Information Security Journal: A Global Perspective, 21:216–229, 2012
ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2012.668747

Taylor & Francis
Taylor & Francis Group

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

Timothy Godlove
Department of Defense/Department of Veterans Affairs, Washington, DC

ABSTRACT With the increased use of teleworkers, it is important to understand how teleworker attitudes are related to the 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 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, and sense of responsibility 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 attitudes of teleworkers regarding data security, sense of control teleworkers have regarding the confidentiality and integrity of data, and the intent of teleworkers to follow security protocols in a telework environment.

KEYWORDS telework, theory of planned behavior

1. INTRODUCTION

With increasing use of telecommuting among organizations, protecting data and information used by teleworkers from nonoffice-based locations is a situation faced by many businesses. High-capacity broadband networks and other communication technologies have provided many advantages and benefits to 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 (Horner, 2011). However, the use of teleworkers also creates challenges for

Address correspondence to Timothy Godlove, 1530 Key Blvd, Arlington VA 22209. E-mail: trgodlove@comcast.net

businesses and managers who work to maintain security of the information and data to which teleworkers have access (Jones, 2007).

Given the increasing use of telework, gaining a better understanding of factors related to maintaining information security 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. A challenge to data security faced by organizations relates to the lack of awareness by teleworkers of security risks and how to maintain data securely in a telework environment (Scarfone, Hoffman, & Souppaya, 2009).

The objective of this study was to examine teleworkers' attitudes regarding compliance with security requirements in a teleworking environment using Ajzen's Theory of Planned Behavior. The study was conducted to explore 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.

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

- *Nonteleworker*. 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.

With the increasing use of teleworkers, the problem of teleworker compliance with information security guidelines takes on greater importance. The business problem addressed in this study is understanding that extent that personal attitudes, social pressure, and a sense of control play in the willingness of teleworkers to comply with their organizations information security guidelines and policies. Understanding the roles that personal attitudes, social pressure, and sense of control play in information security compliance will help managers more effectively create an environment that increases willingness to follow organizational information security policies and procedures both within the office and among teleworkers in a nonoffice-based setting. The findings of this study will add to the body of knowledge about how to improve data security in a telework environment.

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). Telework involves providing workers with a flexible arrangement under which work duties are performed at an approved location from other than the organization's office location from which the employee normally would work (Guide to Telework, 2011). The typical teleworker is a regular employee who works from home no more than two days a week, lives in the same metro area where the organization is located, works for reason of convenience, and often retains a normal desk in the office building or other work area of the organization, works for a small or a large business, has a college degree, and is more than 30 years old (Horner, 2011). Other teleworkers are virtual office workers who work from a remote location with a portable office provided by the organization (Horner). These workers may report to a branch office or maintain contact with the organization through various communication channels other than face-to-face interaction (Tallberg, 2011). Finally, some teleworkers are short-term or long-term contract works who are employed by an organization for a specific task or project and then leave the organization once this defined work or period of work has been completed (Tallberg).

This ever-growing use of teleworking increases convenience and efficiency; however, telework arrangements can have significant implications for organizational data security and the costs associated with security breaches. The greater reliance on telework provides opportunities for breaches of data security through unauthorized viewing of data, data theft, and data leakage (Kilpatrick, 2007). These security concerns also are applicable to nonteleworkers who work in an office setting. However, there are fewer opportunities for information security personnel and supervisors to

interact with teleworkers and monitor compliance with information security policies than there are in an office setting (Kilpatrick). Data breaches can result in significant costs to the business related to: (a) notifying customers/clients that data security has been compromised, (b) assistant victims affected by the data breach, (c) loss of reputation and/or current and future customers, (d) potential litigation, and (e) cost to hire experts to handle the data breach incident and/or develop and implement a data security plan (Ponemon, 2007). Presented in this paper are the results of doctoral research on factors that influence teleworkers willingness to comply with information security guidelines using an original survey study of teleworkers working in a telework environment.

2. METHODOLOGY

The research methodology was derived from literature and an original Teleworkers' Security Survey (Godlove, 2011) instrument focused on the end-user's behavior: providing a timely portrait of the attitudes and experiences of the teleworkers' workforce in regard to security.

