https://doi.org/10.48009/1_iis_2010_649-658

CHANGES IN EMPLOYEE INTENTION TO COMPLY WITH ORGANIZATIONAL SECURITY POLICIES AND PROCEDURES FACTORING RISK PERCEPTION: A COMPARISON OF 2006 AND 2010

Queen Esther Booker, Minnesota State University, Mankato, queen.booker@mnsu.edu
Fred L. Kitchens, Ball State University, fkitchens@bsu.edu

ABSTRACT

Protecting corporate assets, both the physical and the digital is a major concern for managers. Managers seek ways to encourage employees to adhere to and follow organizational security policies to protect not only the organization as a whole but also the employee and the customer as well. Part of the reason existing security measures fail is because employees fail to follow organizational security policies and procedures but this failure is not necessarily due to the organizational controls; it can also be related to the individual's perception of risk and the person's general attitude towards security policies and procedures. This study compares the results of a 2006 national study with data collected in 2010 to compare and contrast how employee intentions have changed during the five year period. The study includes perceived personal risk with constructs for attitudes toward security policies and technologies.

Keywords: Security, theory of planned behavior, risk

INTRODUCTION

Security, as defined by websters.com, is "the state of being free from danger or injury." Managers of the modern organization, thanks to the growth of Internet based technologies and the growth in workplace violence, find themselves constantly focusing on security measures to increase the safety of workers and data alike. They do so through the declaration of policies and the implementation of security devices such as monitoring systems. The literature suggests that barriers to acceptance of security devices can be grouped into the following categories: organizational commitment, physical invasiveness, information invasiveness, ease of use, privacy, and the perceived level of benefit from the device [7, 12].

Security systems (policies and technologies) and the people who manage them have received increased accountability for the security of data regardless if employees actually follow or use organizational security tools. Unfortunately, security policies and technologies often conflicts with personal privacy and perceived risk concerns. Privacy advocates claim security often invades individual's privacy by providing means to capture and monitory information on individuals. Yet, with the need for greater accountability for movements and actions across information systems, organizations employ a variety of technologies to support organizational policies including but not limited to biometric devices, badge systems, password systems, video surveillance, email monitoring, computer usage monitoring, and Internet usage monitoring. [3]

Some security procedures such as protecting access to a building are more acceptable than others such as password policies. This is because employees understand limiting access to the physical building as they themselves limit access to their own homes through keys and various security systems. But networked systems are young by comparison to physical locations, and thus, employees may not have the same level of experience and knowledge to take security precautions as seriously. But the theft and misuse of digital information in the networked organization require organizations to develop tools to protect digital information just as they need to protect the physical and human resources of an organization. The value of digital data requires managers to protect it with specific security policies and technologies, and have mechanisms to enforce these policies [8]. Expectedly, companies engage in networked systems security policies and procedures such as password policies to help measure, shape, or control the behavior of employees.

Previous research has shown that some employees dislike security policies and distrust monitoring systems, and some even actively thwart their organization's use of these systems by altering monitoring equipment/software or by avoiding monitored areas [4, 9, 13, 14, 15, 17, 18]. Others simply do not comply with company policies. If employees succeed in circumventing systems, then the security technology and policies provide little of its intended value. The effectiveness of organizational monitoring techniques, and policies,

then, depends on employees' willingness to comply with their use. Insights into employees' intentions to comply with policies or circumvent monitoring tools are helpful in promoting effective use of these technologies. Studies examining acceptance of monitoring systems as a necessary prerequisite for their functioning include a study on acceptance and use of active badge monitoring systems [6], awareness monitoring systems [20, 21], and password systems [7]. All the studies presented empirical evidence that there are relationships between usage depending on whether or not employees had choice, the level of commitment and loyalty to the organization, and how invasive the technology seemed to the employee. The Booker & Kitchens study included an analysis of risk perception to the employee as well as a construct to measure comfort with public security systems.

The reason for studying employee intentions is that employees are unable to choose whether they want to use or have the technology used for their benefit. For example, many organizations force users to use passwords to access confidential systems and to change their passwords at least annually, and in doing so ask for a password of a certain length as well as have a combination of letters and numbers. Organizations can also use tools to monitor email traffic, email content, Internet traffic and Internet behavior without the consent and knowledge of the employee. Organizations also may use video surveillance equipment active badges, and digitally coded access keys that track an employee's movement or attempted movement into certain parts of the organization's campus.

