focus on different hypotheses and types of correlations, valuable in their own right and constraining the study in a different set of limitations.

3.3.4 Sample Design and Selection

The sample frame for this research was the population of The Telework Exchange, a community of actual, current, or potential formal teleworkers. The organization's membership included federal teleworkers, telework managers, and IT professionals. The Telework Exchange's website averaged about 500 visitors per month. The survey was posted on the Telework Exchange website for 30 days, with the plan to keep it there for the 30-day period or until 150 complete survey responses were received, whichever occurred sooner.

3.4 Feasibility Analysis and Design Selection

To conduct the study, an official request and permission from the Telework Exchange was granted by Cindy Auten, General Manager. Approval to post a link on the Telework Exchange website was obtained by the gatekeeper from the General Manager, as evidenced in Appendix C. In addition, the General Manager requested articles for the bi-monthly publication and a presentation of the research topic at a Telework Exchange Town Hall meeting to promote the research and survey.

The relevant population for this study was persons who considered themselves or were interested in becoming formal teleworkers. This target population was important for the information needed to identify and assess the continued security risk for employees who work from home. The sample represented by The Telework Exchange community included individuals who utilized and managed telework, were teleworkers, or were interested in becoming formal teleworkers. The sample self-selected to participate in the survey based on experience and interest in formal telework, along with the availability of the sample. The attitude of the sample in this study is relevant to the issue of identifying and assessing the continued security risk of employees who work from home.

3.5 Data Collection Plan

The data for this study were gathered from a community of actual, current, or potential teleworkers. Access was available to the membership of The Telework Exchange, a community actively involved in the telework environment. The Telework Exchange’s membership is comprised of over 10,000 federal teleworkers, teleworker managers, IT professionals, and industry advisors. Access was granted to a relevant sample of this population.

3.5.1 Methods of Measurement

The 28-item Teleworker Security Survey (see Appendix D) was developed specifically for the present study and adapted from a similar structured tool used in a study conducted by Herath and Rao (2009). The Teleworker Security Survey consists of 27 items, with nine items each designed to measure the three independent variables presented in Table 1 (i.e., personal attitudes, social pressure, and sense of control). All items on the three independent variable scales, Personal Attitudes, Social Pressure, and Sense of Control, were measured through nine items in each scale, presented on a Likert-type scale with anchors ranging from 1 = *strongly disagree* to 5 = *strongly agree*. Item 28 on The Teleworker Security survey was presented on a rating scale with anchors ranging from 1 = *very unwilling* to 5 = *very willing* to measure the extent to which the respondent indicated a willingness to follow the organization's information security guidelines. The nine items in each of the scales were summed to derive a composite Personal Attitude, Social Pressure, and Sense of Control score to explain willingness to follow an organization's security guidelines.

3.5.2 Instrumentation and Pilot Testing

To establish reliability of the survey instrument, a pilot test of the Teleworker Security Survey was conducted with a sample of 10 teleworker security professionals with knowledge of issues important to establishing and maintaining security in a telework environment. The first aim of the pilot test was to check for problems respondents might have in completing the survey. Pilot study respondents were asked to complete the survey and comment on its length, wording, and instructions. With the objective of strengthening the reliability and validity of the survey instrument, items on the survey were examined on the initial draft for placement and weakness in terms of the definitions from Ajzen's theory of planned behavior (2005).

Based on this feedback, adjustments were made to the final version of the Telework Security survey. Items that best represented the variables to be examined in the study were retained and redundant or confusing items were deleted. The pilot test also provided an opportunity to assess initial validity and reliability levels of survey. Specific steps taken to assess the reliability and validity are explained in greater detail in sections 3.5.3, 3.5.4, and 3.5.5.

3.5.3 Survey Instrument Design and Validation

In survey research, it is important that the survey instrument used is valid and reliable (Nardi, 2003; Straub, 1989; Straub, Boudreau, & Gefen, 2004). Validity of a survey instrument (or any other measurement) means that it measures what it is intended to measure (Nardi, 2003; Straub, 1989). Reliability means that the survey results are consistent–that all things being equal, the results of the survey are essentially the same for a given set of research participants each time they complete the survey (Kline, 2000; Nardi, 2003; Straub, 1989). Straub (1989) presented a model for validating research instruments. The model includes the following steps (Straub, 1989).

1. Establish instrument validity

   a. "Face" Validity
   b. Content Validity

2. Establish instrument reliability

   a. Cronbach's Alpha (α)
   b. Pearson's correlation (*r*)

To validate the survey instrument used in this study, several pre-testing methods were used. Content validity was established through a literature review, a peer review, and a pilot test.

3.5.4 Instrument Validity

The validity of an instrument refers to the appropriateness, meaningfulness, and usefulness of specific inferences made from test scores (Gall, Borg, & Gall, 2006). Because an existing survey that specifically addressed willingness to follow security guidelines and factors related to the personal attitudes, social pressure, and sense of control factors as outline in the theory of planned behavior (Ajzen, 2005) was not found, the Teleworker Security survey was developed specifically for the present study. The extent that the survey covered the relevant variables and conceptual domains was assessed initially using face validity based on the subjective impression of this researcher, two information security experts, and the 10 information security professionals who participated in the pilot study to inspect the survey's constituent items visually to evaluate the thoroughness of content coverage.

The face validity of a survey instrument is the degree to which it "*appears* [italics added] to measure what it *claims* [italics added] to measure" (Kline, 2000, p. 30). The content validity of a survey may be established through literature reviews; a peer-review process, where "experts in the field" examine the survey instrument and concur that it accurately measures the constructs it is intended to measure; or both (Straub, 1989; Straub et al., 2004; Yun & Ulrich, 2002). Pre-testing the survey among a group of subject matter experts provided additional content validation of the survey (Fink & Kosecoff, 1998).

The first steps in establishing the validity of this survey were to establish its face and content validity (Bailey, 1987; Kline, 2000; Straub, 1989; Straub et al., 2004). A review of the extant literature took place and is included in Chapter 2. The literature review provided several conceptual constructs for evaluation, which were used repeatedly to update and modify the survey questions. Once the final draft of the Teleworker Security survey was developed, it was examined by the two information security experts with experience in designing and conducting survey research, as well as by the 10 information security professionals who completed the pilot testing of the survey.

Through an iterative process of review, evaluation, and modification, based on the security professionals’ experience in conjunction with an examination of literature on establishing and maintaining information security, the survey was determined to adequately measure the concepts of interest in the present study. However, because the content validity of the survey was established using two experts and the 10 professionals who completed the survey, this limited the scope of the evaluation and thus the extent to which the survey accurately represents the variables being studied may be limited.

3.5.5 Instrument Reliability

Instrument reliability was established through a test-retest pilot of 10 information security professionals. According to Carmines and Zeller (1979), the test-retest method is, “one of the easiest ways to establish the reliability of empirical measurements” (Carmines & Zeller, 1979, p. 29). The use of a test-retest approach is extremely important in assessing the reliability of a survey instrument (Kline, 2000; Nardi, 2003). In a test-retest approach, the same survey instrument is presented to the same group of participants twice, separated by a period of two to four weeks (Carmines & Zeller, 1979; Kline, 2000; Nunnally, 1964, 1972). The two- to four-week period between the test and retest was recommended by Nunnally (1964), primarily to offset errors in the test's assessment due to day-to-day fluctuations in the responses of individuals taking the test, "the largest source of measurement error in most tests" (Nunnally, 1964, p. 77).

Nunnally (1964) noted that a respondent's memory of the survey and his or her previous answers may cause the correlation between the test and retest to be artificially high. However, other factors may artificially lower the correlation between the test and retest results, such as a change in the underlying theoretical concepts and reactivity (Carmines & Zeller, 1979). Changes in the underlying theoretical concepts are increasingly likely to occur as the time between the test and retest increases (Carmines & Zeller, 1979). Reactivity is the tendency of a respondent to pay more attention to the subject of the survey, due to having been asked about it: the fact of measuring something changing the nature of the thing being measured (Carmines & Zeller, 1979).

Instrument reliability refers to the consistency, stability, and precision of test scores over repeated sessions given over time (Gall et al., 1996). Internal consistency reliability was assessed because several items were summed to derive a scale score. Internal consistency was assessed using Cronbach's (1951) internal consistency reliability coefficient alpha. Nunnally (1964) posed that in the early stages of research, reliabilities of 0.50 to 0.60 are acceptable and that a level of 0.80 is desirable for basic research (p. 226). The Cronbach alpha scores for the three independent variables scales were as follows: (1) Personal Attitude Scale, $\alpha = .6679$; (2) Social Pressure Scale, $\alpha = .6572$; and (3) Sense of Control Scale, $\alpha = .8059$.

3.5.6 Data Collection Procedures

Data collection was accomplished through the use of an online survey hosted on the Internet site Survey Monkey (www.surveymonkey.com). SurveyMonkey is a web-based, survey-writing program that allows the researcher complete control over the design and administration of the survey. SurveyMonkey allows the researcher to (a) provide a link from an e-mail to the web-based survey, (b) export data directly into a spreadsheet or statistical analysis program (e.g., SAS, SPSS) data file for later detailed analysis, (c) password protect access to the survey, and (d) control the repeated access to the survey by a single respondent.

A link to the survey was available through the electronic means of e-mail and posting on The Telework Exchange website. After the conclusion of the survey availability period, the survey results were downloaded and analyzed by the researcher. The data collected did not contain any identifying information about the participants. The parameters of the survey were restricted to responses by IP address to lock out respondents from submitting more than one survey once their responses to the survey had been submitted. In cases where respondents inadvertently provided personal information, the researcher did not make any contact with the respondent. All data collected will be destroyed within 24 months of a successful dissertation defense, but no later than 36 months after the survey was closed.

3.5.7 Data Coding

The survey instrument utilized a 5-point Likert-type semantic differential scale. The five points on the scale ranged from 1 = *strongly disagree* to 5 = *strongly agree* for the independent variables. This 5-point scale was used for each question, excluding the demographic questions. The survey (see Appendix D) consisted of 27 questions with an equal distribution of questions designed to measure each of the three variables presented in Table 3 (i.e., attitudes, subjective norms, perceived behavioral control). Three independent variables included (1) Personal Attitude, survey items 1 to 9; Social Pressure, items 10 to 18; and Sense of Control, items 19 to 27. The survey included one question on the dependent variable. This variable used a 5-point willingness scale ranging from 1 = *very unwilling* to 5 = *very willing*. The additional demographic questions of the survey were not used for this research. A Likert-type scale was used because it included equal intervals between the points. Additionally, each point represented an order (from *strongly disagree* to *strongly agree*, 1-5) that could be represented incrementally.

3.5.8 Data Collected

Data were collected through the survey and interpreted through an analysis of the survey results. Items measuring personal attitude, social pressure, and sense of control were measured by the respondent's agreement or disagreement with statements on the survey.

The first independent variable, personal attitude, was measured by respondents' agreement or disagreement with statements relating telework and the importance of the security of organizational data and the consequences of loss or theft both to the organization and to the respondent, as well as with statements relating to security, confidentiality, and privacy in a broader social and personal context.

The second independent variable, social pressure, was measured by respondents' agreement or disagreement with statements relating telework and the extent to which employees, managers, and policies created pressure to either comply or not comply with practices and whether other employees' compliance with good security practices was likely or unlikely to influence the respondents' compliance.

The third independent variable, the sense of control, was measured by respondents' agreement or disagreement with statements relating to telework and the extent to which they believed their own actions and decisions were likely or unlikely to prevent loss or theft of organizational data; the extent to which they felt they participated in the creation and maintenance of a security environment; and their agreement or disagreement with the proposition that IT security problems required a technical rather than a personal solution.

In relation to the theoretical framework, the results of the survey provided a basis for evaluating whether the subjective norm alone was more predictive of willingness to take ownership of the security environment than subjective norm combined with the other two variables. Because the subjective norm encompassed peer pressure (Ajzen, 2005), it provided a strong indication of whether the TPB is a more useful explanatory model in this context. SurveyMonkey was used to export data directly into a spreadsheet or statistical analysis program (SPSS) data file for detailed analysis.

Chapter 4

Results and Findings

4.1 Data Analysis Plan

The data for this research was collected using The Teleworker Exchange survey made available to respondents on SurveyMonkey, a web-based survey-hosting site. The survey responses were downloaded to a Microsoft Excel spreadsheet and then converted to a SPSS 11.5 version compatible file.

4.1.1 Analysis Procedures

The analysis of the survey data consisted of both descriptive and inferential statistical techniques to identify and any relationships and group differences in scores on the survey items and composite scale scores. Regression analysis was conducted to determine how well the scores on Personal Attitude, Social Pressure, and Sense of Control scales explained willingness to follow an organization's security guidelines.

4.1.2 Methods of Analysis

The data collected for this study were downloaded in Microsoft Excel format and checked for validity and missing data. The Microsoft Excel spreadsheet was then converted into an SPSS document for analysis. Descriptive statistics were generated and correlational analyses took place to determine if any significant relationships existed between the dependent and independent variables. In addition, regression analysis was performed to assess how well the three independent variables explained the dependent variable.

4.2 Results

The objective of this study was to examine teleworkers' attitudes regarding compliance with security requirements in a teleworking environment using the Ajzen's theory of planned behavior. In this chapter, the findings of descriptive and inferential analysis of the data are presented as they pertain to the research questions presented in Chapter 1. As described in Chapter 3, the teleworkers' attitudes, perceptions of social pressure, and sense of control were investigated using a 28-item survey developed for the present study.