2.1. Theoretical Framework

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 that "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). 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. While some security measures are built into information technology (IT) systems for business, some factors related to information and data security are dependent on the willingness of teleworkers to following security policies and procedures. 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. 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 company-controlled spaces and an increased 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 IT 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 study, potential solutions to these problems were identified and organized in a functional manner. The conceptual model in Figure 1 provides the framework for analysis used in the study.

2.2. Context

The study population from which the sample was derived consisted of the approximately 10,000 members of The Telework Exchange, an online public-private membership organization with the focus of providing information and resources related to teleworkers. The desired sample size of 384 participants was calculated based on a formula recommended by Yamane (1967) where sample size $n = N/1 + N(e)^2$ (N = population size and e = level of precision

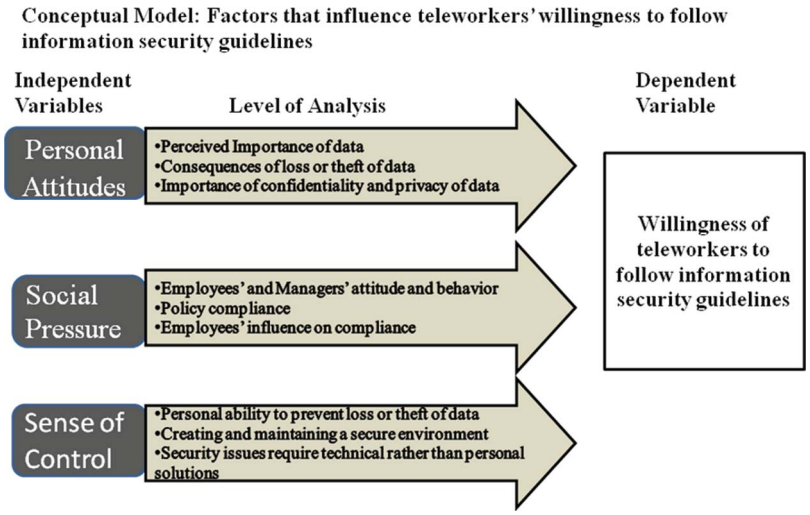

FIGURE 1 Conceptual model for the framework of the study. (color figure available online.)

of .05). From those invited to participate in the study, 150 teleworkers completed the Teleworkers' Security Survey (Godlove, 2011). The survey population and access was available to the membership of The Telework Exchange, a community that self-identified as actively involved in the telework environment. 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.

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 information security controls. For example, managing and maintaining appropriate levels of computer virus protection, firewalls, and user access is more difficult when remote computer systems are used by teleworkers (Scarfone et al., 2009). The ability to maintain information security by providing a secure environment to prevent destruction or theft of computers or data storage devices can be more difficult in a teleworker environment when work is completed in the office (Scarfone et al., 2009).

A study was conducted by Ernst & Young (2008) to assess organizational data security policies and practices concerning teleworkers. A key finding reported was that while business leaders realize that teleworkers represent data security risks, these businesses have not given sufficient attention to dealing with these risks. In addition, it was also reported in the Ernst & Young report that teleworkers in an organization often cross several departments and organizational boundaries that involving the sharing of responsibility for maintaining data security. This can create a problem of ownership of the responsibility for maintaining data integrity and security among teleworkers, especially in terms of identifying and correcting gaps in protection policies and procedures (Ernst & Young, 2008). Another significant finding reported by Ernst & Young was that more than half of those who participated in the study had no policies in place or provided training for teleworkers regarding how to maintain data integrity and security.

Office-based computers and other data retrieval and storage systems often are housed in buildings with security features such as patrol of the premises by security personnel, motion detectors, camera surveillance, and monitored access to offices and computers. While some teleworkers have homes with security systems, it is impossible to monitor the effectiveness of these systems and the extent that security systems are used by teleworkers (Scarfone et al., 2009). Another challenge to data security with teleworkers is that in an office environment, access to data and information can be controlled using a local area network. Teleworkers often have to access data and information from the outside, increasing the risk of security breaches during periods of information retrieval and transmittal (Scarfone et al.). Storage integrity and confidentiality are more difficult to monitor for teleworkers in remote locations than in an office environment (Scarfone et al., 2009). As a result, the attitudes, social pressures, sense of control, and willingness of teleworkers to follow data security procedures are important factors to consider

when creating and maintaining an information security plan. The research focused on the relationship between the Theory of Planned Behavior and teleworkers' attitudes about compliance with security requirements in a teleworking environment.