To date, only a few studies have been conducted that examined employee compliance or resistance to such monitoring systems. Three recent studies that focus primarily on security related concerns include the study by James et al [7] that investigated the intention to use biometric devices, the study by Spitzmuller and Stanton [13] that investigated the intention to thwart monitoring systems related to email, and finally the study by Booker and Kitchens [4] that focused on passwords and risk perceptions.

The objective of this study is to update the Booker & Kitchens 2007 study to determine if attitudes of compliance and resistance with organizationally-imposed policies and monitoring systems as well as public systems have changed from those in 2006. Since the publication of the original study the United States public has been subjected to additional security measures such as use of whole body imaging at airports [11], increased public video surveillance [10], and increased emphasis on password control measures [23]. Having a national view of employees' compliance and resistance behaviors can help managers measure their progress in implementing programs and techniques to minimize the behaviors on the security of the company's physical and information assets.

The next section provides the background for the study. Section 4 discusses the methodology used and Section 5 presents the results as well as the comparisons to the 2007 study. Section 6 describes the limitations of this study along with the conclusion and directions for future research.

BACKGROUND

Spitzmuller and Stanton [13] argued that intention to mitigate security technologies such as video surveillance and computer monitoring are intentional and thus best predicted by intentions toward the attitudes, commitments and beliefs of the individual. Intentions are assumed to capture the motivational factors that influence the behavior and are indicators of how hard people are willing to try in order to perform the behavior [1]. In other words, intentions are immediate antecedents of actual behavior [1, 2].

What factors affect an employee's intention to circumvent security policies? Is it fear of invasion of privacy? Is it due to a concern due to personal risk? Or is it simply an intrusion on individual rights? Previous researchers have suggested and found empirical support for the hypothesis that perceived need for privacy as well as personal ethics, beliefs are related to intentions to use or not use security protocols within organizations, and perceptions of risk are all pertinent to employee intentions [4, 8, 13].

The theory of planned behavior (TpB) has during recent years become one of the most widely used theories to explain and predict human behavior. TpB has been applied to a variety of behaviors related to computer technology, with the most popular being the technology adoption model used to determine ease of use and perceived usability of various technologies [1]. TpB is an extension of the theory of reasoned action. In TpB, perceived behavioral control is theorized to be an additional determinant of intention and behavior [1]. TpB is a theory of predicting intentions based attitudes, beliefs, social norms, intentions, volitional control, and behavior. Volitional control served as a moderator variable: given a certain level of intentions, a behavior would more likely occur in situations where the behavior was under the control of the actor.

TpB frameworks have application to the study of compliance and resistance pertaining to security technologies. Employees may hold certain beliefs and may form attitudes about organizational policies, monitoring and surveillance based on these beliefs. In turn, intentions to comply or resist may relate to attitudes as well as social norms about these behaviors. Whether employees then comply or resist may depend upon intentions and volitional control. Prior research has applied the theory of planned behavior to examinations of unauthorized behavior in organizations. For example, Loch and Conger [8] applied the theory of planned behavior to employees' use of computers in organizations, and found that attitudes and social norms predicted intentions to misuse the organization's computers. Their study thus supported the utility of the theory in predicting behavioral intentions with reference to uses of technology in organizations. Spitzmuller and Stanton [13] applied the theory to behavior of employee's mitigation or lack of compliance with email monitoring and, too, found attitudes and social norms as prediction of intention to not comply.

The Booker and Kitchens study extended the Spitzmuller and Stanton and Loch and Conger studies by including risk. Risk is a personality trait that has been found to have an effect on behaviors that lead to work place errors [5]. A study by Salminen and Heiskanen [12] also addressed the theory of risk behavior and found that people have a steady level of risk they are willing to assume and adjust their behavior accordingly. Thus, people are willing to take more risk in situations that have less inherent risk. In the Booker and Kitchens study, the researchers found that employees with a low perception of risk were more likely to have an intention to comply with security policies and procedures but attitudes towards public security policies and procedures reduced intentions to comply with organizational policies and procedures. This is problematic because the study suggested that public security policies and procedures can negatively impact organizational intentions thus mitigating any processes an organization may undertake to improve compliance. This follow up study was conducted to determine if attitudes in generally are changing and if so if the changes are improving or worsening. Further, given the increased emphasis on public security and the perceived increase of public risk in the United States, this study expected to find lower intentions to comply with organizational policies in 2010 than were found in the 2006 data.