4.2.1 Descriptive Analysis of the Study Variables

Respondents completed a web-based version of the Telework Exchange Survey made available through SurveyMonkey. Through a link provided on The Telework Exchange website, a sample of 150 members agreed to participate in the study and completed an online survey. A combination of descriptive and inferential statistics was used to answer the research questions

4.2.1.1 Willingness to Follow Information Security Policies

Teleworkers indicated that they were strongly willing to follow the organization's information security guidelines (*M* = 4.71 on a scale from 1 = *strongly disagree* to 5 = *strongly agree*) (see Table 1).

Table 1. Descriptive Statistics for Item 28 "Willingness to Follow the Organization's Information Security Guidelines" (N=150)

Item	Willingness	M	M_n	M_d	SD
28	Please indicate the degree of your willingness to follow the organization's information security guidelines.	4.71	5.0	5.0	.483

4.2.1.2 Personal Attitude Scale

Descriptive statistics were generated for scale items and composite scale scores. The nine items of the Personal Attitude Scale were used to generate a Personal Attitude Scale composite score. These items were presented in a 5-point Likert-type scale format ranging from 1 = *strongly disagree* to 5 = *strongly agree* and dealt with teleworkers' perceptions about their willingness to follow an organization's information security guidelines. The mean ratings for the nine attitude scale items ranged from a high of 4.77 (*strongly agree*) for item 3, referring to a belief that understanding the importance of information security and practices is important, to a low of 3.03 (*neutral*) for item 6, referring to attitudes about an organization terminating employees who break the security rules (see Table 2).

Responses to items of the Personal Attitude Scale indicated that teleworkers recognized the importance of information security. The highest rated items concerned teleworkers' attitudes about the importance of maintaining and protecting the integrity of data (items 1, 2, 3, and 7). Teleworkers strongly recognized the importance of information security and practices (item 3, M = 4.77). Teleworkers also indicated a strong belief that there is a serious need to protect information data (item 2, M = 4.47), that adopting security technologies and practices in a telework environment are important (item 7, M = 4.42), and that information stored on an organization's computers is vulnerable to security incidents (item 1, M = 4.38).

The lowest-rated items were teleworkers' perceptions about employee discipline for breaking security policies and being asked to sign a telework statement to protect the security of data (items 4, 5, 6, 8, and 9). Teleworkers were neutral in ratings of the extent that the organization disciplines employees who break information security rules (item 4, *M* = 3.15) or terminates those who repeatedly break security rules (item 6, *M* = 3.03). Teleworkers were neutral in their beliefs that the organization communicates the importance of confidentiality and privacy of data (item 8, *M* = 3.55) and that they would be disciplined if caught violating information security policies (item 5, *M* = 3.645. Most were neutral in their rating that they had been asked to sign a statement to protect and maintain the value of data and its integrity (item 9, *M* = 3.17). Finally, the composite Personal Attitude Scale score of 34.57 out of a possible 45 (3.84 on a scale from 1 to 5) indicated that, overall, teleworkers' beliefs were from *neutral* to *agree* that it is important to maintain the security and integrity of the organization's data.

Table 2 Multiple Regression Descriptive Statistics for the Nine Items of the Personal Attitude Scale

	Variable	*M*	*SD*
	Willingness	4.71	.483
1	I believe that information stored on organization computers is vulnerable to security incidents.	4.38	.941
2	Information security and data protection associated with telework are serious and need attention.	4.47	.835
3	Understanding the importance of information security and practices is important.	4.77	.441
4	My organization disciplines employees who break information security rules.	3.15	1.184
5	If I were caught violating my organization information security policies, I would be disciplines.	3.65	1.065
6	My organization terminates employees who repeatedly break security rules.	3.03	1.213
7	Adopting security technologies and practices is important in a telework environment.	4.42	.690
8	My organization communicates the importance of confidentiality and privacy of data periodically.	3.56	1.129
9	I am asked to sign a telework statement to protect and maintain the value of data and its integrity periodically.	3.17	1.195
	Personal Attitude Scale Score	34.57	4.700

4.2.1.3 Social Pressure Scale

The nine questions of the Social Pressure Scale were used to generate a Social Pressure Scale composite score. These questions were presented in a 5-point Likert-type scale format ranging from 1 = *strongly disagree* to 5 = *strongly agree* and dealt with teleworkers' perceptions about their willingness to follow an organization's information security guidelines. The mean ratings for the nine Social Pressure Scale items ranged from a high of 4.48 (*strongly agree*) for item 17, the belief that every employee can make a difference when it comes to securing an organization's data in a telework environment to a low of 2.17 (*disagree*) for item 14, belief that an their organization's information security procedures in a telework environment are unreasonable (see Table 3).

The highest rated items were employees' perceptions of social pressure in terms of making a difference in maintaining security integrity and feeling social pressure from others to follow security procedures in a telework environment (items 10, 12, 16, 17, 18). Teleworkers believed strongly that every employee can make a difference when it comes to helping secure data in a telework environment (item 17, *M* = 4.48). In addition, teleworkers believed strongly that they would follow the directions of their managers regarding security measures to use to protect the organization's data (item 12, *M* = 4.33). Teleworkers were neutral to being in agreement in their perceptions about the extent they encourage co-workers to follow security procedures (item 16, *M* = 3.72), belief that others comply with security procedures (item 18, *M* = 3.51), and the influence of a manager's attitude toward the seriousness of teleworkers to maintain information security (item 10, *M* = 3.48).

The lowest rated items were teleworker perceptions about the unreasonableness of security policies (item 14, *M* = 2.17) and monitoring frequency of violations to security policies (item 13, *M* = 2.99). Teleworkers are neutral in their perception about how much other employees pressured them to follow information security procedures (item 11, *M* = 3.03) and neutral to moderate agreement about the clarity of how to protect data is provided by the organization (item 15, *M* = 3.35). Finally, the composite Social Pressure Scale score of 31.04 out of a possible 45 (2.34 on a scale from 1 to 5) indicated that, overall, teleworkers' beliefs were from *neutral* to *disagree* that social pressure played a significant role in their understanding of how to protect the organization's data or to following information security procedures.

Table 3Multiple Regression Descriptive Statistics for the Nine Items of the Social Pressure Scale

	Variable	*M*	*SD*
	Willingness	4.71	.483
10	My manager's attitude information security when teleworking is serious.	3.48	1.076
11	My colleagues, who follow the information security procedures, create pressure forcing me to follow them.	3.03	.993
12	If a manager told me of security measures I should be taking that I was currently not taking, I would follow the manager's advice.	4.33	.526
13	Telework practices in my organization are frequently monitored for policy violations.	2.99	1.049
14	My organization information security procedures in a telework environment are unreasonable.	2.17	.820
15	My organization's information security procedures are clear on how to protect organization's data in a telework environment.	3.35	1.006
16	I have encouraged other employees to take steps to ensure organization's data is protected in a telework environment.	3.72	.823
17	Every employee can make a difference when it comes to helping to secure the organization's data in telework environment.	4.48	.622
18	I am convinced other employees comply with the organizations telework guidelines	3.51	.991
	Social Pressure Scale Score	31.07	4.17

4.2.1.4 Sense of Control Scale

The nine questions of the Sense of Control scale were used to generate a Sense of Control scale composite score. These questions were presented in a 5-point Likert-type scale format ranging from 1 = *strongly disagree* to 5 = *strongly agree* and dealt with teleworkers' perceptions about their willingness to follow an organization's information security guidelines. The mean ratings for the nine Sense of Control Scale items ranged from a high of 4.45 (*strongly agree*) for item 21, referring to a belief that taking proper security measures of data is in one's control and personal responsibility, to a low of 2.41 (*disagree*) for item 25, that security measures of the organization are restrictive to the telework environment and interfere with one's job performance (see Table 4).

The highest rated items concerned teleworker sense of control over taking proper measures and following security policies and practices to protect data in a telework environment (items 19, 20, 21, 22, and 24). Teleworkers believed strongly that they were responsible for and were in control of taking proper security measure to secure the integrity of data (item 21, *M* = 4.45). Teleworkers also indicated strong beliefs in following information security policies (item 22, *M* = 4.41) and taking steps to ensure that data were protected when teleworking (item 19, *M* = 4.22). Teleworkers were in agreement with the perceptions of a sense of control over reducing threat (item 20, *M* = 4.19) and the extent that involvement in information security programs makes teleworkers adhere to them (item 24, *M* = 4.01).

The lowest rated items were teleworker perceptions about having the knowledge to protect the data, dealing with technical issues, proper monitoring, and how restrictive data security policies were in the telework environment (items 23, 25, 26, 27). Teleworkers were in agreement that they had enough knowledge to protect the data in a telework environment (item 23, *M* = 3.95).Teleworkers were neutral in their perceptions about the technical solutions necessary to implement information security policies (item 26, *M* = 3.20) and how teleworker computer practices were properly monitored for policy violations (item 27, *M* = 2.99). Teleworkers disagreed that an organization's computer equipment procedures were restrictive and interfere with job performance (item 25, *M* = 2.41). Finally, the composite Sense of Control Scale score of 33.79 out of a possible 45 (3.75 on a scale from 1 to 5) indicated that, overall, teleworkers slightly agreed that they had the responsibility and ability to protect information data in a telework environment.

Table 4 Multiple Regression Descriptive Statistics for the Nine Items of the Sense of Control Scale

	Variable	*M*	*SD*
	Willingness	4.72	.482
19	I have personally taken steps to ensure organization data is protected when teleworking.	4.22	.717
20	When organizational data is in my control, security threats are minimized.	4.19	.663
21	Taking proper security measures of data in my control is my personal responsibility.	4.45	.620
22	I am likely to follow organization information security policies when working in a telework environment	4.41	.571
23	I have enough knowledge to protect organization data in telework environment.	3.95	.777
24	My involvement in information security programs makes me adhere to them.	4.01	.709
25	My organization's computer equipment procedures are so restrictive in a telework environment that it interferes with my job performance.	2.41	.975
26	Information security requires more technical solutions in a telework environment.	3.20	1.069
27	Employee computer practices are properly monitored in a telework environment for policy violations.	2.99	.997
	Sense of Control Scale	33.79	3.640

4.2.2 Analysis and Findings for Study Question

4.2.2.1 Research Question

To what extent are there relationships between personal attitudes, perceptions of social pressure, and sense of control and teleworkers' willingness to follow an organization's information security guidelines?

4.2.2.1a Personal Attitudes.

RQ1a. To what extent are there relationships between items on the Personal Attitude scale and teleworkers' willingness to follow an organization's information security guidelines?

$H1a_0$: There is no relationship between items on the Personal Attitude Scale and teleworkers' willingness to follow an organization's information security guidelines.

$H1a_a$: There is a relationship between items on the Personal Attitude Scale and teleworkers' willingness to follow an organization's information security guidelines.

A multiple regression analysis was used to examine the relationship between items on the Personal Attitude Scale and willingness to following an organization's information security guidelines. While several correlations were statistically significant, these correlations were weak. Though considered statistically significant due to sample size, no real relationship was identified between willingness to following security procedures (dependent variable) and several items on the Personal Attitude Scale (see items 1, 2, 4, 5, 6, 8, and 9) (see Table 5). The strongest correlations between the dependent variable, willingness to follow an organization's information security guidelines and Personal Attitude Scale items were noted for items 3 and 7. There was a weak to moderate relationship between perceptions of understanding the importance of information security and practices (item 3) and willingness to follow security procedures (*r* = .314) and belief that adopting security technologies and practices is important in a telework environment (item 7, *r* = .267).

There was a relationship noted between the overall Personal Attitude scale score and the dependent variable of willingness to follow security guidelines (*r* = .188, *p* < .05). Therefore, results failed to reject the alternative hypothesis that there is a relationship between willingness to follow security policies and Personal Attitude scale. However, while relationships were noted, they were weak or very weak.

Table 5 Multiple Regression Correlations Between the Dependent Variable "Willingness to Follow an Organization's Information Security Guidelines" and Personal Attitude Scale Items and Composite Score

#	Personal Attitude	*r*
1	I believe that information stored on organization computers is vulnerable to security incidents	.062
2	Information security and data protection associated with telework are serious and need attention.	.070
3	Understanding the importance of information security and practices is important.	$.314^{***}$
4	My organization disciplines employees who break information security rules.	.078
5	If I were caught violating my organization information security policies, I would be disciplined.	.052
6	My organization terminates employees who repeatedly break security rules.	.071
7	Adopting security technologies and practices is important in a telework environment.	$.267^{***}$
8	My organization communicates the importance of confidentiality and privacy of data periodically.	$.152^{*}$
9	I am asked to sign a telework statement to protect and maintain the value of data and its integrity periodically.	.029
	Personal Attitude Scale Score	$.188^{*}$

Note: * p < .05; **p < .01; ***p <.001.