The theoretical study population of The Telework Exchange community was 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. 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 information 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 Theory of Planned Behavior is a useful explanatory model in this context.

In the 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 nonteleworker, 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.

2.3. Data Collection

Data related to the dependent and independent variables were collected through the Teleworkers' Security Survey (Godlove, 2011) presented in Table 1 and interpreted through an analysis of the survey results. The three independent variable 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 independent variable used five points on the scale ranged from 1 = *strongly disagree* to 5 = *strongly agree*. The one dependent variable item measured the extent to which the respondent indicated a willingness to follow the organization's information security guidelines. The dependent variable used a five-point willingness scale ranging from 1 = *very unwilling* to 5 = *very willing*. The quantitative study consisted of the analysis of the results from the Teleworkers' Security Survey (Godlove, 2011) completed by a sample of the members of The Telework Exchange.

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. Expert validity of the instrument was further supported through the examination by two information security experts. The assessment of the survey instrument confirmed that the survey covered the relevant variables and conceptual domains. A pilot test was completed by 10 information security professionals and a test-retest pilot was completed by another group of 10 different information security professionals, both groups were teleworkers.

Data collection was accomplished through the use of a Web-based, survey-writing program linked on The Telework Exchange Website for 30 days. In these 30 days, 180 respondents completed the survey. Of those 180 respondents, 150 indicated that they were teleworkers, and their responses were included in the study.

3. RESULTS

The objective of this study was to examine teleworkers' attitudes regarding compliance with security requirements in a teleworking environment using Ajzen's Theory of Planned Behavior. The analysis of survey data consisted of both descriptive and inferential statistical techniques to identify 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 p attitude, social pressure, and sense of control scales explained willingness to follow an organization's security guidelines.

3.1. Descriptive Analysis

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).

TABLE 1 List of survey items

No.	Survey Item
1.	I believe that information stored on an organization's computers is vulnerable to security incidents.
2.	Information security and data protection associated with telework are serious and need attention
3.	Understanding the importance of information security and practices is important.
4.	My organization disciplines employees who break information security rules.
5.	If I were caught violating my organization's information security policies, I would be disciplined.
6.	My organization terminates employees who repeatedly break security rules.
7.	Adopting security technologies and practices is important in a telework environment.
8.	My organization communicates the importance of confidentially and privacy of data periodically.
9.	I am asked to sign a telework statement to protect and maintain the value of data and its integrity periodically.
10.	My manager's attitude toward information security when teleworking is serious.
11.	My colleagues, who follow the information security procedures, create pressure forcing me to follow them.
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.
13.	Telework practices in my organization are frequently monitored for policy violations.
14.	My organization's information security procedures in a telework environment are unreasonable.
15.	My organization's information security procedures are clear on how to protect organization's data in a telework environment.
16.	I have encouraged other employees to take steps to ensure the organization's data is protected in a telework environment.
17.	Every employee can make a difference when it comes to helping to secure the organization's data in telework environment.
18.	I am convinced other employees comply with the organization telework guidelines.
19.	I have personally taken steps to ensure the organization's data is protected when teleworking.
20.	When organizational data is in my control, security threats are minimized.
21.	Taking proper security measures of data in my control is my personal responsibility.
22.	I am likely to follow organizational information security policies when working in a telework environment.
23.	I have enough knowledge to protect the organization's data in telework environment.
24.	My involvements in information security programs make me adhere to them.
25.	My organization's computer equipment procedures are so restrictive in a telework environment that they interfere with my job performance.
26.	Information security requires more technical solutions in a telework environment.
27.	Employee computer practices are properly monitored in a telework environment for policy violations.
28.	Please indicate the degree of your willingness to follow the organization's information security guidelines.

Personal Attitude Scale

Descriptive statistics were generated for scale items and composite scale scores. 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. Teleworkers largely recognized the importance of information security and practices (M = 4.77). Teleworkers also indicated a strong belief that there was a serious need to protect information data (M = 4.47), that adopting security technologies and practices in a telework environment was important (M = 4.42), and that information stored on an organization's computers was vulnerable to security incidents (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. Teleworkers were neutral in ratings of the extent to which the organization disciplined employees who broke information security rules (M = 3.15) or terminated those who repeatedly broke security rules (M = 3.03). Teleworkers were neutral in their beliefs that the organization communicated the importance of confidentiality and privacy of data (M = 3.55) and that they would be disciplined if caught violating information security policies (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 (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 ranged from *neutral* to *agree* that it was important to maintain the security and integrity of the organization's data.

