An Empirical Investigation of Factors Influencing Information Security Behavior

Sunil Hazari, University of West Georgia – Carrollton, GA, shazari@westga.edu
William Hargrave, University of Georgia – Athens, GA, bhargrav@live.com
Beth Clenney, University of West Georgia – Carrollton, GA, bclenney@westga.edu

ABSTRACT

The topic of information security has been studied mostly in the context of organizational and enterprise security. Today, organizational employees who are also home users of computing technology are vulnerable to security breaches unless they abide by company policy to use safeguards such as firewalls and antivirus programs. It is important to understand factors that influence Work Related Home Computing (WRHC) users to maintain information security. This study uses Ajzen's Theory of Planned Behavior to investigate factors related to WRHC users' information security awareness. Demographic characteristics, attitudes, subjective norm, and perceived behavioral control that affect behavioral intention were studied to identify determinants of information security behavior. It was found that intention to maintain information security behavior was predicted mostly by exogenous variables of attitude and confidence of participants in the study.

KEY WORDS

Information security behavior, Ajzen's Theory of Planned Behavior, Path Analysis, Information Security Education, Social and Behavioral Aspects of Information Security.

INTRODUCTION

News about computer crime, identity theft, viruses, and spam is regularly being reported by the media and popular press (Aytes & Connolly, 2004; George & Scerri, 2007). Security threats have kept pace with advances in technology and information systems; they have become even more dangerous. The 2008 FBI/CSI survey of computer crime and security noted that virus attacks are the major source of financial loss, and web hacking incidents have increased dramatically over the past years. Although the majority of respondents to the survey believe that security awareness training for end users is important, not many organizations invest enough resources to provide this training (Richardson, 2008). According to the NCSA/Symantec home user study (2008), 68% of users surveyed admitted to keeping sensitive information (health, financial, personal records) on home computers, and 74% admitted to using the Internet for activities such as banking, stock trading, or reviewing personal medical information. Individuals routinely access banking, finance, and hospital records from computers that may be vulnerable to spyware infections. There is a

constant effort by hackers to compromise security of organizations and individual users by manipulating users to divulge passwords and other confidential information (Adams & Sasse, 1999). Today's new mobile workforce uses wireless and other Internet connected devices from remote locations to access corporate resources irrespective of geographical boundaries. Changes in working conditions require users to work from home offices; which in turn makes it necessary to implement information security at home as well as at the office to maintain ethical and secure behavior (Leonard, Cronan, & Kreie, 2004). E-mail communication with attachments (i.e. spam) poses another threat for incoming and outgoing traffic. In corporate environments, this threat can be combated by using spam filters, white lists, and opt-in/opt-out protocols. It is doubtful that home computing users are aware of available prevention techniques; moreover, they may not have the attitude, competency, or confidence to deter spam, viruses, and spyware infections. This study focuses on employees who perform work related duties from home, either on a part-time or full-time basis. This group is identified as *Work Related Home Computing* (WRHC) users, and the study investigates factors that influence information security behavior of WRHC users.

Straub and Welke (1998) studied the information security risk faced by organizations and identified deterrents and preventive measures for maintaining enterprise information security and controlling risk. Although their research was important, it did not directly apply to home users who may not be governed by organizational policies, and generally have full administrative privileges on their systems. The characteristics of WRHC use are different from organizational computing. Whereas enterprise computers may be behind firewalls, and have updated anti-virus programs installed, a home user is left vulnerable because of lack of management and technical controls. A WRHC user needs to have knowledge of technical and managerial aspect of information security to maintain effective controls. In most organizations there are technicians to maintain enterprise security on several fronts. On the other hand, a WRHC user is solely responsible for all aspects of security on the home system, and it is this weakness that is often exploited by hackers. Spinellis, Kokolakis, and Gritzalis (1999) stated the use of home computers for organizational work can be the source of information security risk, because home environments lack the technical expertise and resources to create and maintain a suitable level of security.

Although technical measures can protect information to a certain degree, users have been consistently identified as the weakest link in the information security chain (Rhodes, 2001; Schneier, 2003; Whitman & Mattord, 2003). Similar to organizational understanding of deployed IT resources and propensity for risk impact, creating related awareness and understanding of information security in home users could deter the chain of events that can lead to loss of data and information (Kotulic & Clark, 2004). In the area of information security, research has often lagged in practice. Dhillon and Blackhouse (2001) stressed the need for more empirical research to develop key principles for the prevention of negative events and therefore to help in the management of security. Aytes and Connolly (2004) noted that further research is needed in areas where users may experience personal financial loss (e.g. identity theft,

credit card fraud) to better understand what risks users are less willing to take. West (2008) also called for a better understanding of principles on how users come to make decisions about information security.