The regression analysis was performed in order to assess how well the nine items on the Personal Attitude Scale explained the dependent variable of willingness to following an organization's information security guidelines (See Table 6). The unstandardized β

coefficients indicated that Personal Attitudes Scale items did not appreciably influence willingness to follow security guidelines. The standardized β coefficients showed that the personal attitude scale contributed little to the model. Finally, based on the ANOVA from the regression analysis, the Personal Attitude model was statistically significant, $F(9,139) = 3.274$, $p < .001$. Based on this significant finding, the results failed to reject the alternative hypothesis that there is a relationship between items on the Personal Attitude scale and the dependent variable willingness to follow an organization's security guidelines. However, standardized β coefficients ranged from a low of -.035 for item 5, "If I were caught violating my organization information security policies, I would be disciplined," to a high of .362 for item 3, "Understanding the importance of information security and practice is important." Based on these standardized β coefficients, it is concluded that the items on the scale have only a slight influence on the criterion variable. In addition, the R for the model was .418, with $R^2 = .175$ and adjusted $R^2 = .121$, indicating that, overall, the model is a weak model because only 12.1% of the variance in the criterion variable of willingness to follow and organization's security guidelines was explained by the Personal Attitude predictor variable.

Table 6 Regression Analysis Summary for the Nine Personal Attitude Predictor Variables Predicting Willingness to Follow Organization's Information Security Guidelines

		B	SEB	*β*	*t*	Sig.
	Constant	2.40	.48		5.02	.001
1	I believe that information stored on organization computers is vulnerable to security incidents.	.08	.06	.155	1.45	.001
2	Information security and data protection associated with telework are serious and need attention.	-.12	.07	-.198	-1.66	.099
3	Understanding the importance of information security and practices is important.	.39	.11	.362	3.75	.001
4	My organization disciplines employees who break information security rules.	.05	.05	.130	.99	.332
5	If I were caught violating my organization information security policies, I would be disciplined.	-.02	.05	-.051	-.46	.646
6	My organization terminates employees who repeatedly break security rules.	-.01	.49	-.035	-.28	.780
7	Adopting security technologies and practices is important in a telework environment.	.11	.07	.150	1.60	.113
8	My organization communicates the importance of confidentiality and privacy of data periodically.	.07	.05	.160	1.43	.155
9	I am asked to sign a telework statement to protect and maintain the value of data and its integrity periodically.	-.05	.04	-.132	-1.40	.163

4.2.2.1b Social Pressure.

RQ1b. To what extent are there relationships between items on the Social Pressure scale and teleworkers' willingness to follow an organization's information security guidelines?

H1b$_0$: There is no relationship between items on the Social Pressure Scale and teleworkers' willingness to follow an organization's information security guidelines.

H1b$_a$: There is a relationship between items on the Social Pressure Scale and teleworkers' willingness to follow an organization's information security guidelines.

A multiple regression analysis was used to examine the relationship between items on the Personal Attitude Scale and willingness to following an organization's information security guidelines. While several correlations were statistically significant, the correlations were weak. No real relationship, or a negligible relationship, was noted between willingness to following security procedures (dependent variable) and several items on the Social Pressure scale (see items 10, 11, 13, 15, 16, and 18) (see Table 7).

The strongest correlations between the dependent variable, willingness to follow an organization's information security guidelines and Social Pressure Scale items were noted for items 12, 14, and 17. There was a weak to moderate relationship between beliefs that every employee can make a difference when it comes to helping secure an organization's data and willingness to following information security guidelines (item 17, *r* = .400) and following managers' advice on security measures to take (item 12, *r* = .349). A weak to moderate negative correlation was noted between willingness to follow security guidelines and perceptions that telework security procedures are unreasonable (item 14, *r* = -.384). In other words, as willingness to following procedures increases, the perceptions of security guidelines are unreasonable decreases.

There was a relationship noted between the overall Social Pressure Scale score and the dependent variable of willingness to follow security guidelines (*r* = .188, p < .05). Therefore, results failed to reject the alternative hypothesis that there is a relationship between willingness to follow security policies and the Social Pressure Scale. However, while significant relationships were noted, they were weak or very weak.

Table 7 Multiple Regression Correlations Between Dependent Variable "Willingness to Follow an Organization's Information Security Guidelines" and Social Pressure Scale Items and Composite Score

#	Social Pressure	*r*
10	My manager's attitude information security when teleworking is serious.	$.257^{**}$
11	My colleagues, who follow the information security procedures, create pressure forcing me to follow them.	.073

12	If a manager told me of security measures I should be taking that I was currently not taking, I would follow the manager's advice.	.349***
13	Telework practices in my organization are frequently monitored for policy violations.	.049
14	My organization information security procedures in a telework environment are unreasonable.	-.384***
15	My organization's information security procedures are clear on how to protect organization's data in a telework environment.	.153*
16	I have encouraged other employees to take steps to ensure organization's data is protected in a telework environment.	.219*
17	Every employee can make a difference when it comes to helping to secure the organization's data in telework environment.	.400***
18	I am convinced other employees comply with the organizations telework guidelines.	.168*
	Social Pressure Scale Score	.244**

Note: * p < .05; **p < .01; ***p <.001.

The regression analysis was performed to assess how well the nine items on the Social Pressure Scale explained the dependent variable of willingness to following an organization's information security guidelines (See Table 8). The unstandardized β coefficients indicated that Social Pressure Scale items did not appreciably influence willingness to follow security guidelines. The standardized β coefficients showed that the social pressure scale score contributed little to the model. Finally, based on the ANOVA from the regression analysis, the Social Pressure model was statistically significant, $F(9,139) = 6.893$, $p < .001$. Based on this significant finding, results failed to reject the alternative hypothesis that there is a significant relationship between items on the Social Pressure Scale and the dependent variable willingness to follow an organization's security guidelines. However, standardized β coefficients ranged from a low of .019 for item 11, "My colleagues, who follow the information security procedures, create pressure forcing me to follow them," to a high of .255 for item 17, "Every employee can make a difference when it come to helping to secure the organization's data in a telework environment." Based on these standardized β coefficients, the items in the scale have only a moderate influence on the criterion variable. In addition, the *R* for the model was .556, with R^2 = .309 and adjusted R^2 = .264, indicating that overall, the model is a weak to moderate model because 26.4% of the variance in the criterion variable of willingness to follow an organization's security guidelines was explained by the Social Pressure predictor variable.

4.2.2.1c Sense of Control.

RQ1c. To what extent are there relationships between items on the Sense of Control Scale and teleworkers' willingness to follow an organization's information security guidelines?

$H1c_0$: There is no relationship between items on the Sense of Control Scale and teleworkers' willingness to follow an organization's information security guidelines.

$H1c_a$: There is a relationship between items on the Sense of Control Scale and teleworkers' willingness to follow an organization's information security guidelines.

Table 8 Regression Analysis Summary for Social Pressure Predictor Variables Predicting Willingness to Follow Organization's Information Security Guidelines

		B	SEB	*β*	*t*	Sig.
	Constant	3.02	.44		6.83	.001
10	My manager's attitude information security when teleworking is serious.	.05	.04	.12	1.20	.232
11	My colleagues, who follow the information security procedures, create pressure forcing me to follow them.	.01	.049	.02	.24	.808
12	If a manager told me of security measures I should be taking that I was currently not taking, I would follow the manager's	.16	.07	.18	2.23	.028
13	Telework practices in my organization are frequently monitored for policy violations.	.03	.04	-.07	-.86	.399
14	My organization information security procedures in a telework environment are unreasonable.	-.14	.05	-.23	-2.89	.004
15	My organization's information security procedures are clear on how to protect organization's data in a telework	-.02	.05	-.04	-.41	.683
16	I have encouraged other employees to take steps to ensure organization's data is protected in a telework environment.	.06	.05	.10	1.22	.226
17	Every employee can make a difference when it comes to helping to secure the organization's data in telework	.19	.06	.26	3.28	.001
18	I am convinced other employees comply with the organizations telework guidelines	.04	.04	.08	1.01	.315

A multiple regression analysis was used to examine the relationship between items on the Sense of Control Scale and willingness to following an organization's information security guidelines. Several weak, but correlations were noted. No real relationship, or a negligible relationship, was noted between willingness to following security procedures (dependent variable) and several items on the Sense of Control Scale (see items 23, 24, 26, and 27) (see Table 9).

The strongest correlations between the dependent variable, willingness to follow information security guidelines, and Sense of Control scale items were noted for items 19, 20, 21, and 22. There were low to moderate correlations between willingness to follow security guidelines and perceptions about responsibility for and taking proper security measures to protect data (item 21, *r* = .4527) and likelihood of following information security policies when working in a telework environment (item 22, *r* = .453). There were weak to moderate relationships in terms of perceptions that one personally can take steps to ensure data is protected in a teleworking environment (item 19, *r* = .381) and that when organizational data is in one's control, security threats are minimized (item 20, *r* = .361).

While two items on the Sense of Control Scale showed significant moderate relationships, overall, there was a weak correlation between the Sense of Control composite scale score and willingness to follow security guidelines (*r* = .346). Therefore, results failed to reject the null hypothesis that there is no real relationship between willingness to follow security policies and the Sense of Control Scale.

Table 9 Multiple Regression Correlations Between the Dependent Variable "Willingness to Follow an Organization's Information Security Guidelines" and Sense of Control Scale Items and Composite Score

#	Sense of Control	*r*
19	I have personally taken steps to ensure organization data is protected when teleworking.	.373***
20	When organizational data is in my control, security threats are minimized.	.336***
21	Taking proper security measures of data in my control is my personal responsibility.	.459***
22	I am likely to follow organization information security policies when working in a telework environment	.430***
23	I have enough knowledge to protect organization data in telework environment.	.196*
24	My involvements in information security programs makes me adhere to them.	.207*
25	My organization's computer equipment procedures are so restrictive in a telework environment that it interferes with my job performance.	-.224**
26	Information security requires more technical solutions in a telework environment.	.014
27	Employee computer practices are properly monitored in a telework environment for policy violations.	.070
	Sense of Control Scale	.346***

Note: * p < .05; **p < .01; ***p <.001.

The regression analysis was performed to assess how well the nine items on the Sense of Control Scale explained the dependent variable of willingness to following an organization’s information security guidelines (See Table 10). The unstandardized β coefficients indicated that sense of control scale items did not appreciably influence willingness to follow security guidelines. The standardized β coefficients showed that the Sense of Control scale score contributed little to the model. Finally, based on the ANOVA from the regression analysis, the Sense of Control model was statistically significant, $F(9,139) = 6.442$, $p < .001$. Based on this statistically significant finding, results failed to reject the alternative hypothesis that there is a relationship between items on the Sense of Control Scale and the dependent variable willingness to follow an organization’s security guidelines. However, standardized β coefficients ranged from a low of -.029 for item 27, “Employee computer practices are properly monitored in a telework environment for policy violations,” to a high of .247 for item 22, “I am likely to follow organization information security policies when working in a telework environment.” Based on these standardized β coefficients, the items in the scale have only a weak influence on the criterion variable. In addition, the R for the model was .544, with $R^2 = .296$ and adjusted $R^2 = .250$, indicating that overall, the model is a weak to moderate model because 26.0% of the variance in the criterion variable of willingness to follow an organization’s security guidelines was explained by the Sense of Control predictor variable.

Table 10 Regression Analysis Summary for Sense of Control Scale Predictor Variables Predicting Willingness to Follow Organization's Information Security Guidelines

		B	SEB	*β*	*t*	Sig.
	Constant	2.85	.35		8.25	.001
19	I have personally taken steps to ensure organization data is protected when teleworking.	.09	.06	.13	1.41	.160
20	When organizational data is in my control, security threats are minimized.	.09	.07	.11	1.05	.294
21	Taking proper security measures of data in my control is my personal responsibility.	.13	.08	.17	1.61	.110
22	I am likely to follow organization information security policies when working in a telework environment	.21	.08	.25	2.52	.013
23	I have enough knowledge to protect organization data in telework environment.	-.09	.06	-.15	-1.60	.112
24	My involvements in information security programs makes me adhere to them.	.05	.06	.07	.79	.432
25	My organization's computer equipment procedures are so restrictive in a telework environment that it interferes with my job performance.	-.07	.04	-.15	-.20	.045
26	Information security requires more technical solutions in a telework environment.	.02	.04	.04	.57	.572
27	Employee computer practices are properly monitored in a telework environment for policy violations.	-.01	.04	-.03	-.37	.710

4.2.2.2 Regression Analysis

Regression analysis was performed to assess how well the three independent variables (Personal Attitude, Social Pressure, and Sense of Control) explained the dependent variable of willingness to following an organization's information security guidelines (See Table 11). The unstandardized *β* coefficients indicated that personal attitudes and social pressure did not appreciably influence willingness to follow security guidelines. The standardized β coefficients showed that both the Personal Attitude and Social Pressure Scale scores contributed little to the model. Finally, the Sense of Control Scale score was the only statistically significant predictor variable, *t*(3, 45) = 3.212, *p* = .002. However, though statistically significant, the standardized β coefficient of .325

indicated that this variable had only a slight influence on the criterion variable. In addition, the *R* for the model was .352, with R^2 = .124 and adjusted R^2 = .106, indicating that overall the model is a poor model because only 10.6% of the variance in the criterion variable of willingness was explained by the predictor variables.

Table 11. Regression Analysis Summary for Predictor Variables Predicting Willingness to Follow Organization's Information Security Guidelines.