Social Pressure Scale

The mean ratings for the nine Social Pressure Scale items ranged from a high of 4.48 for the belief that every employee could make a difference when it cause to securing an organization's data in a telework environment, to a low of 2.17 for the belief that an organization's information security procedures in a telework environment were unreasonable.

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. Teleworkers believed strongly that every employee could make a difference when it cause to helping secure data in a telework environment (M = 4.48). In addition, teleworkers believed strongly that they would follow the directions of their managers regarding security measures to protect the organization's data (M = 4.33). Teleworkers were neutral in their perceptions about the extent to which they encouraged co-workers to follow security procedures (M = 3.72), belief that others complied with security procedures (M = 3.51), and the influence of a manager's attitude toward the seriousness of teleworkers to maintain information security (M = 3.48).

The lowest rated items were teleworker perceptions about the unreasonableness of security policies (M = 2.17) and monitoring frequency of violations to security policies (M = 2.99). Teleworkers were neutral in their perception about how much other employees pressured them to follow information security procedures (M = 3.03) and neutral to moderate in their agreement whether how to protect data was made clear by the organization (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 follow information security procedures.

Sense of Control Scale

The mean ratings for the nine Sense of Control Scale items ranged from a high of 4.45 for a belief that taking proper security measures for data was in one's control and a personal responsibility, to a low of 2.41 for the belief that security measures of the organization were restrictive to the telework environment and interfered with one's job performance.

The highest rated items concerned teleworkers' sense of control over taking proper measures and following security policies and practices to protect data in a telework environment. Teleworkers believed strongly that they were responsible for and in control of taking proper security measure to secure the integrity of data. Teleworkers also indicated strong beliefs in following information security policies and taking steps to ensure that data were protected when teleworking. Teleworkers were in agreement with the perceptions of a sense of control over reducing threats and about the extent to which involvement in information security programs made teleworkers adhere to them.

The lowest rated items were teleworkers' 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. Teleworkers were in agreement that they had enough knowledge to protect the data in a telework environment. Teleworkers were neutral in their perceptions about the technical solutions necessary to implement information security policies and how teleworker computer practices were properly monitored for policy violations. Teleworkers disagreed that an organization's computer equipment procedures were restrictive and interfered with job performance. 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.

3.2. Analysis and Findings of Study Questions

A multiple 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. The research question was about the extent to which there were relationships between personal attitudes, perceptions of social pressure, and sense

of control, and teleworkers' willingness to follow an organization's information security guidelines?

The relationship between items on the Personal Attitude Scale and willingness to follow an organization's information security guidelines were weak. Though considered statistically significant due to sample size, no real relationship was identified between willingness to follow security procedures (dependent variable) and several items on the Personal Attitude Scale. The strongest correlations between the dependent variable and Personal Attitude Scale items were only moderate at best. There was a weak to moderate relationship between perceptions of understanding the importance of information security and practices and willingness to follow security procedures (dependent variable) and belief that adopting security technologies and practices was important in a telework environment.

There was a relationship noted between the overall Personal Attitude Scale score and the dependent variable of willingness to follow security guidelines. Therefore, results failed to reject the alternative hypothesis that there was a relationship between willingness to follow security policies and the Personal Attitude Scale. However, while relationships were noted, they were weak or very weak.

A regression analysis was performed 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. The unstandardized β coefficients indicated that Personal Attitude 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 analysis of variance (ANOVA) from the regression analysis, the Personal Attitude model was statistically significant. From 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, "If I were caught violating my organization information security policies, I would be disciplined," to a high of .362 for, "Understanding the importance of information security and practice is important." On the basis of these standardized β coefficients, it was concluded that the items on the scale had only a slight influence on the criterion variable. The R values for the model indicated that, overall, the model is weak 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.

Social Pressure

A multiple regression analysis was used to examine the relationship between items on the Personal Attitude Scale and willingness to follow 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 follow security procedures (dependent variable) and several items on the Social Pressure Scale.