There is a human element to information security that deals with psychology, motivation, education, and social aspects. This area of *Behavioral Research* addresses why some people are more prone to being hacked and become victims of identity theft and consumer fraud (Kabay, 1993). Pee, Woon, and Kankanhalli (2008) have studied factors influencing employees' non-work-related behavior where the focus was exclusively on employees' use of the Internet for personal use. In contrast to their research, this study takes a different approach by extending the research to employees' work-related computing from remote locations such as employees' residence, public libraries, or cybercafés. Such environments can be used for accessing corporate information required to fulfill job responsibilities. There is, therefore, a need to seek a deeper level of understanding of information security behavior that has become part of daily life of WRHC users. While the category of "home user" is very broad, and may include children, students, housewives, senior citizens etc., a more focused group within this category that can be considered a subset with common characteristics is WRHC users. In this study, the WRHC group was represented by business students at a university. This group was chosen because business students regularly access information that resides in secured environments (such as grades, registration records, library databases, knowledge based systems, and case studies), and business students often work in teams to create knowledge-based documents, such as business plans, company reports, and presentations. The purpose of this study was to investigate factors related to WRHC users' information security awareness. Data related to demographic characteristics, attitudes, subjective norm, and perceived behavioral control that affect behavioral intention were collected to identify determinants of information security behavior.

INFORMATION SECURITY BEHAVIOR

Information security is an important concern for businesses. Companies invest significant funds to ensure that buildings and systems are technically secure, but the responsibility that employees have for maintaining information security is often overlooked. According to Chan, Woon, and Kankanhalli (2005), a breach in security does not generally result from a flaw in the technical system but can be a result of noncompliant employee behavior. These researchers suggest shifting focus to learn why noncompliant behavior takes place. Chan et al. conducted research to determine the factors most common in noncompliant behavior. The two primary factors they were able to identify include individual perception climate and self-efficacy. According to their research, these two factors explained only 26.5% of non-compliant behavior. The researchers further suggested that other factors such as employee habit must account for the remaining behavior, but additional research would have to be conducted. Additionally, the researchers studied the importance of coworker socialization as a part of an employee's environment. The specific relationships

between employees were cited as having a notable impact on employees' propensity toward compliance with information security procedures.

Another study by Banerjee, Cronan, and Jones (1998) found that ethical versus unethical behavior with regard to information security was determined primarily by environment and personality. They also found that intention to behave ethically had bearing on employee behavior and cited that the single strongest factor was the environment. The study emphasized the importance of environment as well as the individual employee. Another factor that affects employee behavior toward information security, and depends on both the environment as well as the individual employee, is task load (Biros, Daly, & Gunsch, 2004). The task load assigned to each employee depends on the environment of the company, and the heavier an employee's task load, the less responsibly they behave with regard to information security. WRHC users may choose to bring work home if the task load is high. Kabay (1993) stated that established principles of social behavior can teach organizations a great deal as they attempt to improve corporate and institutional information security. Enhancing security depends on changing the beliefs, attitudes, and behaviors of individuals and groups, therefore, it follows that social psychology can help organizations understand the best way to work with people to achieve this goal.

The issue of information security behavior at different levels has also been addressed at the government policy level. In outlining a National Strategy to Secure Cyberspace, a set of questions were chosen under different levels (such as home users and small business, large enterprises, critical sectors / infrastructures, national issues and vulnerabilities, and global level) to identify issues to be addressed in the national strategy. Specific under "Level 1: Home users and small business", the questions addressed awareness programs for cybersecurity, assistance from ISP's, disclosure of risk by ISPs and vendors, risks endemic with emerging technologies such as broadband connectivity, and federal broadband initiatives (National Strategy, 2003).

INFORMATION SECURITY LITERACY

Based on newly identified threats, a better understanding of what constitutes information security literacy for end users is needed. The evolution of information security literacy awareness parallels the advancement of computer literacy over the years. The genesis of mainstream computer technology can be traced from introduction of personal computers in the 1980s; network connectivity, graphical user interfaces and the Internet in the 1990s; and the use of portable, mobile, and wireless devices in recent years. Johnson (1980) defined computer literacy as being the ability to conceptualize problems algorithmically to represent them in the syntax of a computer language, to identify conceptual bugs and to express computational ideas with a high degree of organization and readability. Expanding this definition, Bitter (1983) referred to computer literacy as the competency to know how computers work, the ability to enter and retrieve data, knowledge of future general directions of computers, understanding the abuse and misuse of computer technology. The "abuse and misuse" concept can be considered to have elements of information security

behavior. The definition of computer literacy changed from a primary focus on programming languages to a consideration of operational aspects of computers applications and the Internet (Hazari, 1990). Computer literacy in recent years involves the ability to word process documents, send and receive e-mail, use a search engine, and connect to the World Wide Web (Hoffman & Blake, 2003). WRHC users are increasingly involved with using the Internet to access corporate information such as email that may contain proprietary data, so computer literacy plays an important part in maintaining information security behavior.