	B	SEB	*β*	*t*	Sig.
Constant	3.126	.368		8.497	.000
Personal Attitude	-0.005	.011	-0.052	-.495	.621
Social Pressure	0.100	.012	0.087	.830	.408
Sense of Control	0.043	.013	0.325	3.212	.002

4.3 Findings

Overall, teleworkers strongly agreed they were willing to follow the organization's information security guidelines. In terms of personal attitudes, teleworkers believed strongly that information data was vulnerable and that it was important for an organization to have security policies and procedures in place to protect the confidentiality and integrity of the data stored on computers. They also considered it important that teleworkers took the advice of managers as well as adopted security technologies and practices that helped protect data. Teleworkers indicated that they were often not required to sign a statement indicating they would protect the security of data. In addition, they did not express strong agreement that the organization communicated effectively the need to protect data used on their computers.

In terms of social pressure, teleworkers believed strongly that every employee could make a difference when it came to securing an organization's data in a telework environment and that they would follow advice from their managers on how to increase the security of information data. In terms of feeling pressure from co-workers, teleworkers indicated that they felt some pressure, but, overall, were fairly neutral on pressure from co-workers to adhere to security policies and practices. Finally, teleworkers did not feel that their organizations' security procedures were restrictive or that employees who broke security rules were often disciplined or terminated for security breaches.

In terms of sense of control, teleworkers believed strongly that they were responsible for and had the ability to follow security policies and practices to protect the security of the data contained on their computers. They indicated that when they were involved in information security programs, they were more likely to adhere to security policies and procedures. In addition, teleworkers believed that they had knowledge to understand security risks and how to protect against security breaches. Overall, teleworkers did not believe that computer practices were monitored consistently for policy violations. They did not feel the security protocols used by their organization were unreasonable or that they interfered with the ability to do their work.

Overall, the analysis found weak relationships between the dependent variable willingness to follow security guidelines and the independent variables, composite scores on the Personal Attitude Scale, Social Pressure Scale, and Sense of Control Scale. While the regression analysis resulted in significant *F* values, these were most likely based on sample size. The adjusted R^2 for the three independent variables indicated that they were weak to moderate at explaining the willingness of teleworkers to following organizational security guidelines. Even so, those teleworkers who held the strongest personal attitude, social pressure, and sense of control beliefs were more willing to follow their organization’s security guidelines.

Chapter 5

Implications and Conclusion

The goal of the present study was to understand better the role of individual attitudes, social pressure, and sense of control toward the importance of data security in a telework environment. This study helped to understand the role of motivations and intentions and to identify factors that contributed to a willingness of teleworkers to follow data security policies and practices that protect the security and integrity of information data used in telework environments.

5.1 Contributions to Knowledge

In the theory of planned behavior, Ajzen (2005) pointed out that for some intentions, attitudinal considerations are more important than normative considerations. The findings in the present study supported this theory. Personal attitudes related to intentions were found to be stronger than social pressure, especially in terms of attitudes about the vulnerability of data and the importance of keeping it secure in a telework environment. In addition, perceived behavior control was found to be important in willingness to follow security guidelines. Teleworkers held strong attitudes related to behaviors they had taken to protect data security and integrity, as well as the attitude that data security is their responsibility. In the present study, it appeared that personal attitudes and perceived behavior control played a greater role than did social pressure in terms of data protection and willingness to follow organizational information data security policies and practices.

Personal attitudes played an important role in how seriously teleworkers considered the need to secure the data they used. The findings of the present study provided evidence that teleworkers recognized the threat of security breaches and were willing to take steps to protect the security and integrity of data. Because teleworkers' motivation may be reflective of the seriousness with which an organization regards security measures, it is important that the organization clearly articulates this importance to its telework force.

Based on the findings from end-user studies, many workers remain confused about data security policies, due to either lack of policies or no orientation of IT security policies; therefore, these policies are largely ineffectual in maintaining data security and integrity (Booker & Kitchens, 2007). This also was found in the context of teleworking. In the present study, an indication of the basis for this confusion was that teleworkers indicated their organizations did not clearly communicate the importance of confidentiality and privacy of data or what specific measures workers should take to protect the integrity of the data. In addition, teleworkers often were not asked to sign a statement indicating they would comply with policies and procedures to protect and maintain the value of data in the telework environment. Herath and Rao (2009) found in their study of organizations that social pressure or subjective norms of expectation, or lack thereof, coupled with practices by policymakers and organizational leaders, may negatively influence attitudes and intentions of workers about taking personal responsibility for maintaining data security and integrity. In the present study, similar attitudes were found among teleworkers who stated they often received unclear communication regarding security guidelines and thus expectations for behavior.

Herath and Rao (2009) reported that a subjective norm; that is, seeing one's peers routinely comply with security measures, would lead to greater individual compliance among organizational workers. This was not found in the present study that examined subjective norm among teleworkers. Teleworkers were ambivalent about the extent to which they felt pressure by others to comply with security guidelines. The most important influences on subjective norm among teleworkers were from direct supervisors rather than from peers. This is a factor that needs to be considered for further study. It would be helpful to understand how the telework environment is different from the organizational environment in terms the type and quality of communication and how it relates specifically to the exertion of social pressure. That is, to what extent do teleworkers communicate with one another and how does this influence a sense of social pressure that influences behavior?

It may be that other factors exert greater influence on compliance behaviors. There may be similarities in the telework environment that are found within the organizational environment. Herath and Rao's (2009), in their study of organizational workers, concluded that both intrinsic and extrinsic motivators influence intentions to comply with security policies, especially when employees see compliance as helping the organization. Similar effects of intrinsic and extrinsic motivational influences also were found among teleworkers in the current study. For teleworkers in the present study, intrinsic motivators had a greater influence on intentions to comply with security measures. That is, the threat of punishment was not as important as taking personal responsibility to help secure an organization's data or for encouraging others to take steps to ensure data protection in the telework environment. This indicated that teleworkers believed their actions could make a difference in making data more secure. These findings are similar to what has been reported about organizational workers by Herath (2008). Herath noted that while training is important for setting a climate, actual policy compliance intentions by employees are driven primarily by personally held beliefs. This appears to be true both for office-based and remote location workers.

Spitzmuller and Stanton (2006), in support of the theory of planned behavior pertaining to behavioral control, stated that organizational workers were more likely to act on their attitudes if they felt they had the necessary control and knowledge to act according to these attitudes. This also was true among teleworkers in the present study. Teleworkers indicated a willingness to follow organizational security guidelines and indicated they had the knowledge and personal control to act on their beliefs in taking personal responsibility for maintaining data integrity and security. The strong intentions to follow organization information security policies in the telework environment additionally supported the idea that organizational norms, or shared beliefs about standards for acceptable and unacceptable behavior in the workplace, might be at play.

Flood (2001) proposed that among organizational workers, poor compliance is related to powerful security systems that negatively impact functionality of software and thus reduce productivity. However, in the present study, teleworkers did not believe that the current security systems negatively affected system functionality or restricted or interfered with the ability to complete their work. Current information security devices had not created noticeable problems for the majority of teleworkers. It may be that teleworkers have greater opportunities for circumventing security features that allow for less interference on program functionality; as Curran and Canning (2007) reported about workers using handheld devices who turned off security features in order to improve program functionality.

Finally, according to Chatzisarantis et al. (2006), behavior is best predicted from an individual's intentions or the effort he or she is willing to put toward the performance of any given behavior. The theory of planned behavior posits that intentions to perform a behavior are influenced by a combination of attitudes that behaviors will lead to certain consequences, subjective norms, and perceptions of control. In the present study, a weak association was found between social pressure and willingness to follow security guidelines. This finding may reflect that it is not only subjective norms, but the interaction of subjective norms, sense of control, and personal attitudes that exert the greatest influence on behavior. This may support the contention by Chatzisarantis et al. that subjective norms alone may not be sufficient for predicting and explaining human behavior because of the contribution of intrinsic motives in behavioral actions.

5.2 Implications for Future Research

Overall, teleworkers from this study did not indicate that they felt much social pressure to follow security guidelines and practices. The intent to following protocols might involve a complex interaction between internal attitude and environmental factors, as well as social pressure. While teleworkers did not feel much social pressure from co-workers, they did indicate the intent to follow the guidelines of managers and supervisors. Therefore, determining how social pressure influences behavior intent in manager-worker relationships among teleworkers would be helpful. Specifically, further research could be directed at identifying those factors in a telework environment that serve to increase social pressure to follow security protocols as suggested by the manager. For example, it may be that simply receiving attention from the manager may increase intent to follow security guidelines, or manager-worker interaction may increase awareness of security protocols or increase fear of reprimand and sanctions for not following security measures. Research should be directed at determining in what ways interaction with the manager increase pressure to follow security guidelines.

According to the theory of planned behavior, an individual's intention to perform a behavior increases when that behavior is evaluated positively, when there is an experience of social pressure to perform it, and when the individual believes he or she has the means and opportunities to perform the behavior. Based on the theory of planned behavior, the intentions toward a willingness to follow data security guidelines may be associated with a sense of self-efficacy or ability to help secure the organization's data in a telework environment.

Teleworkers indicated a strong belief that they could make a difference in keeping data secure. How social pressure (subjective norm) or interactions contributed to the internalized beliefs that one can effectively secure data information in a telework environment was unclear. This would be an important area for future research. A study that examines co-worker interactions in the telework environment is needed. Specifically, the extent to which teleworkers interact with one another and the content of this interaction needs to be investigated. A first step in understanding how teleworkers interact would be to examine the extent to which these workers identify with one another. Gaining greater understanding of the content and frequency of interactions might enable fostering of the interactions that help to create social pressure among teleworkers to follow security guidelines.

The findings of the present study supported, in part, the contention by Shankar et al. (2007) that social norms have a limited impact on user intention and behavior. A weak relationship was found between social pressure and willingness to follow security guidelines for working in a telework environment. It may be that the social pressure factors investigated in the present study were not those that were most important to teleworkers. Social pressure may not be as strong because teleworkers may not strongly identify with other teleworkers and thus might have a low level of group identification. Further study needs to be conducted to explore factors related to social pressure and subjective norms to determine the extent to which social pressure contributes to user intention.

The results of the present study that social pressure did not play a significant role in willingness to following organizational security guidelines may be due to what Armitage and Conner (2001) posited about social pressure. Armitage and Conner contended that social pressure is more often exerted indirectly and implicitly than directly and explicitly. Therefore, this process would not be reflected in teleworkers' responses to survey items related to direct feelings of pressure by co-workers to comply with organizational information security policies and practices. Further study on the role of subjective norms should take place within the context of indirect and implicit social pressure factors that affect intentions to comply with data security guidelines in a telework environment.

5.3 Implications for Practitioners

Even though strong relationships were not found between independent variables and willingness to follow security protocols, overall, teleworkers were willing to following security guidelines. Fear of termination or disciplinary actions for breaches of security did not appear to be motivating factors as much as seeing the need to protect the confidentiality and integrity of the data stored on individual work computers. This can have significant implications for organizational officers responsible for data security and integrity.

Therefore, a focus on increasing the motivation to keep data secure and follow organizational policy and practices would be to increase knowledge and understanding about the risks and impact of data security breaches.

In addition, the development of subjective norms or social pressure to comply with security guidelines may be increased by creating a telework environment that connects workers through project or team-based work to help workers develop an in-group identity. The ability to help workers feel more connected to the organizational culture may help increase positive social pressure to adopt and implement organizational data security policies and practices.

Finally, the use of company-controlled computers adds another layer of security in addition to teleworker compliance with security guidelines. By using company-distributed computers, the organization has the ability to determine what security software is used and to monitor necessary updates to maintain desired levels of security. The use of company-owned computers also provides control over non-work related programs being loaded onto the hard drive and interfering with data security programs. Even though teleworkers indicated a desire to follow security guidelines, they may inadvertently interfere with security measures when using work computers for personal use or personal computers for work. Therefore, company-provided work computers dedicated to work-related activities may provide a higher level of security than if teleworkers are able to use their computers for both work and personal activities.

5.4 Implications for Policy Makers

Those who draft policy related to telework data security should focus on establishing clear policies and practices that can be implemented cost effectively within an organization. Because telework takes place in multiple locations with differing levels of attention to security, policymakers must have in place a clear protocol on how to address information data security issues. Education is vital because teleworkers who understand the importance of data security and how to best protect the integrity of data are more likely to follow organizational guidelines and practices. In addition, managers and supervisors must be able to articulate guidelines to increase data security as well as escalate the consequences of security breaches. This would tap into the results of the present study, which found that teleworkers indicated a strong intent to follow their managers' advice on how to keep data secure in the telework environment.

Antonopoulos (2007) pointed out the risks to data security when information is stored and accessed on computer systems that are used both for personal and office business. Policymakers must establish protocols to dedicate a computer solely for business purposes and restrict its use to only those purposes. This may require the organization to provide teleworkers with computers and other devices that are used only for work. This would allow the organization to have greater control over security measures and to help teleworkers protect the integrity of the data stored by not exposing them to potential security risks through everyday personal use, where information is more easily compromised (e.g., browsing on the Internet, reducing security levels to gain access to applications not work related, etc.).

5.5 Conclusions

Teleworkers believed strongly that information stored on an organization's computers is vulnerable to security incidents. They also indicated a strong understanding of the importance of information security and practices and the need to adopt security technologies and practices to safeguard information in a telework environment. However, these beliefs were not strongly linked to a willingness to follow an organization’s information security guidelines. Other motivating factors appeared to be at work that were the result of latent factors or a combination of factors not identified in the current study.