METHODOLOGY

The purpose of the 2010 study was to compare and contrast national attitudes towards security policies and procedures with those in 2007. Both studies used a Likert-type scale survey designed to study the user behavior toward security policies and technologies, the intention to use these devices, and the perception of risk to the user, providing insight into possible barriers to adoption of general security technologies. No changes were made to the 2010 survey instrument. The data used in 2007 was collected in 2006 and the data used in the 2010 study was collected in 2010. The survey was made available to individuals at four different types of conventions – a bead show, a home show, a technology convention, and a personal interest show. Individuals who completed the survey were given the chance to win an iPod. An additional Zoomerang survey was made available over the Internet and was advertised through word-of-mouth, email, and through organizations wanting to compare their information to other organizations. The organizations offered their employees a range of prizes from gift cards to an extra week of vacation. The 2007 hypotheses were:

H1a: The more favorable the attitude towards general security protocols, the stronger the individual's intention to comply with organizational security policies.

H1b: The more favorable the attitude towards general security protocols, the stronger the individual's intention to comply with organizational security technologies.

H2a: The lower the perceived risk to the employee in the use of security policies, the stronger the individual's intention to comply with security policies.

H2b: The higher the perceived risk to the employee in the use of security technologies, the stronger the individual's intention to resist the security technologies.

H3a: The higher the perceived commitment to the organization, the stronger the individual's intention to comply with security policies.

H3b: The higher the perceived commitment to the organization, the stronger the individual's intention to comply with security technologies.

The researchers rejected hypotheses H1a and H1b but accepted all the others. The hypotheses for the 2010 study included the same hypotheses as those from the 2007 study. In addition, the researchers added:

H4: The attitude towards general (public security policies) would significantly decrease in 2010 when compared to the 2007 study.

The reason for this hypothesis is that while the relationship between general security and organizational technologies and policies might remain the same, the level of intentions could change given the increased level of surveillance imposed by the government.

The 2010 study followed the 2007 study by attending similar shows to capture a similar group of people. The survey was made available to individuals at four different types of conventions – a bead show, a home show, a technology convention, and a personal interest show. Individuals who completed the survey were given the chance to win an iPod. An additional Zoomerang survey was made available over the Internet and was advertised through word-of-mouth, email, and through organizations wanting to compare their information to other organizations. The organizations offered their employees a range of prizes from gift cards to an extra week of vacation. Table 1 shows the respondents from the various data collection locations:

Collection type	Bead Show	Home Show	Technology Show	Adult Show	Online Survey
Number of respondents 2006	59	68	112	65	215
Number of respondents 2010	46	115	280	107	5249

Table 1. Respondents by Data Collection Location/Method

As with the 2007 study, the largest number of responses was collected through the web. Stanton and Rogelberg's [16] recommendations for ensuring high quality data from web-based samples was followed to ensure high quality.

	Number of Respondents	
Demographic	**2006**	**2010**
Industry Type		
For profit	221	2836
Non-profit	76	53
Government	67	112
Ethnicity		
US Citizen	312	2853
Non US Citizen	54	148
Gender		
Male	216	1897
Female	148	1104
Age Distribution		
> 50	45	257
>=40 to 50	147	554
<40	172	2190
Use Databases on a Daily Basis for Job (Yes)	219	2459
Use the Internet on a Daily Basis for Job (Yes)	216	2841
Degree in a Computer Related Field (Yes)	39	1105
Average Age	37	32

Table 2. Demographic Breakdown of Usable Responses

The 2006 targeted number of responses was 1000 but the collected number was only 519. The number of usable responses was 364. Surveys were eliminated due to incomplete survey or person unemployed or retired. The target for 2010 was also 1000 but the number collected was 5797 with a large percentage from the Internet. Of the 5797 collected surveys, only 3,001 were usable due to respondents being under-

aged, unemployed or retired. The demographic breakdown of the usable responses for both years is shown in Table 2.