Just as computer literacy has evolved, information security literacy has changed over the years. There are several ways in which information can be protected. One method to safeguard information is by using controls. General controls include personnel, physical and organizational controls as well as technical security services and mechanisms (Summers, 1997). For WRHC users, computer security controls can be hardware or software based, and may include biometric devices, anti-virus software, firewalls, intrusion detection systems, spyware detection, and antivirus programs. Lack of controls and the anonymity offered by the web makes all users vulnerable to cybercrime (Parameswaran & Whinston, 2007). Employees are beginning to use Web 2.0 components, MySpace, Facebook, Wikis, Blogs, and RSS feeds as part of their daily computer use. Many companies are allowing employees to use these sites because of the benefits of collaborative technology, but to counter threats brought about by using these websites, companies have also implemented controls such as URL filtering and antivirus scanning as part of the enterprise security policy. However, small businesses may lack the resources to make this part of a comprehensive security policy. Social networking sites in particular have become a huge phenomenon on the Internet and users on these sites are very vulnerable to cybercrime. MySpace and Facebook, two of the largest social networking sites host hundreds of thousands of personal web pages created by their users (Krantz, 2006). These sites allow sharing of pictures, music, and videos, and they are a window into the life of individuals of all ages. In social networks, since users freely exchange multimedia content, a huge potential exists for viruses and other threats, to be spread throughout the network. In addition to network security threats, the sites also provide a venue conducive to identity theft because they encourage users to volunteer personal information and post photos that become accessible by all in web space. Most users willingly provide this information without realizing the consequences of their actions.

With thousands of new users joining social networking sites daily, the potential for malicious content to be exchanged greatly increases. Given the nature of these sites, WRHC users tend to be highly trusting and less aware of the security issues that may be present. Innocuous appearing web pages visited by users may contain code fragments that can initiate attacks from the client device (Parameswaran & Whinston, 2007). Although the firms hosting these websites have some security measures in place, they are not able to police all of the new files being posted daily.

Cybercrime has a strong presence in social networking sites which have been characterized as tainted with illegal activity and disregard for social norms (George &

Scerri, 2007). Predators seeking personal information do not have to search far to find employer information on many users' web pages. Many users post birth date, address, and telephone information. Users assume that the information will be used for positive reasons, and they neglect to see the dangers with posting this information can present. Criminals masquerading under other identities can persuade individuals to provide even more personal information. The problem has become so widespread that many businesses have banned or filtered access to these social networking sites; however, these bans and filters can be easily defeated especially when WRHC users access the sites from their home computers. Employees often become victims of identity theft or confidence tricks as well. Therefore, a study of information security awareness behavior for WRHC users is necessary to mitigate threats posed by Web 2.0 computing.

THEORETICAL MODELS

Most of the research on information security awareness has been descriptive and has not fully explored the possibilities offered by motivation and behavioral theories, or the technology acceptance models in the information security domain (Mathieson, 1991; Siponen, 2000; Legris, Ingham, & Collerette, 2003). Technology acceptance models such as Rogers' (1995) Innovation Diffusion Theory, and Davis' (1989) Technology Acceptance Model have been studied by Information Systems researchers primarily in terms of human factors and IT adoption. Only recently have some empirical studies (e.g. Woon, Tan & Low, 2005; Pee, Woon, & Kankahalli, 2008) used theories such as Protection Motivation Theory, and Theory of Interpersonal Behavior to identify variables affecting decisions related to information security behavior. Along similar lines, Lee and Kozar (2005) had investigated factors affecting adoption of specific technology (anti-spyware systems) by individuals. Human compliance with information security rules require an understanding of how people (e.g. WRHC users) work and think (Highland, 1993).

Some research (e.g. Foltz, 2004; Workman & Gathegi, 2006) has looked at computer crime and information security in the context of Ajzen's (1988) Theory of Planned Behavior (TPB). TPB was based on an earlier Theory of Reasoned Action (TRA) which stated that intention is the prime reason a person will perform a given behavior. The person's behavior will be determined by attitude toward the behavior, belief about the outcome of the behavior, value of the outcome, social impact of other people (called subjective norm), and the person's motivation to adhere to the opinions of others. However, there is a gap in the literature with respect to whether this behavior will be the same in different environments. Will the employee behave the same at the workplace where there are higher levels of technical controls as they may when working at home where they may not be required to adhere to an information security policy? Subjective norm also plays an important part in maintaining information security awareness (Bannerjee et al., 1998). The fact that most individuals can be duped is supported by a research study on phishing websites where 90% of participants were fooled by authentic looking fake sites. Those participants were computer-savvy, and they were specifically performing the task of identifying phony

sites. The only participant in the study not fooled by some of the phishing sites typed in each legitimate address in a separate window and compared the sites. This participant had learned to do this because a family member had previously been duped in a phishing scam (Dhamija, Tygar & Hearst, 2006). This example relates to subjective norm mentioned earlier.

Extending the TRA, the Theory of Planned Behavior (TPB) also introduced the concept of *perceived behavioral control* over skills necessary to perform the behavior. This added construct of perceived behavioral control is similar to Bandura's concept of self-efficacy (1997) which is a person's confidence in their ability to perform the behavior. For this study, confidence in maintaining information security was used as an aspect of perceived behavioral control. TPB theory is based on attitude, subjective norms, and perceived behavioral controls of users that explain behavior intention toward information security awareness. As shown in Figure 1, Ajzen's Theory of Planned Behavior model was used in this study. In this model, a causal flow is proposed from exogenous variables such as attitude, subjective norms, and confidence. The model also studied the relationship between exogenous variables.