The objective of this study was to evaluate the theory of planned behavior as a means of understanding teleworkers’ attitudes to comply with security requirements in a teleworking environment. The study explored whether the theory of planned behavior provides an explanation of teleworkers’ motivation to complying with information security practices and policies. An improved manner of understanding the human element in the maintenance of a secure teleworking environment would be a valuable step towards discovering actionable solutions to security problems in the telework environment.

In conclusion, the results of the present study indicated that there might be latent factors at work that clouded the results in terms of the influence of social pressure and subjective norms on willingness to follow organization information data security guidelines. However, results established that understanding of the risks to data security and knowledge about what teleworkers can do to protect the confidentiality and integrity of data is related to the intent to follow security protocols.

APPENDICES

Appendix A

Definition of Terms

Information Technology: Information technology, as defined by the Information Technology Association of America (ITAA) is "The study, design, development, implementation, support, or management of computer-based information systems, particularly software applications and computer hardware" (Hill, n.d., p. 1). In short, IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information securely.

Malware: A computer program that is covertly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or OS. Common types of malware threats include viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware. (NIST SP 800-114, 2007)

Mobile workers: Employees who, by the nature of their jobs, are generally off-site, and may even have their home base as their homes. Since the nature of their work requires this setup—usually, they are traveling much of the time—they are not considered to be teleworkers. This is different from *hoteling* arrangements, in which frequent teleworkers use shared space when they are onsite.

Non-Teleworkers: Employees who work at an official workplace during regularly scheduled work hours. Many employees take work home with them. This is remote work, but it is not considered to be telework within the scope of the legislation (Office of Personnel Management, 2006).

Official teleworkers: Employees who work outside of the official workplace, via a technological connection, during regularly scheduled work hours, either at home or at an alternative workplace, on a full-time, part-time, or situational basis.

Perceived behavioral control: An individual's perceived ease or difficulty of performing the particular behavior (Ajzen, 1988). It is assumed that perceived behavioral control is determined by the total set of accessible control beliefs.

Personal Computer (PC): A desktop or laptop computer running a standard PC OS (e.g., Windows Vista, Windows XP, Linux/UNIX, and Mac OS X). (NIST SP 800-114, 2007)

Peer Pressure: Pressure from one's peers to behave in a manner similar to or acceptable to them.

Phishing: Deceptive computer-based means to trick individuals into disclosing sensitive personal information. (NIST SP 800-114, 2007)

Remote Access: The ability of an organization’s users to access its non-public computing resources from locations other than the organization’s facilities. (NIST SP 800-114, 2007)

Teleworker: Employees who are allowed to conduct some or all of their work at an alternative worksite, away from the employer's typically used office. Telework is also referred to as telecommuting, flexiwork, and flexiplace. The telework concept can be applied to a variety of work environments (Office of Personnel Management, 2006).

Theory of Planned Behavior: A theory about the link between attitudes and behavior. (Ajzen, 1988)

Theory of Reasoned Action: The components are three general constructs: behavioral intention (BI), attitude (A), and subjective norm (SN). The theory suggests that a person's behavioral intention depends on the person's attitude about the behavior and subjective norms (BI = A + SN). (Ajzen & Fishbein, 1980)

Virtual Private Network (VPN): A tunnel that connects the teleworker’s computer to the organization’s network. (NIST SP 800-114, 2007)

Unofficial Teleworkers: Employees who work at an official workplace, yet also work at home on nights or on weekends. These individuals are not considered official teleworkers.

Appendix B

List of Symbols and Acronyms

3G	3rd Generation
CRM	Customer Relationship Management
GAO	U.S. Government Accountability Office
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
IS	Information System
IT	Information Technology
LAN	Local Area Network
MDM	Mobile Device Management
MPLS	Multiprotocol Label Switching
MST	Monitoring and Surveillance Technologies
NIST	National Institute of Standards and Technology
PC	Personal Computer
PBC	Perceived Behavioral Control
PDA	Personal Digital Assistant
PIN	Personal Identification Number
SGD	Secure Global Desktop
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
USB	Universal Serial Bus
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

Appendix C

Documentation of Research Site Approval

Sent: Thursday, March 04, 2010 10:14 AM
To: Tim Godlove
Cc: moneil@teleworkexchange.com; Dr. Gordon
Subject: Re: Telework Research Study Survey

Tim,

Thank you for your note. When you noted that your target audience was "Telework Exchange members" we assumed you were making observations based on the organizational affiliation. Your clarification is appreciated. We would be happy to post your survey so long as we have the opportunity to review any references to our organization in your final report.
Please let us know it that would work for you.

Thank you,
Erin

From: Tim Godlove [mailto:trgodlove@comcast.net]
Sent: Sunday, February 28, 2010 2:25 PM
To: cauten@teleworkexchange.com
Cc: moneil@teleworkexchange.com; 'Tim Godlove'
Subject: Telework Research Study Survey

Ms. Cindy Auten
Telework Exchange
921 King Street
Alexandria, VA 22314

Dear Ms. Auten,

I am Ph.D. candidate in Information Assurance at the University of Fairfax, Virginia. This is to request approval to utilize the Telework Exchange website in my research and allow a temporary link on your website to the research study survey. I am currently in the planning research phase of the Ph.D. program and once the University of Fairfax's Institutional Review Board Committee has approved my Research Design Specification, I will be ready to collect data.

My research project will study and investigate the relationship between the Theory of Planned Behavior and teleworkers' attitudes to compliance with security requirements in a teleworking environment. The study will explore whether the Theory of Planned Behavior provides a better explanation of teleworkers' attitudes than the effect of peer pressure alone. The focus of this study on teleworkers is unique in the sense that instead of merely determining the scope of work of teleworkers and their practices, it will focus on what motivates teleworkers to comply with security standards. This study can be used to address specific motivational issues and modify behavior of end users. The Telework Exchange population represents federal teleworkers, telework managers, IT professionals, and industry advisors, and meets the prerequisites for a research site and is the reason for my request.

The research instrument would utilize an electronic survey that would be accessed via a website. I will use an online survey site called SurveyMonkey to facilitate the implementation of the test instrument and collect the results. SurveyMonkey has been used successfully to conduct research and has the prerequisite security features and functionality I believe will make the online survey a success, including SSL encryption, secure controlled access via login and password, and physical and electronic protection for all servers.

I am proposing that the survey be a link on the Telework Exchange website with a request for members or non-members to click on the link to participate. The request for participation in the survey will be accompanied by a brief description of the purpose of the survey and an informed consent statement. All participation in the survey will be voluntary and survey participants will remain anonymous. The survey will be 29-questions long and will take approximately 10 minutes to complete.

I expect that I will be able to collect a minimum of 150 complete survey response data sets prior to removing the link from the Telework Exchange website and the SurveyMonkey link will be shutdown. In the unlikely event that there are fewer than 150 complete responses at the end of the survey availability period, I will need to request an approval from the Telework Exchange to host the survey link for a brief extension of about a week or so until I collect the planned 150 data sets. In case of a low response rate during the survey availability period, the researcher will attend the next Telework Exchange Town Hall meeting to discuss the study and advise attendees that there is a survey link on the Telework Exchange.

All data will be downloaded to a PC and stored in an encrypted file using Windows XP encrypting file system. The researcher will create an archive copy of the results on a CD-ROM that will be an encrypted file. This file will be placed in a safe deposit box for archiving purposes.

I will be delighted to present the purpose of the research and its findings, once it has been completed, during a Telework Exchange Townhall Meeting. A copy of the final report and its findings will also be presented to the Telework Exchange leadership.

I appreciate you taking the opportunity to allow me to present my proposal and will be happy to answer any questions you may have.

Thank you for your time and consideration.

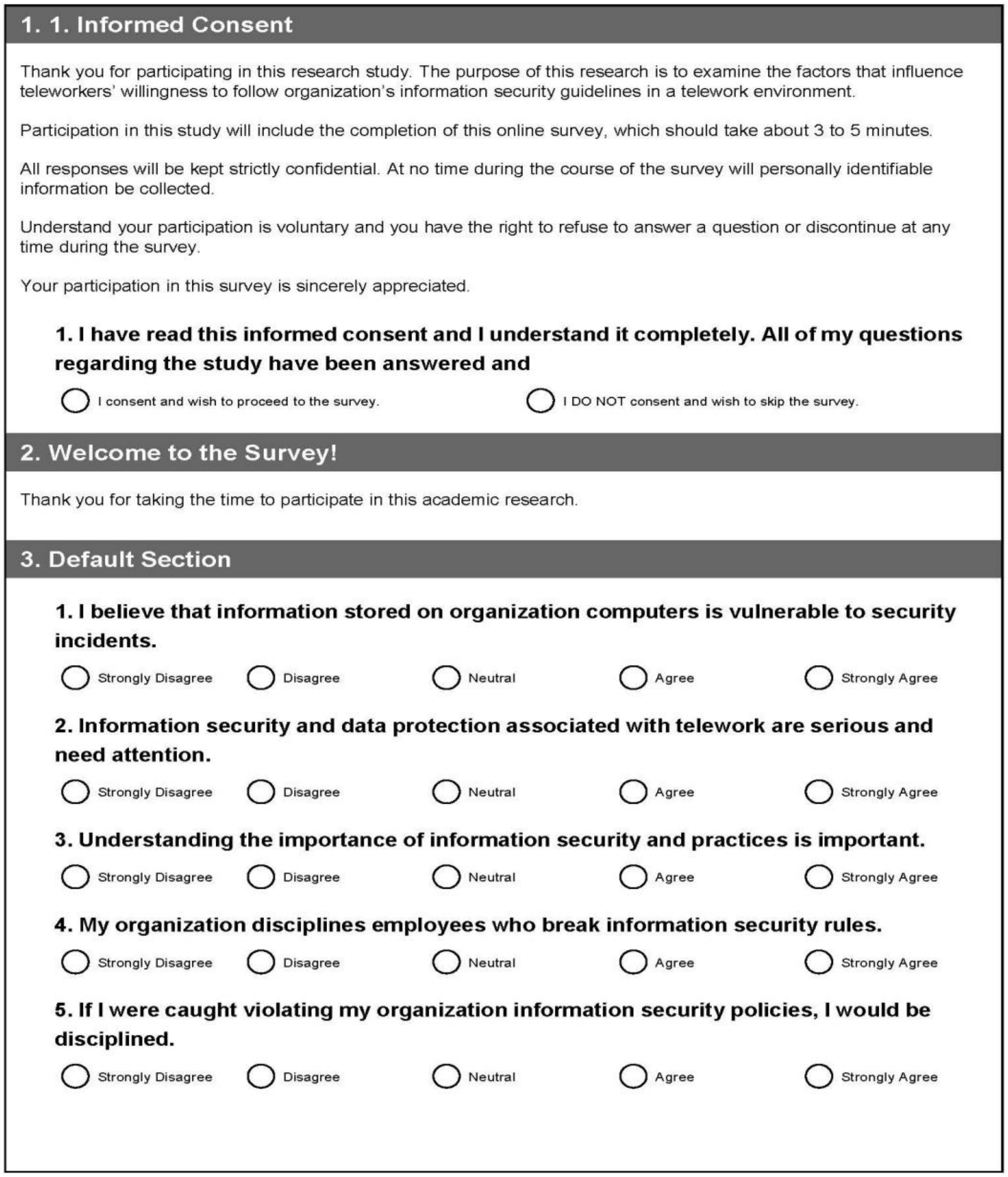
Sincerely,

Tim Godlove

Appendix D

Teleworkers' Security Survey Instrument Utilized

The information within this appendix identifies the survey questions that were asked online. The survey instrument is a web-enabled survey hosted by SurveyMonkey.com and the below does not necessarily indicate how it was presented to the respondent on screen.



1. 1. Informed Consent

Thank you for participating in this research study. The purpose of this research is to examine the factors that influence teleworkers' willingness to follow organization's information security guidelines in a telework environment.

Participation in this study will include the completion of this online survey, which should take about 3 to 5 minutes.

All responses will be kept strictly confidential. At no time during the course of the survey will personally identifiable information be collected.

Understand your participation is voluntary and you have the right to refuse to answer a question or discontinue at any time during the survey.

Your participation in this survey is sincerely appreciated.

1. I have read this informed consent and I understand it completely. All of my questions regarding the study have been answered and

○ I consent and wish to proceed to the survey. ○ I DO NOT consent and wish to skip the survey.

2. Welcome to the Survey!

Thank you for taking the time to participate in this academic research.