The study utilized a Likert-style survey with 37 questions not including the demographic questions. The survey questions are available upon request from the authors. The answers were measured using a 5-point Likert scale ranging from strongly disagree to strongly agree. To ensure that responses from the five different sub-samples could be combined for purposes of analysis, a confirmatory multi-group structural equal model scale of scores in the different sub-samples was performed using a structural equation program with generalized least-squares estimation. The focus was on the conformity of an overall path model rather than on the factor structure of indicators of different constructs. The analysis followed the template provided by Bollen [3] for multi-group analysis and used by Spitzmuller and Stanton [13] and Booker and Kitchens [4]. Results of the multi-group analysis indicated there were no differences between the sub-samples. Therefore, all the sub-samples were combined to test the hypotheses. Also, data collection from multiple sources across multiple organizations makes the results of the study generalizable as the study is not limited to a particular organization's prevailing culture.

Outcome variables in this study were intentions to comply with or resist security policies and technologies and are the same variables used in the 2007 Booker and Kitchens study and are listed in Table 3.

Variable Label	**Outcome Variable Description**
F1	Commitment to the organization
F2	Comfort with public policies on security
F3	Perceive technology as easy to use
F4	Attitude towards organizational security policies
F5	Attitude towards organizational security technologies
F6	Belief of perceived risk regarding organizational security policies
F7	Belief of perceived of risk regarding organizational security technologies
F8	Accept organizational security policies
F9	Accept organizational security technologies
F10	Avoid organizational security policies
F11	Avoid organizational security technologies
F12	Manipulate organizational security policies
F13	Manipulate organizational security technologies
F14	Complain about organizational security policies
F15	Complain about organizational security technologies
F16	Organization organizational has a rules culture
F17	Organization organizational has a caring culture

Table 3: Study Variables

The first step in the analysis was to calculate the descriptive statistics for both years. That information is shown in Table 4 which lists the mean and standard deviation for each of the factors analyzed in the study for both years. Recall the Likert-scale for the survey was a 5 point scale, with one being strongly disagree and 5 being strongly agree. There was a shift in commitment to the organization from neutral towards disagree but this could be explained by the current recession and the layoffs and the increased number of younger people (under 40) in the 2010 study. Further, there was a decline in comfort with public policies on security but an increase in the perception of technology as easy to use. This improvement may be attributable to the increase in the use of the Internet and databases in the number of people who reported both in their day to day work as compared to 2007. The perceived risks of organizational policies and technologies also decreased as intentions to avoid organizational security policies and technologies. However this did not lead to a higher acceptance of either policies or technologies. The 2010 data had more variability than the 2007 data for several variables. However, the means for many variables such as commitment to the organization and comfort with public policies on security were notable lower for 2010 than for 2007 with less variability.

	2007		2010	
Variable	**Mean**	**Std. Dev.**	**Mean**	**Std. Dev.**
F1. Commitment to the organization	3.12	1.25	2.75	1.09
F2. Comfort with public policies on security	3.37	1.32	2.78	1.08
F3. Perceive technology as easy to use	3.82	1.02	4.00	1.15
F4. Attitude towards organizational security policies	3.38	1.36	2.99	1.41
F5. Attitude towards organizational security technologies	3.18	1.36	3.02	1.42
F6. Belief of perceived risk regarding organizational security policies	3.13	1.3	2.99	1.40
F7. Belief of perceived of risk regarding organizational security technologies	3.86	0.96	3.02	1.42
F8. Accept organizational security policies	3.64	1.15	3.18	1.48
F9. Accept organizational security technologies	3.26	1.27	3.02	1.40
F10. Avoid organizational security policies	3.24	1.3	2.94	1.39
F11. Avoid organizational security technologies	3.26	1.28	3.00	1.43
F12. Manipulate organizational security policies	2.73	1.42	2.98	1.42
F13. Manipulate organizational security technologies	2.89	1.41	2.98	1.42
F14. Complain about organizational security policies	3	1.43	3.01	1.41
F15. Complain about organizational security technologies	3.09	1.43	3.00	1.42
F16. Organization organizational has a rules culture	3.02	1.41	3.32	1.33
F17. Organization organizational has a caring culture	3.16	1.22	2.73	1.39

Table 4. Means and Standard Deviations for Study Variables

Cronbach's alpha internal consistency estimates for all scales were also computed for both the 2007 and the 2010 data and was high (.51) using all items. This provided a better suggestion of consistency than the 2006 data that had a Cronbach's alpha of .232. A correlation analysis was performed for the all the variables and are shown for both the 2006 data and the 2010 data are shown in Table 5 and Table 6 respectively.