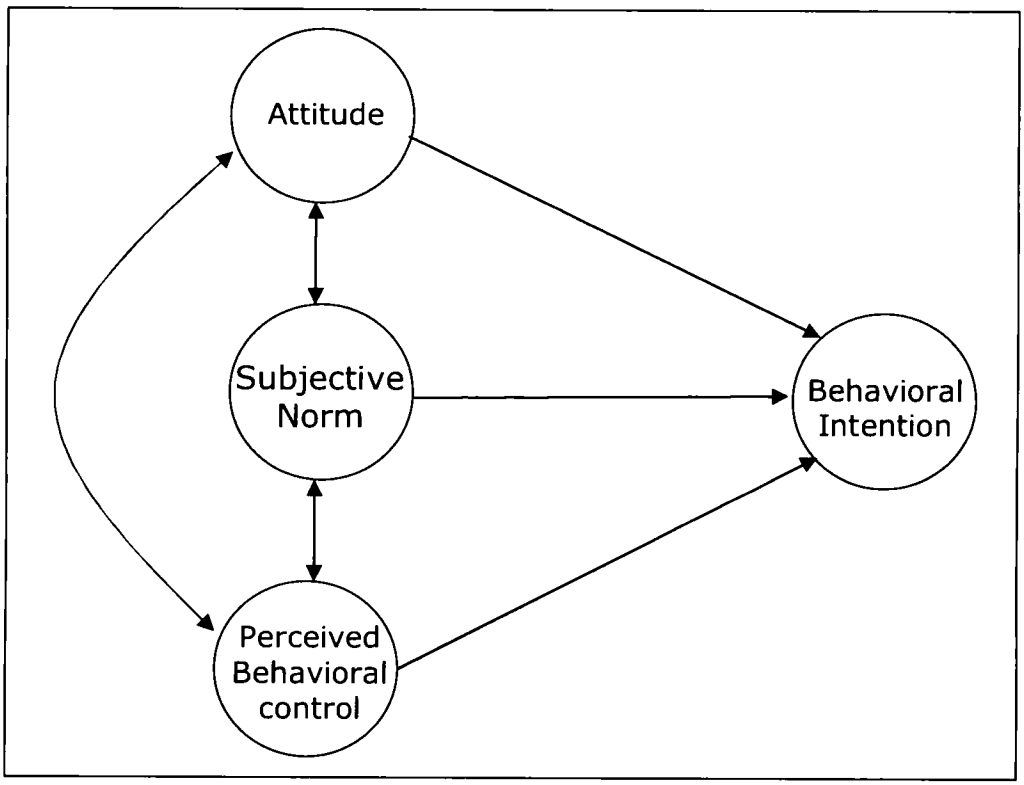

Figure 1. Ajzen's Theory of Planned Behavior

Using the Theory of Planned Behavior, this study investigated WRHC users' behavioral intention relating to awareness of information security on their computers.

Individual attitudes toward information security awareness, the perceived beliefs that are held by other people around WRHC users, characteristics, work experience and current knowledge about information security, were hypothesized to predict the strength of their behavior as follows:

H1: Individuals with more experience will have higher knowledge of information security behavior.

H2: Attitude, subjective norm, and confidence in WRHC users may correlate with each other, as well as with behavioral intention to maintain information security behavior.

H3: WRHC users' behavioral intention to maintain information security can be predicted by attitude, confidence and subjective norm.

What these hypotheses imply is a WRHC user with positive attitude toward information security awareness, who feels informed, and who is confident, will be more likely to maintain information security on his/her home computer. Although TPB has been tested in the past with other types of employees (e.g. Workman & Gathegi, 2006; Dinev & Hu, 2007; Pee, Woo, & Kankahalli, 2008), it has not been tested with WRHC user group demographics. The above hypotheses were tested using empirical data collected as part of the study.

METHODOLOGY

The study included approximately 200 business students (undergraduate and graduate) enrolled in the Business School at a state university in Southeast United States. Business students were chosen for this study as they would be working in positions that require use of information technology in functional areas such as Marketing, Finance, and Information Systems. In most universities, the curriculum prepares business students to work in simulated organizational environments where they access secured databases using passwords (e.g. library), create assignments, such as business plans that may contain proprietary data, discuss cases, and develop presentations in a team environment. Access to information resources for completing tasks can be on-campus or from remote locations. The use of business students as surrogates for professionals or executives in reference to use and evaluation of technology has been found to be acceptable (Briggs, Balthazard, Dennis, 1996). Since the workplace environment has changed and is no longer limited to corporate offices, ubiquitous connectivity of technology devices (such as laptops and PDA's) requires having some knowledge about maintaining information security awareness. An on-line questionnaire was made available to participants of the study. It included 12 scale items relating to information security awareness taxonomy categories. Additional demographic and computer usage items were also included in the questionnaire. A knowledge quiz was administered as part of the questionnaire to identify security awareness and relate this to self-reported measures. Before administering the

questionnaire, items were validated by a group of information systems faculty who provided recommendations for modifying items that they considered unclear or ambiguous. This provided content validity to the questionnaire. The constructs and indicators (observed variables) relating to Ajzen's Theory of Planned behavior that was used in this study was modified from previous research. Attitude items were adapted from Ajzen (1991); Subjective Norm items were adapted from Taylor and Todd (1995); Perceived Behavioral Control items were adapted from Compeau and Higgins (1995), Taylor and Todd (1995); and Intention items were adapted from Davis (1989), Chau and Hu (2001).