The strongest correlations between the dependent variable, willingness to follow an organization's information security guidelines, and the Social Pressure Scale items were weak to moderate at best. 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 the dependent variable ($r = .400$) and following managers' advice on security measures to take ($r = .349$). A weak to moderate negative correlation was noted between willingness to follow security guidelines and perceptions that telework security procedures were unreasonable ($r = -.384$). In other words, as willingness to follow procedures increased the perceptions of security guidelines as unreasonable decreased.

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 was 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.

3.3. Regression Analysis

Regression analysis was performed to assess how well the nine items on the Social Pressure Scale explained the dependent variable of willingness to follow an organization's information security guidelines. 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. On the basis of ANOVA from the regression analysis, the Social Pressure model was found to be statistically significant, $F(9,139) = 6.893$, $p < .001$. On the basis of this significant finding, results failed to reject the alternative hypothesis that there was a significant relationship between items on the Social Pressure Scale and the dependent variable. However, standardized β coefficients ranged from a low of .019 for "My colleagues, who follow the information security procedures, create pressure forcing me to follow them," to a high of .255 for "Every employee can make a difference when it come to helping to secure the organization's data in a telework environment." On the basis of these standardized β coefficients, the items in the scale had 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 was a weak to moderate model because 26.4% of the variance in the dependent variable was explained by the social pressure predictor variable.

Sense of Control

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. While several correlations were significant, these correlations were weak. No real relationship, or a negligible relationship, was noted between willingness to follow security procedures (dependent variable) and several items on the Sense of Control Scale (see items 23, 24, 26, and 27 in Table 2).

The strongest correlations between the dependent variable and Sense of Control Scale items were noted for items 19, 20, 21, and 22. There were low to moderate correlations between the dependent variable 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 could take steps to ensure data is protected in a teleworking environment (item 19, $r = .381$) and that when organizational data are 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 was no real relationship between willingness to follow security policies and the Sense of Control Scale.

Regression analysis was performed to assess how well the nine items on the Sense of Control Scale explained the dependent variable (see Table 3). 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

TABLE 2 **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 the organization's data is protected when teleworking.	.373***
20	When organizational data are 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 the organization's 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 they interfere 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.

TABLE 3 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 the organization's 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 the organization's data in telework environment.	−.09	.06	−.15	−1.60	.112
24	My involvement 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 they interfere 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

ANOVA from the regression analysis, the Sense of Control model was statistically significant, $F(9,139) = 6.442$, $p < .001$. On the basis of 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. 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." On the basis of these standardized β coefficients, the items in the scale had 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 was 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.

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 4). The unstandardized β coefficients indicated that personal attitudes and social pressure did not appreciably influence the dependent variable. The standardized β coefficients showed that both the Personal Attitude and Social Pressure Scale scores contributed little to the model. The Sense of Control Scale score was the only statistically significant predictor variable, $t(3,45) = 3.212$, $p = .002$. The standardized β coefficient of .325, although statistically significant, 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 was a poor model because only 10.6% of the variance in the criterion variable was explained by the predictor variables.

TABLE 4 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. FINDINGS

Overall, teleworkers strongly agreed that they were willing to follow the organization's information security guidelines. In terms of personal attitudes, teleworkers believed strongly that information data were 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. Teleworkers 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, teleworkers did not express strong agreement that the organization communicated effectively the need to protect data used on their computers. While teleworkers had mixed attitudes about how well organizations communicated the importance of protecting data, teleworkers were more likely to follow policies and procedures when they were given information and guidelines on how to create a more secure work environment.

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. The failure of teleworkers to comply with policy and procedures may be related to the level of importance given to training and ongoing communication about data security; the more interaction with the teleworker, may result in greater willingness to regularly comply with data security guidelines.

Overall, weak relationships were found between the dependent variable willingness to follow security guidelines and the independent variables, composite scores on the Personal Attitude, Social Pressure, and Sense of Control scales. 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.

5. DISCUSSION

The findings in the study support the Theory of Planned Behavior and provide further information about the influence of motivations and intentions in the willingness of teleworkers to comply with policies and practices that protect the security and integrity of information data used in telework environments. Data analysis provided evidence that teleworkers recognized the threat of security breaches and were willing to take steps to protect the security and integrity of data. In addition, teleworkers appear to recognize the threat apart from this being communicated to them by the company. 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.