Some surprising outcomes for the 2006 data were the negative correlations. For example, there was a negative correlation between perceived risks of security policies and technologies. Also, the removal of the variable related to perceived risk of organizational security policies improved the Cronbach's alpha to approximately 0.50.

In the 2010 data, there was a negative correlation between commitment to the organization and perception of technology as being easy to use. But there was a positive correlation between commitment to the organization and attitudes towards organizational security policies and procedures for both 2006 and 2010 data. The comparisons of where correlations were similar in terms of being positive or negative are shown in Table 7. The N indicates that correlations for both studies were negative, P means the correlations for both studies were positive and M means the correlations were mixed.

	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17
F1	-0.03	0.03	0.11	0.16	-0.04	0.06	0.13	0.08	0.06	0.01	-0.01	0.01	0.03	-0.01	0.02	-0.02
F2		-0.05	-0.11	-0.03	0.06	0.07	0.01	-0.02	-0.04	-0.05	-0.07	-0.01	0.05	0.07	-0.03	0.01
F3			0.01	0.03	0.03	-0.06	-0.08	-0.01	0.03	0.02	-0.04	0.00	0.14	-0.07	0.05	0.04
F4				0.14	-0.14	0.03	0.06	0.08	0.05	0.05	-0.02	-0.04	0.03	-0.01	-0.02	-0.03
F5					-0.07	0.07	0.10	0.05	0.03	0.05	-0.02	0.04	-0.01	0.01	-0.04	0.02
F6						-0.04	-0.08	-0.68	-0.62	-0.58	-0.51	-0.03	0.00	0.09	0.00	-0.04
F7							0.76	0.08	-0.02	0.05	0.01	0.10	-0.03	-0.04	0.00	-0.01
F8								0.07	0.01	0.03	0.02	0.10	-0.02	-0.04	-0.04	-0.02
F9									0.60	0.82	0.45	0.00	0.04	-0.07	0.04	0.10
F10										0.48	0.73	0.05	0.04	-0.09	0.00	0.08
F11											0.35	-0.03	0.02	-0.02	0.04	0.11
F12												0.04	0.03	-0.07	0.07	-0.02
F13													0.10	-0.06	0.05	0.03
F14														0.04	-0.01	0.00
F15															-0.02	-0.08
F16																0.04

Table 5. Inter-correlations among Study Variables for the 2006 data (2007 study)

	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17
F1	0.02	-0.07	0.01	0.00	-0.01	0.01	0.00	0.02	0.01	-0.02	0.01	-0.02	-0.03	0.01	0.05	-0.07
F2		-0.04	0.00	0.01	-0.02	0.02	0.02	0.00	0.01	-0.03	0.00	-0.03	-0.02	0.00	0.04	-0.04
F3			0.02	0.00	0.03	-0.03	-0.07	0.02	-0.02	0.00	-0.01	-0.04	-0.01	0.00	-0.05	-0.01
F4				-0.02	-0.04	-0.01	-0.02	-0.04	0.00	-0.01	-0.02	0.00	0.02	0.01	0.00	0.01
F5					0.02	0.01	0.00	0.00	0.05	0.01	0.03	0.03	0.00	-0.02	0.03	-0.02
F6						0.03	-0.01	-0.01	0.02	0.00	0.01	0.00	-0.01	0.00	0.00	0.01
F7							0.02	-0.01	0.00	-0.03	0.01	0.00	-0.02	-0.01	-0.01	0.02
F8								0.01	-0.01	0.00	0.00	0.01	-0.01	-0.02	0.02	-0.02
F9									-0.04	0.01	0.04	0.00	0.00	0.01	0.00	0.00
F10										0.01	-0.01	0.02	0.00	-0.01	0.02	0.03
F11											0.03	0.02	0.02	0.00	-0.03	-0.02
F12												-0.03	0.01	0.01	0.00	0.01
F13													-0.01	0.03	0.00	0.03
F14														-0.02	0.00	0.01
F15															0.01	0.04
F16																-0.05