The construct of *Attitude* refers to interest, motivation, and degree toward evaluation of behavior; *Subjective Norm* is the influence of others and social pressure that may lead to performing a behavior; *Perceived Behavioral Control* is an individual's confidence in performing a behavior; *Intention* is antecedent of performing a behavior which will lead to a desired outcome. Indicator variables used within each construct were as follows:

Attitude:
A1: I am interested in maintaining security on computer(s) I own or use
A2: I like working with computers
A3: A secure computer would help me avoid problems when accessing the Internet

Subjective Norm:
S1: My friends/family would think highly of me if they knew I maintain security on my computer
S2: I recommend to my friends/family that they should use security programs on their computers
S3: When browsing the Internet I use security on my computer because I have heard from others it is the proper thing to do

Perceived Behavioral Control:
C1: I am confident that I can learn about maintaining security on computers I own or use
C2: I am confident that I can install and maintain software such as firewall or antivirus programs on my computer
C3: I am confident that I can identify any problems on my computer that are a result of weak security on my computer

Behavioral Intention:
I1: I intend to keep maintaining security on my computer after this semester is over
I2: When using the Internet, maintaining computer security is a high priority for me
I3: I would like to learn more about the general area of computer security

DATA ANALYSIS AND RESULTS

Data analysis was conducted using SPSS/AMOS software. Results included inter-item reliability of indicators (observed variables) in the scale. The elements in the model were checked to determine if they were significantly related to each other. Cluster Analysis was used to distinguish between levels of knowledge of respondents. A Path Analysis was then conducted to test the fit between data collected in this study as it applied to Ajzen's model. Results are given as below.

The total number of respondents to the questionnaire was 179. There were 106 females and 73 males. All but three students indicated that they owned a computer. The survey included four constructs: Attitude, Subjective Norm (SN), Perceived Behavioral Control (PBC), and Behavioral Intention (BI). Each construct was represented by measurable indicators in the survey. The indicator items were presented randomly to respondents in an online survey. Data was collected using a seven point Likert scale with "Strongly Disagree" and "Strongly Agree" as anchors and "Undecided" as midpoint.

Hypothesis 1: Individuals with more experience will have higher knowledge of information security behavior.

Respondents' awareness and knowledge had previously been shown to prevent risky behavior (Luckwago et al., 2003). For this study, to determine knowledge of students' awareness of information security, a seven-item quiz was administered to respondents. Validity of the quiz was established by getting input on items from two instructors who teach information systems courses. Table 1 shows mean score of respondents.

Table 1: Scores of Respondents on Seven-Item Knowledge Quiz

Gender	***N***	***m***	***sd***
Male	76	4.43	1.30
Female	103	4.15	1.46
Total	179	4.27	1.40

Cluster analysis helped determine the difference between knowledge levels of respondents. Using the Hierarchical Cluster Analysis of finding three clusters by using the nearest neighbor method, it was found that a "low knowledge" group consisted of 19 respondents and had a mean score of 1.74 out of maximum seven correct answers, the "average knowledge" group consisted of 30 respondents and had a mean score of 3.00, and a "high knowledge" group consisted of 130 respondents and had a mean score of 4.93 out of seven maximum points. An independent samples t-test comparing the mean scores of males (m=4.43, sd = 1.3) and females (m=4.15, sd=1.46) found no significant difference in quiz scores (t (177) = 1.37, $p > .05$).

Students participating in the survey were enrolled in three courses taught by different instructors. Instructor 1 taught a graduate course in Leadership, and Instructors 2 and 3 taught undergraduate courses in Computer Information Systems. Students from

different departments (including pre-majors) in the Business School took these courses. None of the three courses specifically covered the topic of information security in courses so any information on information security awareness was considered to be pre-existing knowledge. Instructor 1 had a total of 31 students who scored an average of 4.97 (sd=1.25) on the knowledge quiz, Instructor 2 had 94 students who scored 4.03 (sd=1.37), and Instructor 3 had 54 students who scored 4.27 (sd=1.42).

A one-way ANOVA was computed comparing the knowledge quiz scores of the respondents who took a course from one of the three different instructors. This was done to see if any threats to validity emerged because three different classes were used. A significant difference was found among the instructors ($F(2,176) = 5.468$, $p<.05$). Tukey's HSD was used to determine the nature of differences between instructors. This analysis revealed that students who had Instructor 1 scored higher ($m = 4.97$, $sd = 1.25$) than students who had Instructor 2 ($m=4.03$, $sd =1.37$). There was no significant difference with students who had Instructor 3 ($m= 4.27$, $sd = 1.42$).