3. Default Section

1. I believe that information stored on organization computers is vulnerable to security incidents.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

2. Information security and data protection associated with telework are serious and need attention.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

3. Understanding the importance of information security and practices is important.

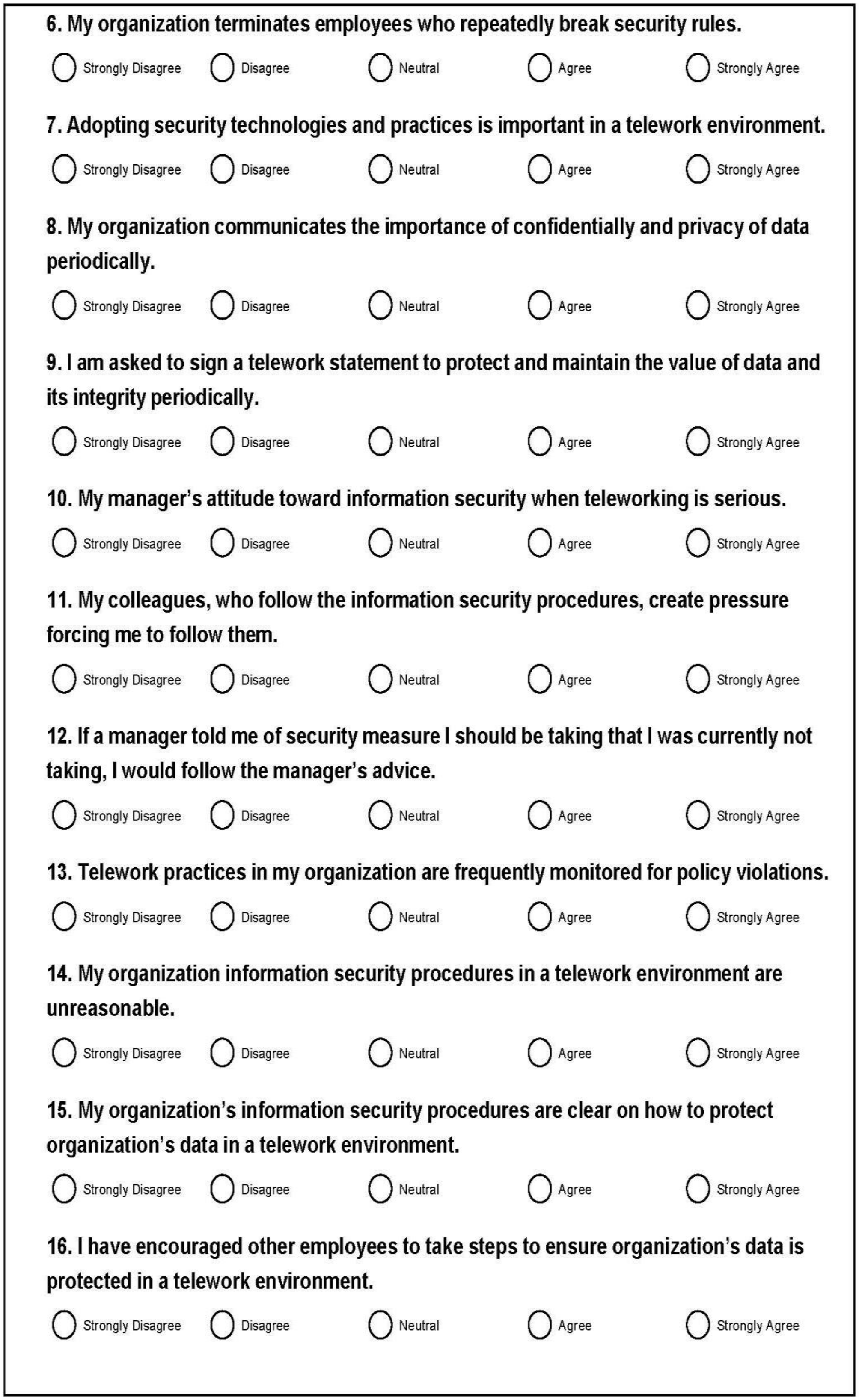
○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

4. My organization disciplines employees who break information security rules.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

5. If I were caught violating my organization information security policies, I would be disciplined.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree



6. My organization terminates employees who repeatedly break security rules.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

7. Adopting security technologies and practices is important in a telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

8. My organization communicates the importance of confidentially and privacy of data periodically.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

9. I am asked to sign a telework statement to protect and maintain the value of data and its integrity periodically.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

10. My manager's attitude toward information security when teleworking is serious.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

11. My colleagues, who follow the information security procedures, create pressure forcing me to follow them.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

12. If a manager told me of security measure I should be taking that I was currently not taking, I would follow the manager's advice.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

13. Telework practices in my organization are frequently monitored for policy violations.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

14. My organization information security procedures in a telework environment are unreasonable.

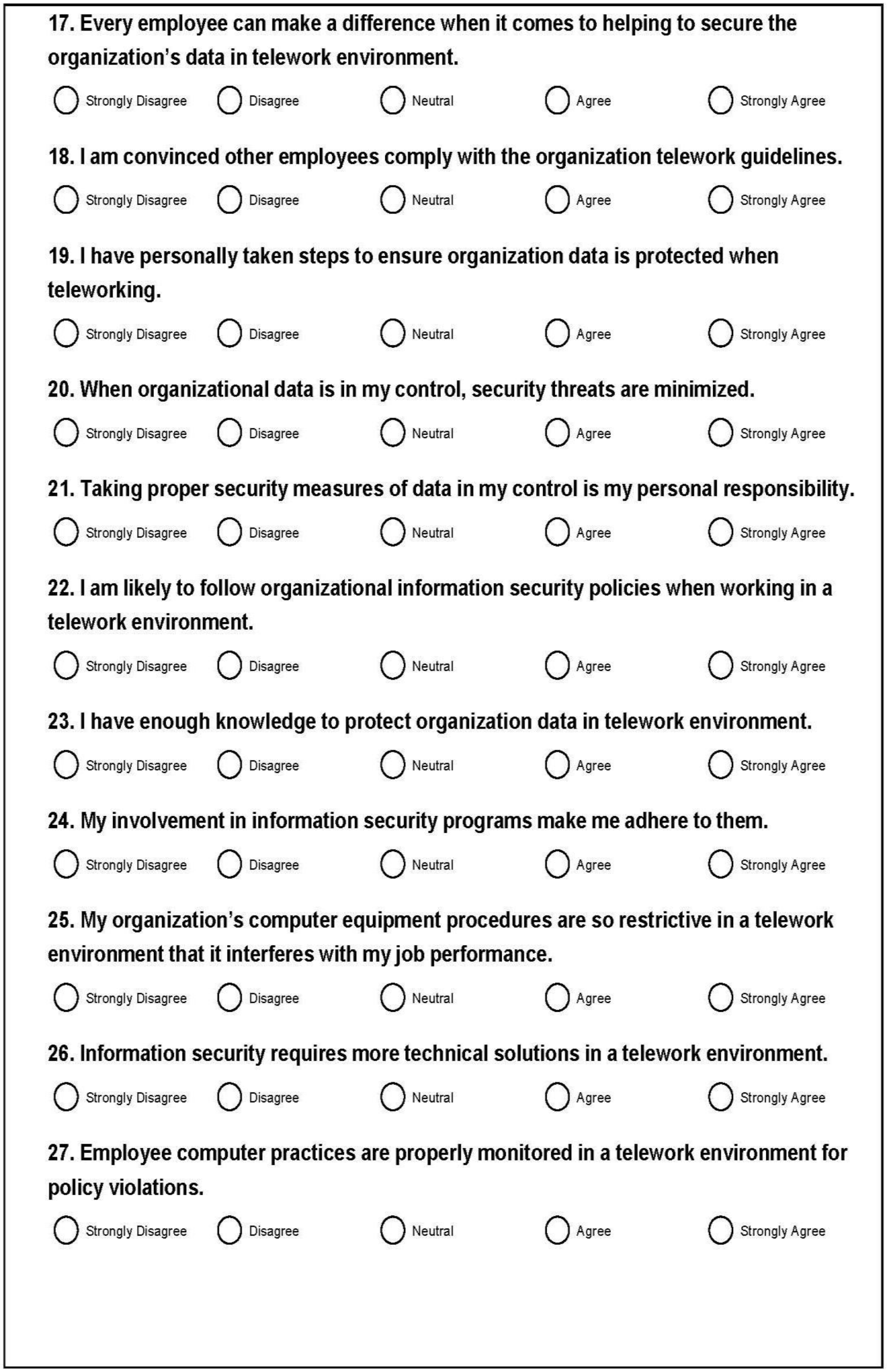
○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

15. My organization's information security procedures are clear on how to protect organization's data in a telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

16. I have encouraged other employees to take steps to ensure organization's data is protected in a telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree



17. Every employee can make a difference when it comes to helping to secure the organization's data in telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

18. I am convinced other employees comply with the organization telework guidelines.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

19. I have personally taken steps to ensure organization data is protected when teleworking.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

20. When organizational data is in my control, security threats are minimized.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

21. Taking proper security measures of data in my control is my personal responsibility.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

22. I am likely to follow organizational information security policies when working in a telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

23. I have enough knowledge to protect organization data in telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

24. My involvement in information security programs make me adhere to them.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

25. My organization's computer equipment procedures are so restrictive in a telework environment that it interferes with my job performance.

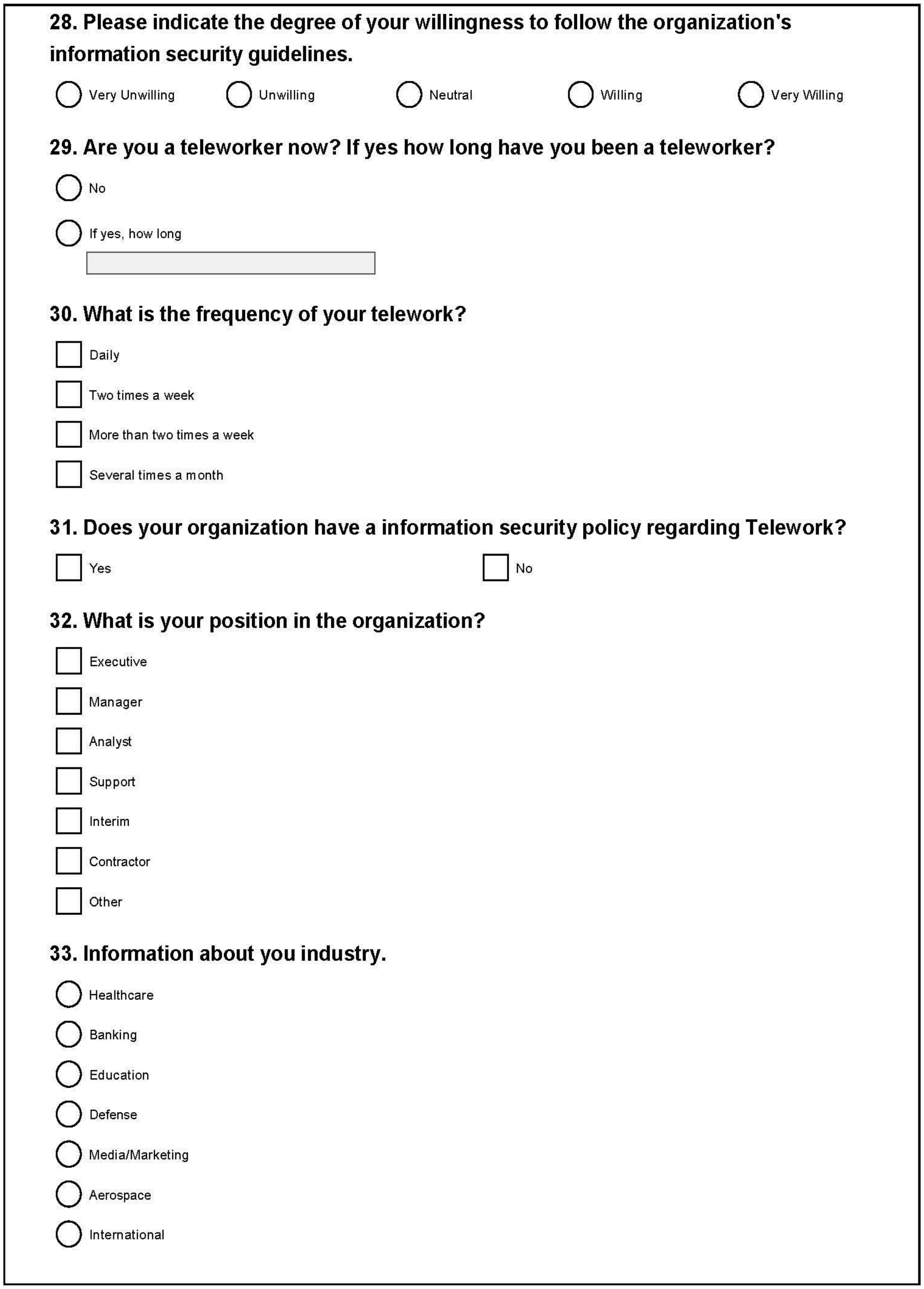
○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

26. Information security requires more technical solutions in a telework environment.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

27. Employee computer practices are properly monitored in a telework environment for policy violations.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree



28. Please indicate the degree of your willingness to follow the organization's information security guidelines.

○ Very Unwilling ○ Unwilling ○ Neutral ○ Willing ○ Very Willing

29. Are you a teleworker now? If yes how long have you been a teleworker?

○ No

○ If yes, how long

30. What is the frequency of your telework?

□ Daily

□ Two times a week

□ More than two times a week

□ Several times a month

31. Does your organization have a information security policy regarding Telework?

□ Yes □ No

32. What is your position in the organization?

□ Executive

□ Manager

□ Analyst

□ Support

□ Interim

□ Contractor

□ Other

33. Information about you industry.

○ Healthcare

○ Banking

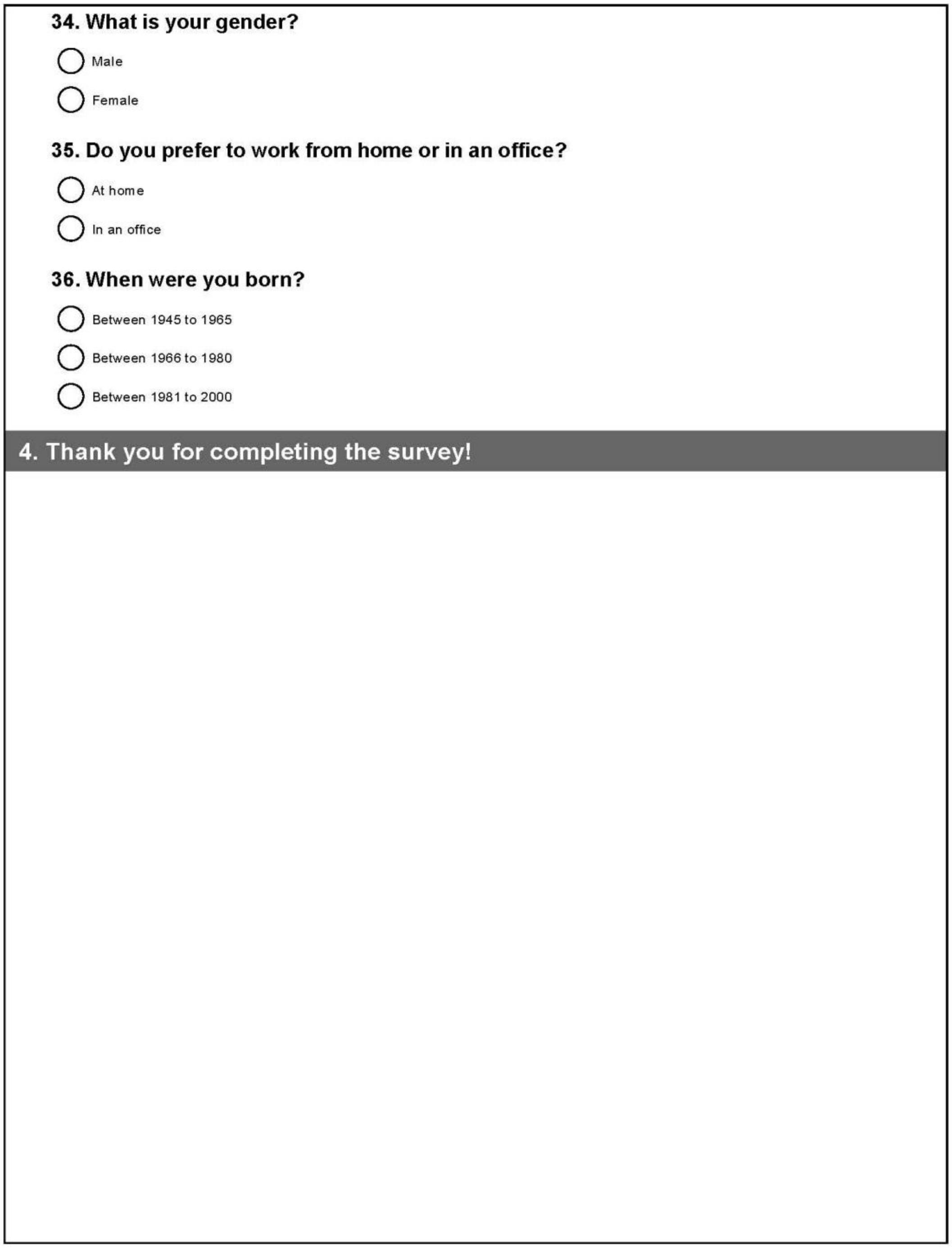
○ Education

○ Defense

○ Media/Marketing

○ Aerospace

○ International



34. What is your gender?

○ Male

○ Female

35. Do you prefer to work from home or in an office?

○ At home

○ In an office

36. When were you born?

○ Between 1945 to 1965

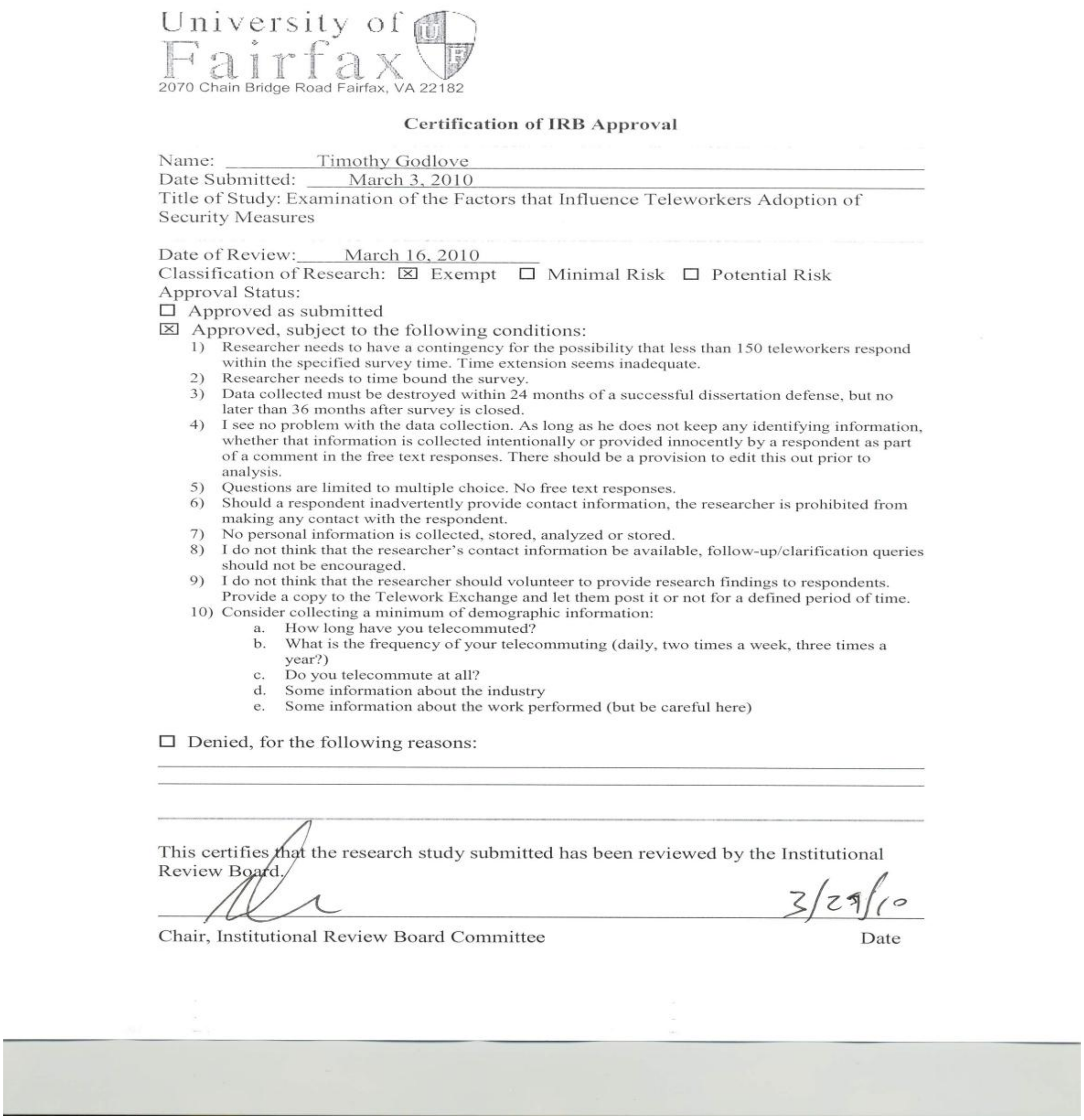
○ Between 1966 to 1980

○ Between 1981 to 2000

4. Thank you for completing the survey!

Appendix E

Certification of IRB Approval



University of Fairfax
2070 Chain Bridge Road Fairfax, VA 22182

Certification of IRB Approval

Name: Timothy Godlove

Date Submitted: March 3, 2010

Title of Study: Examination of the Factors that Influence Teleworkers Adoption of Security Measures

Date of Review: March 16, 2010

Classification of Research: ☒ Exempt ☐ Minimal Risk ☐ Potential Risk

Approval Status:

☐ Approved as submitted

☒ Approved, subject to the following conditions:

1) Researcher needs to have a contingency for the possibility that less than 150 teleworkers respond within the specified survey time. Time extension seems inadequate.
2) Researcher needs to time bound the survey.
3) Data collected must be destroyed within 24 months of a successful dissertation defense, but no later than 36 months after survey is closed.
4) I see no problem with the data collection. As long as he does not keep any identifying information, whether that information is collected intentionally or provided innocently by a respondent as part of a comment in the free text responses. There should be a provision to edit this out prior to analysis.
5) Questions are limited to multiple choice. No free text responses.
6) Should a respondent inadvertently provide contact information, the researcher is prohibited from making any contact with the respondent.
7) No personal information is collected, stored, analyzed or stored.
8) I do not think that the researcher's contact information be available, follow-up/clarification queries should not be encouraged.
9) I do not think that the researcher should volunteer to provide research findings to respondents. Provide a copy to the Telework Exchange and let them post it or not for a defined period of time.
10) Consider collecting a minimum of demographic information:
    a. How long have you telecommuted?
    b. What is the frequency of your telecommuting (daily, two times a week, three times a year?)
    c. Do you telecommute at all?
    d. Some information about the industry
    e. Some information about the work performed (but be careful here)

☐ Denied, for the following reasons:

This certifies that the research study submitted has been reviewed by the Institutional Review Board.

3/29/10

Chair, Institutional Review Board Committee   Date

Reference List

Ajzen, I. (1988). *Attitudes, personality, & behavior*. Chicago, IL: Dorsey Press.

Ajzen, I. (2005) *Attitudes, personality, and behavior*, Maidenhead, England: Open University Press.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Allenby, B., & Roitz, J. (Eds.). (2003). *Implementing the knowledge economy: The theory and practice of telework*. Charlottesville, VA: Darden Graduate School of Business.

Antonopoulos, A. M. (2007, October 10) Combining work and play threatens business security. *Network World*. Retrieved from http://www.networkworld.com/ columnists/2007/101007-risk-reward.html?fsrc=rss-antonopoulos

Armitage, C. J., & Christian, J. (2003). From attitudes to behavior: Basic and applied research on the theory of planned behavior. *Current Psychology, 22*, 187–195. doi: 10.1007/s12144-003-1015-5

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology, 40,* 471-499. doi:10.1348/014466601164939

Auten, C. (2008, March 7). Ready, set, go: How to put telework in the fast lane. *EWeek*, 1-4. Retrieved from http://www.eweek.com/c/a/Enterprise-Applications/Ready-Set-Go-How-to-Put-Telework-in-the-Fast-Lane/

Baginsky, M. (2004). Peer support: Expectations and realities. *Pastoral Care in Education,* 3-11. doi:10.1111/j.0264-3944.2004.00280.x

Bain, B. (2007, September 13). Justice says no to private PCs for telework. *FCW.com*. Retrieved from http://www.fcw.com/online/news/150044-1.html

Bailey, K. D. (1987). *Methods of social research* (3rd ed.). New York, NY: The Free Press.

Bandura, A. (1977). *A social learning theory*. Englewood, NJ: Prentice-Hall.

Booker, Q., & Kitchens, F. L. (2007). Predicting employee intention to comply with organizational security policies and procedures factoring risk perception. In Dhanda, K.K., & Hackney, R. (Eds.), *Proceedings of the Annual ISOneWorld Conference. "Engaging Academia and Enterprise Agenda".* DC: Information Institute Publishing.

Booker, Q., & Kitchens, F. L. (2010). Predicting employee intention to comply with organizational security policies and procedures factoring risk perception: A comparison of 2006 and 2010. *Issues in Information Systems, 11*(1), 649-658. Retrieved from http://www.iacis.org/iis/2010_iis/Table%20of%20Contents %20No1_files/649-658_LV2010_1522.pdf

Booker, Q., Rebman, C., & Kitchens, F. L. (2009). *Integrating business intelligence training into a "Principles of Management" class.* Paper presented at the 2009 Decision Science Institute Annual Meeting, New Orleans, LA.

Boss, S. R., & Kirsch, L. J. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. *Proceedings of the International Conference on Information Systems* (pp. 1-18). Montreal, Canada.

Brandel, M. (2007, February 26). Home office lockdown. *Computerworld,* 27-30.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *Management Information Systems Quarterly (34:3),* pp. 523-548

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

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2008). Information security control resources in organizations: A multidimensional view and their key drivers. (Working Paper 09-MIS-001) MIS Division, Faculty of Commerce and Business Administration at the University of British Columbia.*University of British Columbia Working Paper*.

Chatzisarantis, N. L. D., Hager, M. S., Smith, B., & Sage, L. D. (2006).The influences of intrinsic motivation on execution of social behavior within theory of planned behavior. *European Journal of Social Psychology, 36,* 229-237. doi:10.1002/ejsp.299

Chow, S. T., Gustave, C., & Vinokurov, D. (2009). Authenticating displayed names in telephony. *Bell Labs Technical Journal, 14,* 267-282. doi:10.1002/bltj.20367

Chu, F. (2005, April 16). Tarantella reins in remote chores. *Eweek,* 45-47.

Clark, M. W. (2006, May). Cell phone technology and physical surveillance. *FBI Law Enforcement Bulletin,* 25-34.

Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security, 6,* 1-14. doi: 10.1007/s10207-006-0006-6

Cohen, A. (2001, Summer). Worker watchers. *Fortune/Cnet Technology Review,* 70-80.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334. doi:10.1007/BF02310555

Curran, K., & Canning, P. (2007). Wireless handheld devices become trusted network devices. *Information Systems Security, 16,* 134-146. doi:10.1080/10658980701401686

Denscombe, M. (2001). Peer group pressure, young people, and smoking: New developments and policy implications. *Drugs: Education, Prevention, and Policy, 8,* 7-32. doi:10.1080/09687630124121

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8,* 386-408.

Edwards, C. (2005, June 20). Wherever you go, you're on the job. *BusinessWeek,* 1-5.

Farmer, L.A. (2005). Situational leadership: A model for leading telecommuters. *Journal of Nursing Management, 13,* 483-489. doi:10.1111/j.1365-2934.2005.00573.x

Fink, A., & Kosecoff, J. (1998). *How to conduct surveys: A step-by-step guide* (2nd ed.). Thousand Oaks, CA: Sage.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fitchard, K. (2004, March 22). The invisible intruders. *Telephony,* 46-50. Available at http://www.telephonyonline.com

Flood, K. (2001, February 5). The forgotten side of network security. *Network World, 12,* 276-283.

Freeman, E. H. (2005, July). Privacy and dot.com bankruptcies: Protection of personal data. *Legally Speaking: Information Security Journal: A Global Perspective, 14,*9-13. doi:10.1201/1086.1065898X/45390.14.3.20050701/89146.3

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management, 7,* 159-180.

Gall, M. D., Borg, W. R., & Gall, J. P. (1996). *Educational research: An introduction* (6th ed.). White Plains, NY: Longman.

Garcia, A. (2008, September 15). Managing a mobile platform. *EWeek,* 28-32.

Gross, G. (2008, July 30). Study: Companies need to address telework security. *Computer World*. Retrieved from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=personal_technology&articleId=9111082&taxonomyId=165&intsrc=kc_top

Hartig, T., Kylin, C., & Johansson, G. (2007). The telework tradeoff: Stress mitigation vs. constrained restoration. *Applied Psychology: An International Review, 56,* 231-253. doi:10.1111/j.1464-0597.2006.00252.x

Hayes, F. (2008, August 4). Cryptic reading. *Computerworld,* 36.

Herath, T. (2008). *Essays on information security practices in organizations*. Buffalo, NY: State University of New York.

Herath, T., & Rao, R. (2009) Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems, 47,* 154-165. doi:10.1016/j.dss.2009.02.005

Hersey, P., Blanchard, K. H., & Johnson, D. E. (2008*). Management of organizational behavior: Leading human resource*s (9th ed.). Upper Saddle River, NJ: Prentice Hall.

Hines, M. (2007, August 21). Mobile workers still struggling with security: A new study shows that even as the business use of mobile devices increases, many users are unconcerned or uninformed about security issues and practices. *InfoWorld*. Retrieved from http://www.infoworld.com/article/07/08/21/Mobile-workers-still-struggling-with-security_1.html

Hrubes, D., Ajzen, I., & Daigle, J. (2001). Predicting hunting intentions and behavior: An application of the theory of planned behavior. *Leisure Sciences, 232,* 165-178. doi:10.1080/014904001316896855

Hyrkas, K., Koivula, M., Lehti, K., & Paunonen-Ilmonen, M. (2003). Nurse managers' conceptions of quality management as promoted by peer supervision. *Journal of Nursing Management, 11,* 48-58. doi:10.1046/j.1365-2834.2003.00345.x

Jackson, B. (2008, September). SONY site falls prey to automated hacker hijack. *PCWorld, 1*, 56.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing, 18*(3), 1-24. doi: 10.4018/joeuc.2006070101

Johnston, K. L., & White, K. M. (2003). Binge-drinking: A test of the role of group norms in the theory of planned behavior. *Psychology and Health, 18,* 63-77. doi:10.1080/08870440210000037835

Jones, K. C. (2007, November 5). Businesses more concerned about mobile, remote security, but still ignore training. *InformationWeek.* Retrieved from http://www. informationweek.com/news/showArticle.jhtml?articleID=202802456

Kambourakis, G., Maglogiannis, I., & Rouskas, A. (2005). PKI-based secure mobile access to electronic health services and data. *Technology and Health Care, 13,* 511-526.

Kaven, O. (2004, August 3). Keep your office safe. *PC Magazine,* 93-101. Retrieved from http://www.pcmag.com

Kilpatrick, I. (2007, November). Dam data leakage at source: How unified encryption management (UEM) is changing the threat landscape. *Software World, 12*(4).

Kline, P. (2000). *A psychometrics primer*. London, England: Free Association Books.

Knorr, E. (2004, May 10). Is true mobility at hand? *Infoworld,* 33-34.

Lampson, B. (2005). *Microsoft, accountability, and freedom.* Retrieved from http:// research. microsoft.com/lampson/slides/accountabilityAndFreedomAbstract.htm

Liu, J., & Issarny, V. (2007). An incentive compatible reputation mechanism for ubiquitous computing environments. *International Journal of Information Security, 6,* 297-311. doi:10.1007/s10207-007-0029-7

Maier, R., & Sametinger, J. (2004). Peer-to-peer information workspaces. *International Journal of Software Engineering, 14,* 79-102.

Mears, J. (2007, April 3). Legislation promotes federal teleworkers; Telework Enhancement Act of 2007 would open more doors to telecommuting. *Network World.* Retrieved from http://www.nwwsubscribe.com/news/2007/040307-telework-legislation.html

Mobility management causing concern. (2007, December 6). *Communication News.* Retrieved from http://www.commnews.com

Nardi, P. M. (2003). *Doing survey research*. Boston, MA: Pearson Education.

National Institute of Standards and Technology. (2007). *User's guide to securing external devices for telework and remote access.* SP-800-114. Retrieved from http://csrc.nist.gov/publications/nistpubs/

Ng, B. Y., & Rahim, M. A. (2005, July). *A socio-behavioral study of home computer users' intention to practice security*. Paper presented at the Ninth Pacific Asia Conference on Information Systems (pp. 234-247). Bangkok, Thailand.

Nunnally, J. C. (1964). *Educational measurement and evaluation*. New York, NY: McGraw-Hill.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior toward IS security policy compliance. *Proceedings of the 40th Annual Hawaii International Conference on Systems Sciences* (pp. 156-166). New York, NY: IEEE. doi:10.1109/HICSS.2007.206

Price, S. M. (2008). Host-based security challenges and controls: A survey of contemporary research. *Information Security Journal: A Global Perspective, 17,* 170-178. doi:10.1080/19393550802369800

Ransbotham, S., & Mitra, S. (2008) Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121-139. doi: 10.1287/isre.1080.0174

Regan, P. (2003). Privacy and commercial use of personal data: Policy developments in the United States. *Journal of Contingencies and Crisis Management, 11,* 12-20. doi:10.1111/1468-5973.1101003

Riemenschneider, C. K., Hardgrave, B. C., & Davis, F. D. (2002). Explaining software developer acceptance of methodologies: A comparison of five theoretical models. *IEEE Transactions on Software Engineering, 28,* 1135-1145. doi:10.1109/TSE.2002.1158287

Shankar, A., Conner, M., & Bodansky, H. J. (2007). Can the theory of planned behavior predict maintenance of a frequently repeated behavior? *Psychology, Health, & Medicine, 12,* 213-224. doi:10.1080/09540120500521327

Simpson, P. (2004, August). Secure your mobile road warriors. *Communications News*, 32-34.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, *8*(1), 31-41.

Siponen, M. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, *14,* 303-315. doi:10.1057/palgrave.ejis.3000537

Spitzmuller, C., & Stanton, J. M. (2006). Examining employee compliance with organizational surveillance and monitoring. *Journal of Occupational and Organizational Psychology*, *79,* 245-272. doi: 10.1348/096317905X52607

Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. *Human Performance, 13*, 85-113. doi:10.1207/S15327043HUP1301_4

Stanton, J. M. (2002). Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, & A. Wenn (Eds.), *Socio-technical and human cognition elements of information systems* (pp. 79–103). London, England: Idea Group.

Stanton, J. M., Caldera, C., Guzman, I. R., Isaac, A., Lin, P., Mathur, M., ... Zakaria, N. (2003, April). *Behavioral information security: An overview, research agenda, and preliminary results.* The Security Conference, Las Vegas, NV.

Stanton, J. M., & Weiss, E. M. (2000). Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. *Computers in Human Behavior, 16*, 423–440. doi:10.1016/S0747-5632(00) 00018-2

Stanton, J. M., & Weiss, E. M. (2003). Organisational databases of personnel information: Contrasting the concerns of human resource managers and employees. *Behaviour and Information Technology, 22*(5), 291–304. doi:10.1080/01449290310001599733

Sternstein, A. (2007, June 4). Survey: Unauthorized teleworkers a security risk. *National Journal's Technology Daily*. Retrieved from http://www.govexec.com/dailyfed/0607/060407tdpm1.htm

Straub, D. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169. doi:10.2307/248922

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(Article 24), 380-427.

Thibodeau, P. (2007, February 19). Web use spike in pandemic may make telework tough. *Computerworld,* 6-7.

Thurman, M. (2006, November 13). Tackling security for mobile CRM. *Computerworld,* 34-35.

Turner, G., & Shepherd, J. (1999). A method in search of a theory: peer education and health promotion. *Health Education Research*, *14*, 235-247. doi:10.1093/her/14.2.235

Vijayan, J. (2009). State uncertainty: Security rules slow to take hold in Mass. *Computerworld, 23,* 12-14.

Wagner, C. G. (2004, March). Fear and loathing in the virtual workforce. *The Futurist,* 6-7.

Warner, J. A. (2009). *The impact of IT security psychological climate on salient user beliefs toward IT security: An empirical study.* (Doctoral dissertation), Barry Kaye College of Business, Florida Atlantic University. Boca Raton, Fl. Retrieved from Publication of Archival Library and Museum Material, State University Libraries of Florida

Wellman, B., Salaff, J., Dimitrova, D., Garton, L., Gulia, M., & Haythornthwaite, C. (1996). Computer networks as social networks: Collaborative work, telework, and virtual community. *Annual Review of Sociology*, *22*, 213-238. doi:10.1146/annurev.soc.22.1.213

Willison, R. (2006) Understanding the perpetration of employee computer crime in the organizational context. *Information and Organization*, *16*, 304-324. doi:10.1016/j.infoandorg.2006.08.001

Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.) New York: Harper and Row.

Yun, J., & Ulrich, D. A. (2002). Estimating measurement validity: A tutorial. *Adapted Physical Activity Quarterly, 19*(1), 32-47.

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behavior, 23,* 605–633. doi:10.1002/job.157

Zweig, D., & Webster, J. (2003). Personality as a moderator of monitoring acceptance. *Computers in Human Behavior, 19,* 479–493. doi:10.1016/S0747-5632(02) 00075-4

Biography

Tim Godlove is currently a Department of Veterans Affairs (VA) Senior Program Analyst at DoD/VA Interagency Program Office where he supports the information technology integration efforts for the DoD/VA Virtual Lifetime Electronic Record (VLER). In this position, he assists DoD, VA, and private sector healthcare providers to achieve successful implementation of the VLER and other initiatives that are critical for the interagency progress towards enhanced care, benefits, and services for the nation's service members, Veterans, and their families.

Prior leadership assignments included VA Team Lead, Oversight and Compliance, leading independent and objective risk assessment for cyber security, privacy, research, records management, and information physical security controls for compliance at VA facilities throughout the United States. Additional assignments were Deputy Information Assurance (IA), Missile Defense Agency (MDA), where he served as principal advisor to the MDA Chief Information Officer on IA/Computer Network Defense, directing daily management to reduce risks and vulnerabilities to protect and improve the security posture of more than 200 information systems of the MDA enterprise, including weapons systems and administrative networks; Information Assurance Manager, Office of Assistant Secretary of Defense (Health Affairs), where he led Certification & Accreditation teams to certify more than 12 different major health providers for the Medical Health System; and Information Technology Officer, Defense Intelligence Agency (DIA), where he led the integration of the Joint Staff Information Network (JSIN) Top Secret/Unclassified and Global Communication Control Systems (GCCS) information systems into the DIA operational environment in support of military and intelligence operations.

Serving on active duty with the U.S. Navy, Mr. Godlove held a variety of positions in operational commands and staff assignments in the continental United States and Europe. Prior to retiring, he served as Senior Navy Aide/Protocol Officer for the Chairman of the Joint Chiefs of Staff. Other assignments included Officer in Charge, Base Support Battalion Operation Joint Forge; Executive Officer, Reserve Component Affairs Directorate, Headquarters, U.S. European Command; and Operations Chief, Military Liaison Team, Bulgaria.

Having been in the Pentagon on September 11, 2001, Tim realized the events of that day created a new appreciation and need for security measures in the United States. His quest to assist the nation from preventing such an event in cyberspace has led him to pursue a Doctor of Philosophy with the University of Fairfax. Tim holds a Master of Science Administration in Information Resources Management from Central Michigan University, a Bachelor of Arts from Chapman University, and he has completed the Chief Information Officer Program and Information Assurance certification (NSTISSI No. 4011) at the National Defense University. He is a 2008 graduate of Leadership VA Program.

Tim serves on the Federal CIO Council IT Workforce Committee as the Vice-Chair, Managing Talent. He has published articles on information security and privacy concerns on electronic healthcare records in information security journals.