Table 6. Inter-correlations among Study Variables for the 2010 data (2010 study)

	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17
F1	M	M	P	P	N	P	P	P	P	M	M	M	M	M	P	N
F2		N	N	M	M	P	P	M	M	N	M	N	M	P	M	M
F3			P	P	P	N	N	M	M	M	N	M	M	M	M	M
F4				M	N	M	M	M	P	M	N	N	P	M	N	M
F5					M	P	M	P	P	P	M	P	N	M	M	M
F6						M	N	N	M	N	M	M	M	M	M	M
F7							P	M	M	M	P	M	N	N	M	M
F8								P	M	M	P	P	N	N	M	N
F9									M	P	P	M	P	M	M	M
F10										P	M	P	M	N	M	P
F11											P	M	P	N	M	M
F12												M	P	M	M	M
F13													M	M	P	P
F14														M	M	M
F15															M	M

Table 7: Correlation Comparisons between 2006 and 2010 data

Of the 135 correlations, more than half (75) had a change in coefficient sign. The major shifts occurred in correlations to F6: Belief of perceived risk regarding organizational security policies with a seventy three percent change and F3: Perceive technology as easy to use.

RESULTS

Recall the hypotheses for the study for both the 2006 and 2010 data:

H1a: The more favorable the attitude towards general security protocols, the stronger the individual's intention to comply with organizational security policies.

H1b: The more favorable the attitude towards general security protocols, the stronger the individual's intention to comply with organizational security technologies.

H2a: The lower the perceived risk to the employee in the use of security policies, the stronger the individual's intention to comply with security policies.

H2b: The higher the perceived risk to the employee in the use of security technologies, the stronger the individual's intention to resist the security technologies.

H3a: The higher the perceived commitment to the organization, the stronger the individual's intention to comply with security policies.

H3b: The higher the perceived commitment to the organization, the stronger the individual's intention to comply with security technologies.

The additional hypothesis for the 2010 study was:

H4: The attitude towards general (public security policies) would significantly decrease in 2010 when compared to the 2007 study.

For both the 2006 data and the 2010 data, Hypotheses H1a and H1b can be rejected by the correlation analysis. Attitudes towards general public security measures were not influenced by organizational policies or technologies. Hypotheses 2a and 2b both related to the perception of risk to the individual. Based on the correlation analysis, perceived risk of policies was correlated with acceptance of policies but the perceived risk of security technology was NOT correlated with acceptance of security technologies for the 2006 data. For the 2010 data, neither was true so the 2a is accepted for the 2006 data and rejected for 2010, and 2b is rejected for both 2006 and 2010.

Hypotheses 3a and 3b both related to intention to comply with policies and technologies as related to the commitment and loyalty to the organization. The correlation model for the 2006 data has positive correlations. This was not the case with the 2010

data. Therefore, the hypotheses are accepted for 2006 and rejected for 2010.Hypothesis 4 was a comparison of attitudes towards general security public policies. A t-test was used to compare the means of the two data sets. The t-value was significant at p<.000 so Hypothesis 4 is accepted. The summary of hypotheses and their acceptance or rejections are shown in Table 8.

	2006		2010	
Hypothesis	**Accept**	**Reject**	**Accept**	**Reject**
1a		X		X
1b		X		X
2a	X			X
2b		X		X
3a	X			X
3b	X			X
4			X	

Table 8. Summary of Hypothesis Testing

CONCLUSIONS AND NEXT STEPS

The purpose of this study was to examine if perceived risk factored into intention to comply with organizational security policies and technologies, and if this factor changed between 2006 and 2010. The study compared results from the five year span of data collection. The study also extended existing research by looking across industries and across organizations. Due to the data collection methods, no one industry or organization dominated the study. However, the outcomes indicate several important factors, none as important, though, than the fact that perceived risk was the most significantly correlated variable in both models. While the influence changed between the years, the perception of risk increased significantly in the 2010 data. The message is clear: regardless of the industry or size of the organization, perceived risk from the use of security technologies and policies must be managed to minimize employees attempting to circumvent and or avoid the very systems put into place to protect the organization's digital assets. Thought must be put into place to alleviate fears regarding loss of individual privacy. Further, this preliminary analysis suggests that external influences may impact an organization's ability to mitigate its own security behavioral problems, particularly those related to government. More data needs to be collected to understand to what degree external forces influence individual behaviors.