A Spearman *rho* correlation was calculated examining the relationship between individuals' experience using the Internet and knowledge of information security topics as measured by the questions on the survey instrument. A weak correlation that was not significant was found ($r(177)= .090$, $p> .05$). Experience was not related to knowledge about information security behavior.

Hypothesis 2: Attitude, subjective norm, and confidence in WRHC users may correlate with behavioral intention to maintain information security behavior.

For testing this hypothesis, results shown in Table 2 were used. Correlation between the four constructs was significant at the $p<.01$ level.

Table 2: Descriptive Statistics of Survey Items

	m	***sd***	***Attitude***	***SN***	***PBC***	***BI***
Attitude (α=.82)	5.53	2.86	--			
SN (α=.77)	5.95	3.05	.73(**)	--		
PBC (α=.85)	5.93	2.87	.60(**)	.63(**)	--	
BI (α=.66)	5.00	3.08	.68(**)	.61(**)	.67(**)	--

m=mean, *sd*=standard deviation, α=reliability coefficient
** Correlation is significant at the 0.01 level ($p<.01$).

Cronbach alpha (α), which is a measure of internal consistency (or Reliability) was also calculated for individual constructs and the scale. Although Cronbach alpha reliability coefficient of the overall scale was found to be .88, it was noted that the

construct of behavioral intention had lowest level of reliability indicating better items are needed for this construct. Nunally (1978) has stated that overall Cronbach alpha of 0.8 is considered acceptable criterion for internally consistent scales.

Hypothesis 3: WRHC user behavior and intention to maintain information security can be predicted by attitude, confidence and subjective norm.

A Path Analysis was conducted on the model to test Hypothesis 3. Figure 2 shows standardized structural path coefficients for the model.

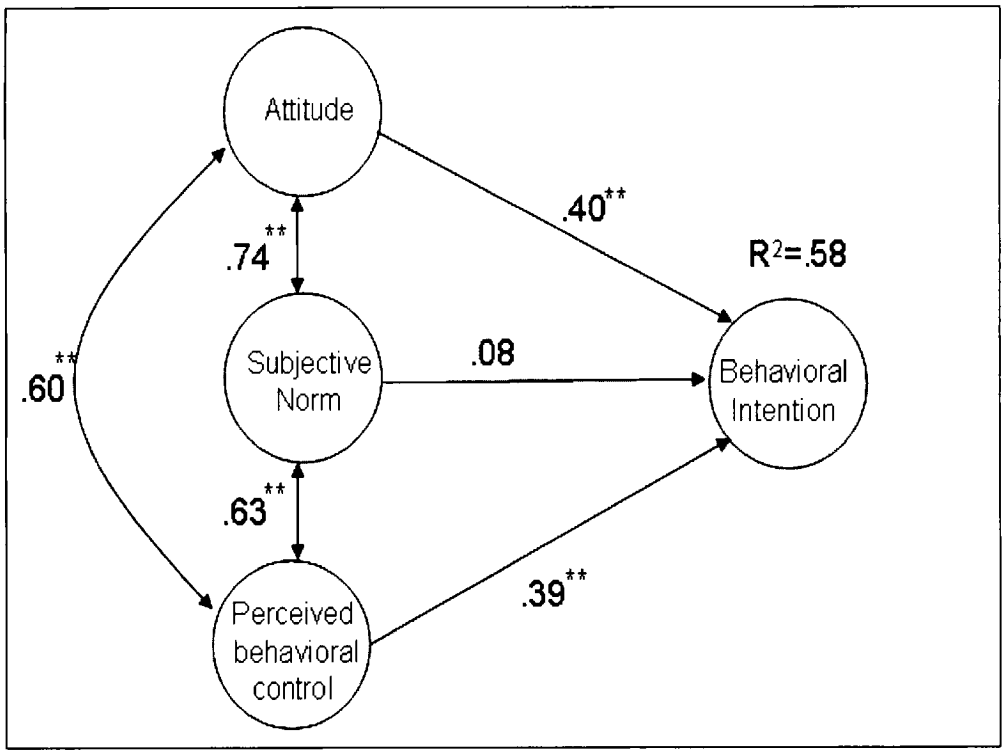

Figure 2: Path Analysis of Ajzen's Theory of Planned Behavior

Multiple regressions were conducted as part of Path Analysis to predict respondents' behavioral intention toward information security behavior. A significant regression was found ($F(3,175)=78.88$, $p<.01$), with an R^2 of .58. The model explained 58% of a WRHC individual's intention to maintain information security by using antecedents of Attitude, Subjective Norm, and Perceived Behavioral Control.

DISCUSSION

Results support the use of TPB to explain WRHC user intention to maintain information security. The study showed that attitudes, subjective norm, perceived behavioral control (confidence) are related to maintaining information security awareness. For the sample used in the study, majority of respondents had good knowledge of information security awareness as measured by the instrument. Previous studies (e.g. Nyamathi, Bennett, Leake, Lewis, & Flaskerud, 1993; Woon, Tan, & Low, 2005) have found that a user's knowledge has an effect on behavior. Knowledge is important in maintaining information security awareness because of increased sophistication used by hackers in phishing schemes to extract information from unsuspecting users. The results also showed experience in using the Internet is not related to knowledge about information security behavior. This implies training is essential in informing and reinforcing the need to maintain information security when employees perform work-related tasks from home computers. Gender differences did not exist in the context of information security awareness as well as knowledge of information security topics. Since there was a direct path from each variable to each other variable, a saturated model fitting the data was noted. The saturated model found in this study can also provide useful information in the search for a more parsimonious, unsaturated model where some of the parameters of the saturated are not estimated (Hershberger, 2005).