5.1. Implication for Future Research

This study provides a survey instrument that may be further refined and validated in future studies using different variables. Using the survey instrument, researchers may explore other theoretical frameworks. In addition, researchers may use the survey instrument

and apply the same study design to target different demographic, for example, different age group, y gen, baby boomers, or an organization with only teleworkers.

While 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.

Though 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.

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.

5.2. 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 computers with software that controls access and transferability of data 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 nonwork-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 the use of teleworkers' computers used for both work and personal activities.

5.3. 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. Telework takes place in multiple locations with differing types and levels of access to data. This may result in different levels of attention to security by teleworkers; therefore, policy makers must have in place a clear protocol on how to address information data security issues that match the level of data access and security required. Education is vital because teleworkers who understand the importance of

data security and how best to 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.

Policy makers 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).

6. CONCLUSION

The study explored whether the Theory of Planned Behavior provided an explanation for the motivating factors that influence teleworkers to follow security guidelines. The results established that teleworkers believed strongly that information stored on an organization's computers was 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, the data demonstrated that beliefs were not strongly linked to a willingness to follow an organization's information security guidelines. Other motivating factors could be influencing teleworker willingness to comply with security policies and procedures that were not identified in the current study. Possible latent factors could be levels of influence of social pressure and subjective norms on the willingness to follow organization information data security guidelines. From the standpoint of information security research, this study contributes to the body of literature regarding teleworker motivations and intentions and how these affect complying with organizational data security plans. Factors were identified through this study that contributed to teleworkers' willingness to follow company data security policies and practices in telework environments.

ACKNOWLEDGMENTS

The author thanks David Oxenhandler, President of University of Fairfax, Vienna, Virginia, United States and members of his dissertation committee, Dr. Jean Gordon, Dr. David Lease, and Dr. Laura Pogue, for their assistance in guiding this research. A special thanks to Dr. Ken Bahn, Dean of Doctoral Research and Janice Orcutt, EdS., Dean, Academic Systems, Services and Assessment both of University of Fairfax for providing support. Cindy Auten, General Manager of The Telework Exchange also deserves special thanks for graciously providing the research site and actively supporting the survey assessment, without which this study could not have been completed.

REFERENCES

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

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

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

Ernst & Young. Center for Democracy & Technology. (2008). *Risk at home: privacy and security risks in telecoummting.* Retrieved from: https://www.cdt.org/privacy/20080729_riskathome

Godlove, T. R. (2011). *Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines.* Doctoral dissertation, University of Fairfax.

Horner, J. (2011). Telework: Saving gas and reducing traffic from the comfort of your home. Mobility Choice [Online]. Retrieved from http://www.mobilitychoice.orgMCtelecommuting.pdf/

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

Kilpatrick, I. (2007, November). Dam data leakage at source: How unified encryption management (UEM) is changing the threat landscape. Software World, 12(4). Retrieved from http://www.thefreelibrary.com/Dam+data+leakage+at+source%3A+how+unified+encryption+management+(UEM)...-a0172560692

Ponemon, L. (2007). The business impact of data breach. Traverse City, MI: Ponemon Institute. Retrieved from http://www.scottandscottllp.com/resources/data_breach.pdf

Scarfone, K., Hoffman, P., & Souppaya, M. (2009). Guide to enterprise telework and remote access security: Recommendations of the National Institute of Standards and Technology. Special Publication 800-46, Revision 1. Washington, DC: U.S. Department of Commerce.

Tallberg, E. (2011). What is telework? WiseGeek.com [Online]. Retrieved from http://www.wisegeek.com/what-is-telework.htm
Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). New York, NY: Harper and Row.

BIOGRAPHY

Timothy Godlove, Ph.D. is Senior Program Manager for the Department of Veterans Affairs. Dr. Godlove has more than 25 years of experience in multidimensional administrative, information technology, information assurance, project and risk management, and strategic planning. He holds a Ph.D. in information assurance from the University of Fairfax, Vienna, Virginia, a Master of Science Administration degree in information resources management from Central Michigan University, a Bachelor of Arts from Chapman University, and he has completed the Chief Information Officer Program at the National Defense University. He also holds the Information Assurance (NSTISSI No. 4011) and Federal IT Security Professional-Manager (FITSP-M) certifications. Dr. Godlove 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 in information security journals.