This study requires significant further development. The next steps are to further analyze the data to determine if there are significant behaviors that can be extracted between age, gender, ethnicity, organization type and by technology experience. This study suggests a cookie-cutter model for managing intentions but it is unlikely a cookie-cutter model will work for all organizations. Therefore, another next step is to determine model nuances for specific types of organizations such as health care institutions, financial institutions and educational institutions. Further, this analysis relied on correlation analysis which in itself is not always definitive model for interpreting results. Factor analysis and regression models are critical in fully understanding the interactions between the variables and the output. Further, additional analysis should be conducted on the various data collection methods. The Cronbach's alphas were too small to insure internal consistency. Also, though the structured equation model indicated the subsets could be grouped for the purpose of analysis, there is likely to be bias in the different data collection methods that need to be studied.

REFERENCES

1. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 1–33.
2. Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: The role of intention, perceived control and prior behavior. Journal of Experimental Social Psychology, 22, 453–474.
3. Bollen, K. A. (1989). Structural equations with latent variables. New York: Wiley.
4. Booker, Q. & Kitchens, F. L. (2007). Predicting Employee Intention to Comply with Organizational Security Policies and Procedures Factoring Risk Perception. *IS One World Conference*.
5. Dahlbäck, O. (1990a). Personality and risk taking. Personality and Individual Differences, 11, 1235-1242
6. Harper, R. H. R. (1995). Why people do and don't wear active badges: A case study.

Computer Supported Cooperative Work, 4(4), 297–318.
7. James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006) Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. Journal of Organizational and End User Computing. Hershey: Jul-Sep 2006. 18 (3) 3, 1-24
8. Loch, K. D., & Conger, S. (1996). Evaluating ethical decision-making and computer use. Communications of the ACM, 39(7), 74–83.
9. Nussbaum, K., & du Rivage, V. (1986). Computer monitoring: Mismanagement by remote control. Business and Society Review, 56, 16–20.
10. Rampus, S. (2009) Video Surveillance in the Workplace, Buzzle.com (http://www.buzzle.com/articles/video-surveillance-in-the-workplace.html, accessed 3.10.2010)
11. Ravitz, J. (2009) Airport Security Bares All, or Does It? CNN.com/travel (http://www.cnn.com/2009/TRAVEL/05/18/airport.security.body.scans/, accessed 1.12.2010)
12. Salminen, S. and Heiskanen, M. (1997). Correlations between traffic, occupational, sports and home accidents. Accident Analysis and Prevention, **29**(1), 33-36.
13. Spitzmuller, C. & Stanton J. M. (2006). Examining employee compliance with organizational surveillance and monitoring, Journal of Occupational and Organizational Psychology, 79, 245–272
14. Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. Human Performance, 13, 85–113.
15. Stanton, J. M. (2002). Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, & A. Wenn (Eds.), Socio-technical and human cognition elements of information systems (pp. 79–103). London: Idea Group.
16. Stanton, J. M., & Rogelberg, S. G. (2001). Using Internet/Intranet web pages to collect organizational research data. Organizational Research Methods, 4, 199–216.
17. Stanton, J. M., & Weiss, E. M. (2000). Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. Computers in Human Behavior, 16, 423–440.
18. Stanton, J. M., & Weiss, E. M. (2003). Organisational databases of personnel information: Contrasting the concerns of human resource managers and employees. Behaviour and Information Technology, 22(5), 291–304.
19. Turner, R., Account Lockout Best Practices White Paper – Understanding Password Policies, diTii.com (http://www.ditii.com/2009/05/20/account-lockout-best-practices-white-paper-understanding-password-policies/, accessed May 15, 2010)
20. Zweig, D., & Webster, J. (2003). Personality as a moderator of monitoring acceptance. Computers in Human Behavior, 19(4), 479–493.
21. Zweig, D., &Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. Journal of Organizational Behavior, 23(5), 605–633.