In studying the relationship among exogenous variables, the three variables of Attitude, Subjective Norm, and Perceived Behavioral Control showed strong path coefficients. Subjective Norm was not highly weighted while Behavioral Intention, Attitude and Perceived Behavioral control had moderate weight with intention to maintain information security awareness. The Subjective Norm finding was contrary to that reported earlier by Bannerjee et al. (1998) as well as Chan et al. (2005). Attitude and confidence had the highest influence on intention to maintain awareness about information security.

Based on this finding, organizational training programs and colleges should offer technology related courses which include content to teach students about information security issues, thereby giving them more confidence and a better attitude, especially when using the Internet and social networking sites where identity theft and compromise of personal information is most likely to happen. This content can also be covered in new employee orientation workshops since technology devices belonging to the company (such as laptops and PDAs) may be used to access non-work related web sites. The training programs can also focus on information management decision making by presenting scenarios that address risks, associated costs, consequences, and benefits of such actions (West, 2008). The managerial implications of this study go beyond focusing on technology requirements to maintain information security. While a WRHC user may be offered training in technical aspects of information security (such as the configuration of personal firewalls, or periodically running a virus/spyware scan), managers should be cognizant that social and psychological factors of individuals also play an important part in sustaining such behavior. End users must be motivated to take pro-security actions. Limitations of this study include the fact that two undergraduate and one graduate course were used in the study to

represent WRHC users, and that all students were from the same college at one university. The model used in this study accounted for 58% of the variance indicating there are other variables that should be investigated for explaining additional variance.

CONCLUSION

Today, technology devices are purchased, installed, maintained, and used by individuals who may not have specialized knowledge of information technology and security. These devices are then used to access work-related as well as non-work related websites from remote locations. Weak links and vulnerabilities that may be introduced as a result of daily use exist within any system regardless of how well it is installed and maintained. Although technology countermeasures can act as a deterrent in devices for acts already perpetrated, only the human element, interacting with technology, can act as a true deterrent to theft and asset misappropriation consequences of lapse in information security behavior. In the past security specialists have often turned to social psychology to help understand the best way to approach employees and educate them in change their attitudes and behaviors toward fraud, identity theft, and information security. By understanding social cognition, we can better teach users about effective information security behavior. Social cognition helps us to understand how different people (such as WRHC users in this study) are influenced by ideas that affect behavior, and how attitude, experience, knowledge can guide an individual's behavior. This study extended Theory of Planned Behavior to predict information security awareness and behavior of employees who perform work-related computing on home computers. Results of this study can provide insights to managers on employee behavior, motivation, and attitude, which are critical factors to consider maintaining compliance with organizational security policies when employees perform work-related tasks from home computers. More research needs to be done on socio-demographic factors that affect user behavior toward information security. Gender differences regarding information security behavior can be investigated, as well as further scale development and validation in the area since a standardized scale measuring information security awareness does not exist. Social computing Web 2.0 sites which rely on active user collaboration and behavior can also be researched as potential risk factors for organizational security.

REFERENCES

Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

Ajzen, L. (1988). *Attitudes, Personality, and Behavior.* IL: Dorsey Press.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

Bandura, A. (1997). Self-*Efficacy: The Exercise of Control*. New York: W. H. Freeman and Company.

Banerjee, D., Cronan, T., and Jones, T. (1998). Modeling IT Ethics: A study in situational ethics. Retrieved September 12, 2008, from http://proquest.umi.com.

Biros, D., Daly, M., and Gunsch, G. (2004). The Influence of Task Load and Automation Trust on Deception Detection. Retrieved November 16, 2008, from http://proquest.umi.com.

Bitter, C. G., & Davis, S. J. (1985). Measuring the development of computer literacy among teachers. *AEDS Journal*, *18*(4), 243-253.

Briggs, R. O., Balthazard, P.A. & Dennis, A. R. (1996). Graduate business students as surrogates for executives in the evaluation of technology. *Journal of End User Computing, 8*(4), 11-17.

Chan, M., Woon, I, and Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Retrieved December 7, 2008, from http://proquest.umi.com.

Chau, Y. K., & Hu, J. H. (2001). Information technology acceptance by individual professionals: a model comparison approach. *Decision Sciences, 32*(4), 699-718.

Compeau, D. R., & Higgins, C. A. (1995). Computer self efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-212.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006) Why phishing works, Proceedings of the Conference on Human Factors in Computing System, Montreal, April 2006. Retrieved September 14, 2008 from Harvard University Engineering & Applied Sciences Department Web site: http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

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

Dinev, T. & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of Association for Information Systems*, *8*(7), 386-408.

Foltz, C. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, *12*(2), 154-166.

George, C. & Scerri, J. (2007). Web 2.0 and user-generated content: legal challenges in the new frontier. *Journal of Information, Law and Technology*. Retrieved March 8, 2008 from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/george_scerri/

Hazari, S. I. (1990). Development of a training model for microcomputer instruction of a college faculty. *Dissertation Abstracts International*, 51 (01). (UMI No. ABA91-06537).

Hershberger, S. L. (2005). Saturated model. *Encyclopedia of Statistics in Behavioral Science*. doi: 10.1002/0470013192.bsa580.

Highland, H. J. (1993). A view of information security tomorrow. In E. G. Dougall (Ed.), *Computer security*. Holland: Elsevier.

Hoffman, M., & Blake, J. (2003). Computer literacy: Today and tomorrow. *Journal of Computing Sciences in Colleges*, *18*(5), 221-233.

Johnson, M. F. (1980). Computer literacy: What is it? *Business Education Forum*, *35*(3), 18-22.

Kabay, M. (1993). Social Psychology holds lessons for security experts. *The Risks Digest*, *19*(24), 33. Retrieved November 10, 2008 from ProQuest Database.

Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597-607.

Krantz, M. (2006). "The Guys Behind MySpace.com," *USA Today*. Published online: 12 February 2008.http://www.usatoday.com/money/companies/management/2006-02-12-myspace-usat_x.htm

Leonard, L., Cronan, T. Kreie, J. (2004). What influences IT ethical behavior intentions: planned behavior, reasoned action, perceived importance, or individual characteristics? *Information and Management*, 42(1), 143-158.

Lukwago, S., Kreuter, M., Holt, C., Steger-Mey, K., Bucholtz, D., Skinner, C. (2003). Sociocultural correlates of breast cancer knowledge and screening in urban African American Women, *American Journal of Public Health*, *93*(8), 1271-1275.

Lee, Y., & Kozar, K. (2005, August). Investigating factors affecting adoption of anti-spyware systems. *Communication of the ACM*, *48*(8), 72-77.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*(3), 191-204.

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research, 3*(2), 173-191.

National Strategy to Secure Cyberspace. (2003, February). Retrieved December 14, 2008 from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

NCSA/Symantec Home User Study (2008). Retrieved January 29, 2009 from http://staysafeonline.mediaroom.com

Nunally, J. C. (1978). *Psychometric theory*. New York: McGraw-Hill.

Nyuamathi, A., Bennett, C., Leake, B., Lewis, C., and Flaskerud, J. (1993). AIDS-Related knowledge, perceptions, and behaviors among impoverished minority women, *American Journal of Public Health*, 83(1), 65-72.

Parameswaran, M., & Whinston, A. B. (2007). Social Computing: An Overview, *Journal of the Association for Information Systems. 8*(6), 336-350.

Pee, L. G., Woon, I. M., & Kankanhalli, A. (2008). Explaining non-work related computing in the workplace: A comparison of alternative models. *Information & Management, 45*(2), 120-130.

Rhodes, K. (2001). Operations security awareness: The mind has no firewall. *Computer Security Journal, 18*(3), 27-36.

Richardson, R. (2008). *CSI/FBI Computer crime and security survey*. Retrieved January 29, 2009 from http://www.gocsi.com

Rogers, E.M. (1995). *Diffusion of Innovations* (4th ed.). Free Press: New York, NY.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world*. NY: Copernicus books.

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

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security, 7*(3), 121-128.

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

Summers, R. (1997). *Secure computing: Threats and safeguards*. New York, NY: McGraw-Hill.

Taylor, S., Todd, P. A. (1995). Understanding information security usage: a test of competing models. *Information Systems Research, 6*(2), 144-176.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34-41.

Whitman, M., & Mattord, H. (2003). *Principles of information security.* MA: Thomson - Course Technology.

Woon, I. M., Tan, G. W., Low, R. T. (2005). A protection motivation theory approach to home wireless security. *Proceedings of the Twenty-Sixth International Conference on Information Systems*, Dec. 11-14, 2005, 367-380.

Workman, M. & Gathegi, J. (2006). Punishment and ethics deterrents: A study of insider security contravention, *Journal of the American Society for Information Science and Technology*, *58*(2), 212-222.

Sunil Hazari is an Associate Professor in the Richards College of Business, University of West Georgia. His teaching and research interests are in the areas of Business Education, Information Security, Web Usability, and Web 2.0 applications. He has authored several peer-reviewed journal publications in Information and Instructional Technology areas, has presented papers at regional and national conferences, and is editorial board member of several information system journals. Website: http://www.sunilhazari.com/education

Beth Clenney is a Lecturer in the Richards College of Business, University of West Georgia where she teachers courses in the Department of Management. She has received several teaching awards, including Beta Gamma Sigma Teacher of the Year, and the University of West Georgia Teacher of the Year. She is currently working on her Ph.D. at Georgia State University.

William Hargrave is a doctoral student at the University of Georgia. His dissertation topic deals with analysis of post-secondary business-communication classes for cooperative learning practices. He previously taught business communication and computer courses at the University of West Georgia.